CISA® Official Review Manual

28th Edition



CISA Certified Information Systems Auditor®
An ISACA® Certification

ISACA®

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. Among those credentials, ISACA advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified in Risk and Information Systems Control® (CRISC®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified Data Privacy Solutions Engineer™ (CDPSE™) credentials. ISACA is a global professional association and learning organization that leverages the expertise of its more than 170,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

Disclaimer

ISACA has designed and created *CISA® Official Review Manual 28th Edition* primarily as an educational resource to assist individuals preparing to take the ISACA certification exam. It was produced independently from the ISACA exam and the ISACA Certification Committee, which has had no responsibility for its content. Copies of past exams are not released to the public and were not made available to ISACA for preparation of this publication. ISACA makes no representations or warranties whatsoever with regard to these or other ISACA publications assuring candidates' passage of the ISACA exam.

Reservation of Rights

© 2024 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA.

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Support: support.isaca.org
Website: www.isaca.org

Participate in the ISACA Online Forums: https://engage.isaca.org/onlineforums
X: www.x.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
Facebook: www.facebook.com/ISACAGlobal
Instagram: www.instagram.com/isacanews/

ISBN 978-1-60420-981-5
CISA® Official Review Manual 28th Edition

Purpose of the CISA Official Review Manual 28th Edition

ISACA is pleased to offer the 28th edition of the *CISA® Official Review Manual*. The purpose of this manual is to provide Certified Information Systems Auditor (CISA) candidates with the technical information and reference material to assist them in preparation for the Certified Information Systems Auditor exam.

The content in this manual is based on the CISA Job Practice, available at *https://www.isaca.org/credentialing/cisa/cisa-exam-content-outline*. **This job practice is the basis for the CISA exam**. The development of the job practice involves thousands of CISA-certified individuals and other industry professionals worldwide who serve as committee members, focus group participants, subject matter experts and survey respondents.

The *CISA® Official Review Manual* is updated to keep pace with rapid changes in the information systems (IS) audit, control and security professions. As with previous manuals, the 28th edition is the result of contributions from many qualified authorities who have generously volunteered their time and expertise. We respect and appreciate their contributions and hope their efforts provide extensive educational value to *CISA® Official Review Manual* readers.

Certification has positively impacted many careers; the CISA designation is respected and acknowledged by organizations around the world. We wish you success with the CISA exam. Your commitment to pursuing the leading certification in IS audit, assurance, control and security is exemplary.

©ISACA. All Rights Reserved.

Page intentionally left blank

Acknowledgments

The 28th edition of the *CISA® Official Review Manual* is the result of the collective efforts of many volunteers. ISACA members from throughout the global IS audit, control and security professions participated, generously offering their talent and expertise. This international team exhibited a spirit and selflessness that have become the hallmark of contributors to this manual. Their participation and insight are truly appreciated.

Authors
Elastos Chimwanda, CISA, CISSP, CCSP, CIA, ISO/IEC 27001 Lead Auditor, Zimbabwe
Toby DeRoche, CISA, CAAP, CCSA, CFE, CIA, CICA, CRMS, SA, USA
Kyle Miller, CISA, CDPSE, CISSP, QSA, USA

Expert Reviewers
Sanjiv Kumar Agarwala, CISA, CISM, CGEIT, CDPSE, CISSP, FBCI, India
Akinwale Akindiya, CISA, Nigeria
Mohammed Alfehaid, CISA, CISM, CRISC, Saudi Arabia
Ibrahim Sulaiman Alnamlah, CISA, Saudi Arabia
Osman Azab, CISA, CISM, CGEIT, CRISC, Egypt
Sunil Bakshi, CISA, CISM, CGEIT, CRISC, CDPSE, CISSP, AMIIB, MCA, India
Zsolt Bederna, CISA, CISM, CGEIT, CRISC, CISSP, C|EH, ISO 27001 Lead Auditor, ITIL-F, Hungary
Walid Bouzouita, CISA, CRISC, CDPSE, CIA, CET, ITIL, PRINCE2 Practitioner, ISO 9001, ISO 20000, ISO 21001, ISO 27001, ISO 27002, ISO 31000, ISO 37301, Tunisia
Meng Fai Chan, CISA, CDPSE, CISSP, GRID, Singapore
Marvel Ruvimbo Chigama, CISA, CISM, CISSP, CEH, ITIL v3 Foundation, UK
Wole Davis, CISA, CFE, Nigeria
Darlene Dawson, CISA, CRISC, USA
Ninad Dhavase, CISA, Australia
Dr Marco Ermini, PhD, CISA, CISM, CRISC, CDPSE, AWS-CCP, AWS-CSAA, AWS-CSS, CCISO, CISSP, GCIH, ISO/IEC 27001 Lead Auditor, Germany
Katja Feldtmann, CISA, CISM, CRISC, CDPSE, CISSP, CCSP, New Zealand
Sandra Fonseca, CISA, CISM, CRISC, CDPSE, USA
Shigeto Fukuda, CISA, CDPSE, Japan
Mohamed Ahmed Gohar, CISA, CISM, CGEIT, CRISC, CISSP, App Sec LI, AXELOS Resilia Practitioner, CCC-BDF, CCC-CTA, CCC-IOTF, CEH, CLPTP, CPDE, CSSGB, DASA-DevOps, ISO/IEC 20000 LI/LA, ISO/IEC 24762 LITDRM, ISO/IEC 27001 LI/LA, ISO/IEC 27002 LM, ISO/IEC 27005 LRM, ISO/IEC 27032 LCM, ISO/IEC 27034, ISO/IEC 27035 LIM, ISO/IEC 38500 LITCGM, ISO 21500 LPM, ISO 22301 LI/LA, ISO 31000 LRM, ISO 37301 LI, ITIL v3 Expert, ITIL v3 Practitioner, ITIL v4 MP, PECB CLCSM, PMP, TOGAF 9/10, Egypt

©ISACA. All Rights Reserved.

Acknowledgments *(cont.)*

Danny Ha, PhD, CISA, CISM, CGEIT, CRISC, CDPSE, Certified Art-Tech-AI-NFT-Art Crime Sotheby London, Certified CISL Cambridge Sustainability UK, Certified Fintech Oxford UK, CISSP, CSSLP, CME, CRT, ESG Assurance Audit, FCP-ERM, FCRP, Honourable ISO-TC Committee Member, Honourable Judge (AI/Metaverse) University of Hong Kong, ISO 31000/9001/45001/14001/27001 LI/LA, ITIL-Expert, MIT-AI, PMP, UK
Mathew Holdt, CISA, CFE, CIA, USA
Miroslav Rósenov Ivanov, CISA, Norway
Leighton Johnson III, CISA, CISM, CGEIT, CRISC, CDPSE, CISSP-ISSEP, CET, CMMC CCA, USA
Joseph Johnston, CISA, CISM, USA
Muhammad Abul Kalam Azad, CISA, CISM, CRISC, CDPSE, CISSP, Bangladesh
Rajul Kambli, CISA, CMA, USA
Ramaswami Karunanithi, CISM, CGEIT, CRISC, CA (Australia & India), CAMS, CBCI, CCSK, CCSP, CFE, CFSA, CGAP, CGMA (USA), CHFI, CIA, CIPP/E, CISSP, CMA (India & USA), CPA (Australia & USA), CPRM, CSCA, CSFX, CRMA, FCS, GRCA, GRCP, Lead Auditor ISO 27001, PBA, PMP, PRINCE2 Practitioner, RMP, Australia
Omar Khan, CISA, Italy
Irene Kopaliani, PhD, CISA, CISM, CDPSE, CISSP, CCSP, USA
Steven Sim Kok Leong, CISA, CISM, CGEIT, CRISC, CDPSE, Singapore
Hubertus Jeroen Kroon, CISA, CISM, CGEIT, CRISC, CDPSE, CISSP, CC, CCAK, CCSP, CCSK, ITIL, Lead Auditor ISO 27001, LI ISO 27001, the Netherlands
Shruti Kulkarni, CISA, CRISC, CISSP, CCSK, ITIL v3, UK
Ashok Kumar DL, CISA, CISM, CDPSE, CFE, CIA, CISSP, CRMA, India
Luong Trung Thanh, CISA, CISM, CGEIT, CDPSE, Vietnam
Michael Malcolm, CISA, CCSK, CIA, CISSP, CSSBB, Canada
A. T. Manjunath, CISA, India
Larry Marks, CISA, CISM, CGEIT, CRISC, CDPSE, CISSP, CCSK, PMP, USA
Shobhit Mehta, CISA, CISM, CGEIT, CRISC, CISSP, CCSP, HITRUST CCSFP, ISO 27001 Lead Auditor, USA
Christine Lilian Mukhongo, CISA, CISM, CGEIT, CRISC, Kenya
Geetha Murugesan, CISA, CGEIT, CRISC, CDPSE, COBIT 5 Certified Assessor, CSA Star, ISO 22301:2019, ISO 27001:2013, ISO 31000:2018, ISO 9000:2015, India
Nnamdi Nwosu, CISA, CISM, CGEIT, CRISC, CEH, University of the People, USA
Eoin O'Beara, CISA, CRISC, Ireland
Teju Oyewole, DSc., CISA, CISM, CRISC, CDPSE, C|CISO, CCSP, CISSP, PMP, ISO 27001, Canada
Tafadzwa Padare, CISA, CISM, CRISC, CISSP, CEH, Ireland
Kanupriya Parab, CISA, CISM, CRISC, CDPSE, Canada
Upesh Parekh, CISA, CRISC, India
Vaibhav Patkar, CISA, CISM, CGEIT, CRISC, CDPSE, CISSP, CCSK, India
Mark Pearce, CISA, CISM, CGEIT, CRISC, CDPSE, CIIP, CIPM, GCLD, GSLC, UK
Varun Prasad, CISA, CISM, USA
Robert Prince, CISA, CISSP, USA
Tabish Qureshi, CISA, CISM, CASP+, CEH v11, ITIL, MCS, MCSA, MCSE, Microsoft Azure Solutions Architect Expert, PMP, PRINCE2 Foundation and Practitioner, SAP Activate Project Manager, Saudi Arabia
Sree Krishna Rao, CISA, UK
Sampa David Sampa, CISA, IGP, Zambia

Acknowledgments *(cont.)*

Chandrasekhar Sarma Garimella, CISA, CISM, CRISC, CDPSE, AWS SA, CCNA, CFE, COSO ERM, ISO 27001 Lead Auditor, ISO 9001 Lead Auditor, India
Srinivasan Shamarao, CISA, CISM, CGEIT, CRISC, CDPSE, ACA, CIA, CIPP/E (IAPP), CIPM (IAPP), India
Vivek Silla, CISA, CISM, CRISC, CISSP, CEH, CHFI, CICA, CIPM, SCF, ISO 20000-1 Lead Auditor, ISO 27001 Lead Auditor, ITIL Foundation, Saudi Arabia
Fadi Sodah, CISA, CISM, Jordan
Katalin Szenes, PhD, CISA, CISM, CGEIT, CISSP, University of Óbuda, John von Neumann Faculty of Informatics, Hungary
Rajesh T. R., CISA, CISM, CRISC, CDPSE, AWS Certified Security Specialist, CCSK, CEH, Certified Cyber Crime Intervention Officer, Google Certified Cloud Security Engineer, ITIL, ISO 27001 Lead Auditor, ISO 31000 Lead Auditor, Microsoft Azure Solutions Architect Expert, PMI-ACP, TISAX, TOGAF9, Zero Trust Certified Architect (ZTCA), India
Satyajit Turumella, CISA, CDPSE, Kenya
Marilize Van Schalkwyk, CISA, CISM, CIA, CRMA, Namibia
Brian Vasquez, CISA, CEH, CISSP, CySA+, GCIH, GSLC, GSTRT, Security+, USA
James Wallmuller, CISA, CRISC, CDPSE, CSX, USA
Ross Wescott, CISA, CIA, CUERME, USA
Prometheus Yang, CISA, CISM, CRISC, Taiwan

©ISACA. All Rights Reserved.

New—CISA Job Practice

Beginning in 2024, the Certified Information Systems Auditor (CISA) exam tests the new CISA job practice.

An international job practice analysis is conducted periodically to maintain the validity of the CISA certification program. A new job practice forms the basis of the CISA exam.

The primary focus of the job practice is on the current tasks performed and the knowledge used by CISAs. By gathering evidence of the current work practice of CISAs, ISACA ensures that the CISA program continues to meet the high standards for the certification of professionals throughout the world.

The findings of the CISA job practice analysis are carefully considered and directly influence the development of new test specifications to ensure that the CISA exam reflects the most current best practices.

The new job practice reflects the areas of study to be tested and is compared below to the previous job practice. The complete CISA job practice is available at *https://www.isaca.org/credentialing/cisa/cisa-exam-content-outline*.

Previous CISA Job Practice	New CISA Job Practice
Domain 1: Information System Auditing Process (21%)	Domain 1: Information System Auditing Process (18%)
Domain 2: Governance and Management of IT (17%)	Domain 2: Governance and Management of IT (18%)
Domain 3: Information Systems Acquisition, Development and Implementation (12%)	Domain 3: Information Systems Acquisition, Development and Implementation (12%)
Domain 4: Information Systems Operations and Business Resilience (23%)	Domain 4: Information Systems Operations and Business Resilience (26%)
Domain 5: Protection of Information Assets (27%)	Domain 5: Protection of Information Assets (26%)

TABLE OF CONTENTS

About This Manual 19
Overview 19
Format of This Manual 19
Preparing for the CISA Exam 19
Getting Started 20
Using the CISA Official Review Manual 20
Features in the Review Manual 20
Types of Questions on the CISA Exam 20
Preparing for the Exam 21
Using ISACA Exam Preparation Resources 21
About the CISA Official Questions, Answers & Explanations Database 21

Chapter 1

Information System Auditing Process 23
Overview 24
Domain 1 Exam Content Outline 24
Learning Objectives/Task Statements 24
Suggested Resources for Further Study 24
Self-Assessment Questions 24
Chapter 1 Answer Key 28
Part A: Planning 31
1.1 IS Audit Standards, Guidelines, Functions and Codes of Ethics 31
1.1.1 ISACA IS Audit and Assurance Standards 31
1.1.2 ISACA IS Audit and Assurance Guidelines 32
1.1.3 ISACA Code of Professional Ethics 32
1.1.4 ITAF TM 33
1.1.5 IS Internal Audit Function 33
Audit Charter 33
Management of the IS Audit Function 33
IS Audit Resource Management 33
Using the Services of Other Auditors and Experts 34
1.2 Types of Audits, Assessments and Reviews 34
1.2.1 Control Self-Assessment 36
Objectives of CSA 36
Benefits of CSA 36
Disadvantages of CSA 36
The IS Auditor's Role in CSA 36
1.2.2 Integrated Auditing 37
1.3 Risk-Based Audit Planning 38
1.3.1 Individual Audit Assignments 38
1.3.2 Effect of Laws and Regulations on IS Audit Planning 39
1.3.3 Audit Risk and Materiality 41
1.3.4 Risk Assessment 42

©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

1.3.5 IS Audit Risk Assessment Techniques....42
1.3.6 Risk Analysis....43
1.4 Types of Controls and Considerations....43
1.4.1 Internal Controls....43
1.4.2 Control Objectives and Control Measures....43
IS Control Objectives....44
General Control Methods....44
IS-Specific Controls....45
Business Process Applications and Controls....45
1.4.3 Control Classifications....47
1.4.4 Control Relationship to Risk....49
1.4.5 Prescriptive Controls and Frameworks....50
1.4.6 Evaluation of the Control Environment....50
Management Control Monitoring....50
Independent Evaluation of the Control Environment....51
Part B: Execution....53
1.5 Audit Project Management....53
1.5.1 Audit Objectives....53
1.5.2 Audit Phases....53
Planning....54
Fieldwork/Documentation....55
Reporting/Follow Up....56
1.5.3 Audit Programs....56
Minimum Skills to Develop an Audit Program....57
1.5.4 Audit Work Papers....57
1.5.5 Fraud, Irregularities and Illegal Acts....57
1.5.6 Agile Auditing....58
Agile Auditing Overview....58
Benefits of Agile Auditing....58
Agile Auditing Compared to Established Assurance Standards....59
1.6 Audit Testing and Sampling Methodology....60
1.6.1 Compliance Versus Substantive Testing....60
1.6.2 Sampling....61
Sampling Risk....63
1.7 Audit Evidence Collection Techniques....63
1.7.1 Interviewing and Observing Personnel in Performance of Their Duties....65
1.8 Audit Data Analytics....66
1.8.1 Computer-Assisted Audit Techniques....67
CAATs as a Continuous Online Audit Approach....68
1.8.2 Continuous Auditing and Monitoring....68
1.8.3 Continuous Auditing Techniques....69
1.8.4 Artificial Intelligence in IS Audit....70
Audit Algorithms....71
Interpretation of AI/ML Results....72
AI/ML Audit Risk and Considerations....73
1.9 Reporting and Communication Techniques....73
1.9.1 Communicating Audit Results....73
1.9.2 Audit Report Objectives....74
1.9.3 Audit Report Structure and Contents....74

 ©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

1.9.4 Audit Documentation....75
1.9.5 Follow-Up Activities....76
1.9.6 Types of IS Audit Reports....76
1.10 Quality Assurance and Improvement of the Audit Process....77
1.10.1 Audit Committee Oversight....77
1.10.2 Audit Quality Assurance....77
1.10.3 Audit Team Training and Development....77
1.10.4 Monitoring....77
Case Study....79
Case Study....79
Chapter 1 Answer Key....82

Chapter 2

Governance and Management of IT....85
Overview....86
Domain 2 Exam Content Outline....86
Learning Objectives/Task Statements....86
Suggested Resources for Further Study....87
Self-Assessment Questions....87
Chapter 2 Answer Key....90
Part A: IT Governance....93
2.1 Laws, Regulations and Industry Standards....93
2.1.1 Impact of Laws, Regulations and Industry Standards on IS Audit....93
2.1.2 Governance, Risk and Compliance....94
2.2 Organizational Structure, IT Governance and IT Strategy....95
2.2.1 Enterprise Governance of Information and Technology....96
2.2.2 Good Practices for EGIT....96
2.2.3 Audit's Role in EGIT....97
Three Lines Model....97
2.2.4 Information Security Governance....99
Effective Information Security Governance....99
2.2.5 Information Systems Strategy....100
2.2.6 Strategic Planning....100
2.2.7 Business Intelligence....101
2.2.8 Organizational Structure....105
IT Governing Committees....105
Roles and Responsibilities of Senior Management and Boards of Directors....106
Matrix of Outcomes and Responsibilities....107
IT Organizational Structure and Responsibilities....109
Data Ownership....109
IT Roles and Responsibilities....110
Vendor and Outsourcer Management....111
Network Management....113
Separation of Duties Within IT....114
Separation of Duties Controls....116
Compensating Controls for Lack of Separation of Duties....116

©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

2.2.9 Auditing IT Governance Structure and Implementation....117
Reviewing Documentation....117
2.3 IT Policies, Standards, Procedures and Guidelines....117
2.3.1 Policies....117
Information Security Policy....118
Review of the Information Security Policy....119
2.3.2 Standards....120
2.3.3 Procedures....120
2.3.4 Guidelines....120
2.4 Enterprise Architecture and Considerations....121
2.5 Enterprise Risk Management....122
2.5.1 Developing a Risk Management Program....123
2.5.2 Risk Management Life Cycle....123
Step 1: IT Risk Identification....124
Step 2: IT Risk Assessment....124
Step 3: Risk Response and Mitigation....125
Step 4: Risk and Control Monitoring and Reporting....126
2.5.3 Risk Analysis Methods....126
Qualitative Analysis Methods....126
Semiquantitative Analysis Methods....126
Quantitative Analysis Methods....126
2.6 Data Privacy Program and Principles....127
2.6.1 Privacy Documentation....128
Types of Documentation....128
2.6.2 Audit Process....130
2.7 Data Governance and Classification....131
2.7.1 Data Inventory and Classification....132
2.7.2 Legal Purpose, Consent and Legitimate Interest....132
Legal Purpose....133
Consent....133
Legitimate Interest....133
2.7.3 Data Subject Rights....134
Transborder Data Flow....135
Part B: IT Management....137
2.8 IT Resource Management....137
2.8.1 Value of IT....137
2.8.2 Implementing IT Portfolio Management....137
2.8.3 IT Management Practices....137
2.8.4 Human Resource Management....138
Recruiting and Hiring....138
Employee Handbook....138
Training....138
Scheduling and Time Reporting....139
Terms and Conditions of Employment....139
Expectations During Employment....139
Employee Performance Management....139
Disciplinary Actions....140
Promotion Policies....140
Required Vacations....140

 ©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

Retention and Succession Plans 140
Termination Policies 140
2.8.5 Enterprise Change Management 141
2.8.6 Financial Management Practices 141
Cost Allocation 141
IS Budgets 141
Software Expenses versus Capitalization 141
2.8.7 Information Security Management 142
2.9 IT Vendor Management 143
2.9.1 Sourcing Practices 143
2.9.2 Outsourcing Practices and Strategies 144
Industry Standards/Benchmarking 146
Globalization Practices and Strategies 146
Outsourcing and Third-Party Audit Reports 147
2.9.3 Cloud Governance 147
2.9.4 Governance in Outsourcing 148
2.9.5 Capacity and Growth Planning 149
2.9.6 Third-Party Service Delivery Management 149
Monitoring and Review of Third-Party Services 149
Managing Changes to Third-Party Services 149
Service Improvement and User Satisfaction 150
2.10 IT Performance Monitoring and Reporting 150
2.10.1 Key Performance Indicators 150
2.10.2 Key Risk Indicators 151
2.10.3 Key Control Indicators 151
2.10.4 Performance Optimization 151
Critical Success Factors 151
Methodologies and Tools 152
2.10.5 Approaches and Techniques 153
Six Sigma 153
Business Agility/Agile Methodology 153
IT Balanced Scorecard 153
IT Portfolio Management Versus Balanced Scorecard 154
Additional Approaches for Performance Measurement 155
2.11 Quality Assurance and Quality Management of IT 155
2.11.1 Quality Assurance 155
2.11.2 Quality Management 156
2.11.3 Operational Excellence 156
Case Study 157
Case Study 157
Chapter 2 Answer Key 160

Chapter 3

Information Systems Acquisition, Development and Implementation 161
Overview 162
Domain 3 Exam Content Outline 162

©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

Learning Objectives/Task Statements....162
Suggested Resources for Further Study....162
Self-Assessment Questions....162
Chapter 3 Answer Key....166
Part A: Information Systems Acquisition and Development....169
3.1 Project Governance and Management....169
3.1.1 Project Management Practices....169
3.1.2 Project Management Structure....170
3.1.3 Project Management Roles and Responsibilities....171
3.1.4 Project Management Techniques....173
3.1.5 Portfolio/Program Management....174
3.1.6 Project Management Office....174
Project Portfolio Database....175
3.1.7 Project Benefits Realization....175
3.1.8 Project Initiation....176
3.1.9 Project Objectives....176
3.1.10 Project Planning....178
Information System Development Project Cost Estimation....178
Software Size Estimation....178
Function Point Analysis....179
Cost Budgets....180
Software Cost Estimation....180
Scheduling and Establishing the Time Frame....180
Gantt Charts....180
3.1.11 Project Execution....182
3.1.12 Project Controlling and Monitoring....183
Management of Scope Changes....183
Management of Resource Usage....183
Management of Risk....183
3.1.13 Project Closing....183
3.1.14 IS Auditor's Role in Project Management....184
3.2 Business Case and Feasibility Analysis....184
3.2.1 IS Auditor's Role in Business Case Development....185
3.3 System Development Methodologies....186
3.3.1 Business Application Development....186
3.3.2 SDLC Models....186
3.3.3 SDLC Phases....189
Phase 1—Feasibility Study....190
Phase 2—Requirements Definition....191
Phase 3A—Software Selection and Acquisition....192
Phase 3B—Design....192
Phase 4A—Configuration....195
Phase 4B—Development....196
Phase 5—Final Testing and Implementation....197
Phase 6—Postimplementation Review....198
3.3.4 IS Auditor's Role in SDLC Project Management....198
3.3.5 Software Development Methods....198
Prototyping/Evolutionary Development....198
Rapid Application Development....199

 ©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

Agile Development....200
Object-Oriented System Development....200
Component-Based Development....201
Web-Based Application Development....202
Software Reengineering....203
Reverse Engineering....203
DevOps and DevSecOps....203
Business Process Reengineering and Process Change....204
3.3.6 System Development Tools and Productivity Aids....205
Computer-Aided Software Engineering....205
Code Generators....206
Fourth-Generation Languages....206
3.3.7 Infrastructure Development/Acquisition Practices....207
Project Phases of Physical Architecture Analysis....208
Planning Implementation of Infrastructure....209
3.3.8 Hardware/Software Acquisition....211
Acquisition Steps....212
3.3.9 System Software Acquisition....213
IS Auditor's Role in Software Acquisition....216
3.4 Control Identification and Design....216
3.4.1 Application Controls....216
Input/Origination Controls....216
Processing Procedures and Controls....218
3.4.2 Output Controls....222
Part B: Information Systems Implementation....225
3.5 System Readiness and Implementation Testing....225
3.5.1 Testing Classifications....225
Other Types of Testing....227
3.5.2 Software Testing....227
3.5.3 Data Integrity Testing....228
Data Integrity in Online Transaction Processing Systems....228
3.5.4 Application Systems Testing....228
Automated Application Testing....230
IS Auditor's Role in Information Systems Testing....230
3.5.5 System Implementation....231
Implementation Planning....231
3.6 Implementation Configuration and Release Management....232
3.6.1 Configuration Management Systems....232
3.7 System Migration, Infrastructure Deployment and Data Conversion....233
3.7.1 Data Migration....233
Refining the Migration Scenario....234
Fallback (Rollback) Scenario....235
3.7.2 Changeover (Go-Live or Cutover) Techniques....236
Parallel Changeover....236
Phased Changeover....236
Abrupt Changeover....237
3.7.3 System Change Procedures and the Program Migration Process....237
Critical Success Factors....238
End-User Training....238

©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

3.7.4 System Software Implementation....238
3.7.5 Certification/Accreditation....238
3.8 Postimplementation Review....239
3.8.1 IS Auditor's Role in Postimplementation Review....240
Case Study....241
Case Study....241
Chapter 3 Answer Key....244

Chapter 4

Information Systems Operations and Business Resilience....245
Overview....246
Domain 4 Exam Content Outline....246
Learning Objectives/Task Statements....246
Suggested Resources For Further Study....246
Self-Assessment Questions....247
Chapter 4 Answer Key....250
Part A: Information Systems Operations....253
4.1 IT Components....253
4.1.1 Networking....254
Local Area Network....256
Wide Area Network....259
TCP/IP and Its Relation to the OSI Reference Model....260
Network Administration and Control....262
Converged Protocols....264
Internet Protocol Networking....265
Network Address Translation....266
4.1.2 Computer Hardware Components and Architectures....267
Processing Components....267
Input/Output Components....267
Types of Computers....267
4.1.3 Common Enterprise Back-End Devices....269
Proxy Servers....269
4.1.4 USB Mass Storage Devices....270
Risk Related to USB Mass Storage Devices....270
Security Controls Related to USB Mass Storage Devices....271
4.1.5 Wireless Communication Technologies....271
4.1.6 Hardware Maintenance Program....272
Hardware Monitoring Reports and Procedures....272
4.1.7 Hardware Reviews....273
4.2 IT Asset Management....274
4.3 Job Scheduling and Production Process Automation....274
4.3.1 Job Scheduling Software....274
4.3.2 Scheduling Reviews....275
4.4 System Interfaces....276
4.4.1 Risk Associated With System Interfaces....276
4.4.2 Controls Associated With System Interfaces....277

 ©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

4.5 End-User Computing and Shadow IT 277
4.5.1 End-User Computing 278
4.5.2 Shadow IT 278
4.6 Systems Availability and Capacity Management 279
4.6.1 IS Architecture and Software 279
4.6.2 Operating Systems 279
Software Control Features or Parameters 280
Software Integrity Issues 280
Operating System Reviews 281
4.6.3 Access Control Software 282
4.6.4 Data Communications Software 282
4.6.5 Utility Programs 283
4.6.6 Software Licensing Issues 283
4.6.7 Source Code Management 284
4.6.8 Capacity Management 285
4.7 Problem and Incident Management 286
4.7.1 Problem Management 287
4.7.2 Process of Incident Handling 287
4.7.3 Detection, Documentation, Control, Resolution and Reporting of Abnormal Conditions 287
4.7.4 Support/Help Desk 288
4.7.5 Network Management Tools 288
4.7.6 Problem Management Reporting Reviews 289
4.8 IT Change, Configuration and Patch Management 290
4.8.1 Patch Management 290
4.8.2 Release Management 291
4.8.3 IS Operations 292
IS Operations Reviews 292
4.9 Operational Log Management 294
4.9.1 Types of Logs 294
4.9.2 Log Management 295
Data Collection 295
Generating Alerts 296
Storing and Protecting Logs 296
Analyzing Log Data 296
Reporting Concerns 297
Log Management Integration With SIEM and IT Governance 297
4.10 IT Service Level Management 298
4.10.1 Service Level Agreements 298
4.10.2 Monitoring of Service Levels 300
4.10.3 Service Levels and Enterprise Architecture 300
4.11 Database Management 300
4.11.1 DBMS Architecture 301
Detailed DBMS Metadata Architecture 301
4.11.2 Database Structure 301
Hierarchical Database Model 301
Network Database Model 302
Relational Database Model 303
Object-Oriented Database Management System 304

©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

NoSQL....305
4.11.3 Database Controls....305
4.11.4 Database Reviews....306
Part B: Business Resilience....309
4.12 Business Impact Analysis....309
4.12.1 Classification of Operations and Criticality Analysis....311
4.13 System and Operational Resilience....311
4.13.1 Application Resiliency and Disaster Recovery Methods....312
4.13.2 Telecommunication Networks Resiliency and Disaster Recovery Methods. 312
4.14 Data Backup, Storage and Restoration....313
4.14.1 Data Storage Resiliency and Disaster Recovery Methods....313
4.14.2 Backup and Restoration....314
Offsite Library Controls....314
Cloud Backup....315
Security and Control of Offsite Facilities....315
Media and Documentation Backup....315
Types of Backup Devices and Media....315
Periodic Backup Procedures....316
Frequency of Rotation....317
Types of Media and Documentation Rotated....317
4.14.3 Backup Schemes....318
Full Backup....318
Incremental Backup....318
Differential Backup....318
Method of Rotation....318
Record Keeping for Offsite Storage....319
3-2-1 Backup Strategy....320
4.15 Business Continuity Plan....320
4.15.1 IT Business Continuity Planning....320
4.15.2 Disasters and Other Disruptive Events....322
Pandemic Planning....322
Dealing With Damage to Image, Reputation or Brand....322
Unanticipated/Unforeseeable Events....323
4.15.3 Business Continuity Planning Process....323
4.15.4 Business Continuity Policy....324
4.15.5 Business Continuity Planning Incident Management....324
4.15.6 Development of Business Continuity Plans....326
4.15.7 Other Issues in Plan Development....326
4.15.8 Components of a Business Continuity Plan....326
Key Decision-Making Personnel....328
Backup of Required Supplies....328
Insurance....329
4.15.9 Plan Testing....329
Specifications....330
Test Execution....330
Documentation of Results....330
Results Analysis....330
Plan Maintenance....331
4.15.10 Business Continuity Management Good Practices....331

 ©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

4.15.11 Auditing Business Continuity 332
Reviewing the Business Continuity Plan 332
Evaluation of Offsite Storage 334
Interviewing Key Personnel 334
Reviewing the Alternative Processing Contract 334
Reviewing Insurance Coverage 334
4.16 Disaster Recovery Plans 335
4.16.1 Recovery Point Objective, Recovery Time Objective and Mean Time to Repair 335
4.16.2 Recovery Strategies 336
4.16.3 Recovery Alternatives 337
Contractual Provisions 338
Procuring Alternative Hardware 339
4.16.4 Development of Disaster Recovery Plans 339
IT DRP Contents 340
IT DRP Scenarios 340
Recovery Procedures 340
Organization and Assignment of Responsibilities 340
4.16.5 Disaster Recovery Testing Methods 342
Types of Tests 342
Testing 343
Test Results 344
4.16.6 Invoking Disaster Recovery Plans 344
Case Study 345
Case Study 345
Chapter 4 Answer Key 348

Chapter 5

Protection of Information Assets 349
Overview 350
Domain 5 Exam Content Outline 350
Learning Objectives/Task Statements 350
Suggested Resources for Further Study 350
Self-Assessment Questions 351
Chapter 5 Answer Key 354
Part A: Information Asset Security and Control 357
5.1 Information Asset Security Policies, Frameworks, Standards and Guidelines 357
5.1.1 Information Asset Security Policies, Procedures and Guidelines 357
Characteristics of an Information Security Policy 358
Information Security Procedures 359
Information Security Guidelines 359
5.1.2 Information Security Frameworks and Standards 359
5.1.3 Information Security Baselines 362
Access Standards 365

©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

5.2 Physical and Environmental Controls....365
5.2.1 Environmental Exposures and Controls....365
Equipment Issues and Exposures Related to the Environment....365
Controls for Environmental Exposures....366
5.2.2 Physical Access Exposures and Controls....369
Physical Access Exposures....369
Physical Access Controls....370
Auditing Physical Access....371
5.2.3 Industrial Control Systems Security....372
ICS Risk....372
ICS Security Best Practices....373
5.3 Identity and Access Management....373
5.3.1 Identity and Access Management....374
Benefits of IAM....374
IAM Life Cycle Management....375
IAM Best Practices....375
5.3.2 Authentication, Authorization and Accountability....379
Authentication....379
Authorization....381
Accountability....382
5.3.3 Zero-Trust Architecture....382
ZTA Best Practices....383
Implementing IAM Using ZTA....383
5.3.4 Privileged Access Management....384
PAM Risk....384
PAM Best Practices....385
5.3.5 Directory Services....385
5.3.6 Identity Governance and Administration....386
Elements of IGA....386
5.3.7 Identity as a Service....387
Benefits of IDaaS....387
Risk of IDaaS....388
IDaaS Best Practices....388
5.3.8 System Access Permission....388
5.3.9 Types of Access Controls....389
5.3.10 Information Security and External Parties....391
Identification of Risk Related to External Parties....391
Addressing Security When Dealing With Customers....392
Addressing Security in Third-Party Agreements....392
5.3.11 Digital Rights Management....394
DRM Restrictions....394
DRM Technologies....395
Best Practices for DRM....396
5.3.12 Logical Access....396
Logical Access Exposures....396
Familiarization With the Enterprise's IT Environment....396
Paths of Logical Access....397
General Points of Entry....397
5.3.13 Access Control Software....397

 ©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

5.3.14 Logon IDs and Passwords....398
Features of Passwords....398
Password Attacks....399
Login ID and Password Good Practices....400
5.3.15 Remote Access Security....401
Remote Access Risk....401
5.3.16 Biometrics....401
Management of Biometrics....401
Biometric Performance Metrics....402
Physically Oriented Biometrics....403
Behavior-Oriented Biometrics....403
Biometric Audit Considerations....404
5.3.17 Naming Conventions for Logical Access Controls....404
5.3.18 Federated Identity Management....405
FIM Technologies....406
Benefits of FIM....407
Limitations of FIM....407
FIM Versus SSO....408
5.3.19 Auditing Logical Access....408
Familiarization With the IT Environment....408
Assessing and Documenting the Access Paths....408
Interviewing Systems Personnel....409
Reviewing Reports From Access Control Software....409
Reviewing Application Systems Operations Manual....409
5.4 Network and Endpoint Security....409
5.4.1 IS Network Infrastructure....409
5.4.2 Enterprise Network Architectures....410
5.4.3 Types of Networks....410
5.4.4 Network Services....411
5.4.5 Network Standards and Protocols....412
5.4.6 Virtual Private Networks....412
VPN Protocols....413
VPN Best Practices....414
5.4.7 Network Attached Storage....415
5.4.8 Content Delivery Networks....416
Benefits of CDNs....416
CDN Security Risk....417
CDN Security Best Practices....417
5.4.9 Network Time Protocol....417
NTP Risk....418
Best Practices for Using NTP....419
5.4.10 Applications in a Networked Environment....419
Client-Server Technology....419
Client-Server Security....420
Middleware....421
On-Demand Computing....421
5.4.11 Network Infrastructure Security....421
Internet Security Controls....422

©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

5.4.12 Firewalls....423
Firewall General Features....423
Firewall Types....423
Next Generation Firewalls....425
Web Application Firewall....426
Examples of Firewall Implementations....428
Firewall Issues....428
Firewall Platforms....428
5.4.13 Unified Threat Management (UTM)....429
Benefits of Using a UTM....430
5.4.14 Network Segmentation....430
Methods of Network Segmentation....430
Benefits of Network Segmentation....431
Network Segmentation Best Practices....431
5.4.15 Endpoint Security....432
Endpoint Detection and Response....432
Extended Detection and Response....433
5.5 Data Loss Prevention....434
5.5.1 Types of DLPs....434
5.5.2 Data Loss Risk....435
5.5.3 DLP Solutions and Data States....437
Data at Rest....437
Data in Transit....437
Data in Use....437
5.5.4 DLP Controls....437
5.5.5 DLP Content Analysis Methods....438
5.5.6 DLP Deployment Best Practices....438
5.5.7 DLP Risk, Limitations and Considerations....439
5.6 Data Encryption....440
5.6.1 Elements of Encryption Systems....440
5.6.2 Link Encryption and End-to-End Encryption....442
5.6.3 Symmetric Key Cryptographic Systems....443
5.6.4 Public (Asymmetric) Key Cryptographic Systems....443
5.6.5 Elliptic Curve Cryptography....444
5.6.6 Quantum Cryptography....445
5.6.7 Homomorphic Encryption....445
Types of Homomorphic Encryption....446
Challenges With Homomorphic Encryption....446
5.6.8 Digital Signatures....446
5.6.9 Digital Envelope....447
5.6.10 Applications of Cryptographic Systems....447
Transport Layer Security....448
IP Security....448
Security Association....449
5.6.11 Kerberos....449
5.6.12 Secure Shell....450
SSH Key Security Best Practices....450
5.6.13 Domain Name System Security Extensions....451

 ©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

5.6.14 Email Security....451
Common Email Attacks and Techniques....451
Email Security Controls....453
5.6.15 Encryption Audit Procedures....453
5.7 Public Key Infrastructure....454
5.7.1 Digital Certificates....454
5.7.2 Key Management....455
5.7.3 Certificate Revocation....455
5.7.4 Certificate Revocation List....456
Online Certificate Status Protocol....456
5.7.5 PKI Infrastructure Risk....457
5.7.6 Audit Procedures for PKI....457
5.8 Cloud and Virtualized Environments....459
5.8.1 Virtualization....459
Typical Controls....461
5.8.2 Virtual Circuits....462
5.8.3 Virtual Local Area Network....462
5.8.4 Virtual Storage Area Networks....463
Benefits of VSAN....463
5.8.5 Software-Defined Networking....464
The Advantages of SDN....464
The Disadvantages of SDN....465
SDN Attacks and Vulnerabilities....465
SDN Deployment Best Practices....466
5.8.6 Containerization....466
Best Practices for Container Security....468
5.8.7 Secure Cloud Migration....469
Cloud Migration Security Risk....469
5.8.8 The Shared Responsibility Model....471
Cloud Deployment Models....471
Cloud Service Models....472
SRM Best Practices....473
5.8.9 Key Risk in Cloud Environments....473
5.8.10 DevSecOps....474
DevSecOps Benefits....475
DevSecOps Best Practices....475
5.9 Mobile, Wireless and Internet of Things Devices....475
5.9.1 Mobile Computing....476
5.9.2 Mobile Device Threats....476
5.9.3 Mobile Device Controls....477
5.9.4 Mobile Device Management....478
Best Practices for MDM....479
5.9.5 Bring Your Own Device....479
5.9.6 Internet Access on Mobile Devices....480
5.9.7 Audit Procedures for Mobile Devices....481
5.9.8 Mobile Payment Systems....482
Mobile Payment Threats....483
Mobile Payment Systems Security Best Practices....484

©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

5.9.9 Wireless Networks 484
Wireless Wide Area Networks 485
Wireless Local Area Networks 485
WEP and Wi-Fi Protected Access 485
Wireless Personal Area Networks 486
Ad Hoc Networks 486
Wireless Security Threats and Risk Mitigation 487
Wireless Secure Encryption Protocols 488
Auditing Procedures for Wireless Networks 489
5.9.10 Internet of Things 490
IoT Risk 491
IoT Security Controls 491
Part B: Security Event Management 493
5.10 Security Awareness Training and Programs 493
5.10.1 The Information Security Learning Continuum 493
5.10.2 Benefits of a Security Awareness, Training and Education Program 494
5.10.3 Approach to Security Awareness, Training and Education 494
5.10.4 Conditions for a Successful Security Awareness Training and Education Program 495
5.10.5 Conducting a Needs Assessment 495
Information Sources for Needs Assessment 496
5.10.6 Implementing an Awareness and Training Program 496
5.11 Information System Attack Methods and Techniques 498
5.11.1 Fraud Risk Factors 498
5.11.2 Computer Crime Issues and Exposures 498
5.11.3 Internet Threats and Security 507
Network Security Threats 507
Passive Attacks 507
Active Attacks 508
Causal Factors for Internet Attacks 508
Targeted Attacks 508
The OWASP Top 10 508
5.11.4 Malware 508
Virus and Worm Controls 509
Management Procedural Controls 509
Technical Controls 509
Antimalware Software Implementation Strategies 510
5.11.5 Ransomware 511
Mitigating Active Ransomware Infections 512
Ethical Considerations for Ransomware 513
5.12 Security Testing Tools and Techniques 513
5.12.1 Objectives of Security Testing 513
5.12.2 Security Assessments and Security Audits 514
5.12.3 Vulnerability Assessments 514
5.12.4 Penetration Tests 514
Phases of Penetration testing 515
Vulnerability Assessments Versus Penetration Testing 518
Penetration Testing Versus Ethical Hacking 519
5.12.5 Threat Readiness/Information Security Teams 519

 ©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

5.12.6 Security Testing Techniques....520
5.12.7 Security Operations Center....520
Full Network Assessment Reviews....521
5.12.8 Security Testing Audit Procedures....522
Terminal Identification....522
Terminal Cards and Keys....522
Logon IDs and Passwords....522
Controls Over Production Resources....523
Logging and Reporting of Computer Access Violations....523
Follow-Up Access Violations....523
Bypassing Security and Compensating Controls....523
5.13 Security Monitoring Logs, Tools and Techniques....524
5.13.1 Information Security Monitoring....524
5.13.2 Intrusion Detection Systems....524
Features....525
Limitations....525
Policy....525
5.13.3 Intrusion Prevention Systems....525
Honeypots and Honeynets....526
Best Practices for IDS/IPS Implementation....527
5.13.4 Audit Logging in Monitoring System Access....527
Access Rights to System Logs....527
Tools for Audit Trail (Logs) Analysis....528
Cost Considerations....528
5.13.5 Protecting Log Data....529
5.13.6 Security Information and Event Management....529
Benefits of SIEM....530
Features of SIEM....531
SIEM Implementation Best Practices....531
5.13.7 Security Monitoring Tools....532
5.14 Security Incident Response Management....532
5.14.1 Incident Response Process....532
5.14.2 Computer Security Incident Response Team....534
5.14.3 Incident Response Plan....535
5.14.4 Security Orchestration, Automation and Response....536
Benefits of SOAR....536
5.15 Evidence Collection and Forensics....537
5.15.1 Types of Investigations....537
5.15.2 Types of Computer Forensics....538
5.15.3 Phases of Computer Forensics....539
5.15.4 Audit Considerations....539
Data Protection....539
Data Acquisition....540
Imaging....540
Extraction....540
Interrogation....540
Ingestion/Normalization....540
Reporting....540
5.15.5 Computer Forensic Techniques....540

©ISACA. All Rights Reserved.

TABLE OF CONTENTS *(cont.)*

5.15.6 Computer Forensics Tools....541
5.15.7 Chain of Custody....542
5.15.8 Best Practices to Secure Digital Evidence....542
Case Study....545
Case Study....545
Chapter 5 Answer Key....546

Appendix A

CISA Exam General Information....547
Successful Completion of the CISA Exam....547
Experience in IS Auditing, Control and Security....547
Description of the Exam....547
Registration for the CISA Exam....547
CISA Program Accreditation Renewed Under ISO/IEC 17024:2012....547
Scheduling the Exam....548
Sitting for the Exam....548
Budgeting Your Time....549
Grading the Exam....549

Appendix B

CISA Job Practice....551
Knowledge Areas....551
Information System Auditing Process....551
Governance and Management of IT....551
Information Systems Acquisition, Development and Implementation....552
Information Systems Operations and Business Resilience....552
Protection of Information Assets....552
Secondary Classifications–Tasks....553

Glossary

Glossary....555

Acronyms

Acronyms....571

 ©ISACA. All Rights Reserved.

About This Manual

Overview

The *CISA® Official Review Manual 28th Edition* is intended to assist candidates with preparing for the CISA exam. This manual is one source of preparation for the exam and is not the only source. **It is not a comprehensive collection of all the information and experience that are required to pass the exam.** No single publication offers such coverage and detail. If candidates read through the manual and encounter a topic that is new to them or one in which they feel their knowledge and experience are limited, they should seek additional references. The CISA exam is a combination of questions that test candidates' technical and practical knowledge and their ability to apply their experience-based knowledge in given situations.

The *CISA® Official Review Manual 28th Edition* provides the knowledge and activities for the functions in the CISA job practice content areas and as described in the *ISACA Exam Candidate Information Guide* (*https://www.isaca.org/credentialing/exam-candidate-guides*):

Domain 1	Information System Auditing Process	18 percent
Domain 2	Governance and Management of IT	18 percent
Domain 3	Information Systems Acquisition, Development and Implementation	12 percent
Domain 4	Information Systems Operations and Business Resilience	26 percent
Domain 5	Protection of Information Assets	26 percent

The manual has been developed and organized to assist candidates in their study. CISA candidates should evaluate their strengths, based on knowledge and experience, in each of these areas.

Note

Each chapter reviews the knowledge that CISA candidates are expected to understand to support and accomplish the tasks that they should be able to accomplish for a job practice domain. These tasks constitute the current practices for the IS auditor. The detailed CISA job practice can be viewed at *https://www.isaca.org/credentialing/cisa/cisa-exam-content-outline*. *The* CISA exam is based on this job practice.

Format of This Manual

Each *CISA® Official Review Manual* chapter follows the same format:

- The Overview section provides a summary of the focus of the chapter along with:
  - The domain exam content outline
  - Related task statements
  - Suggested resources for further study
  - Self-assessment questions
- The Content section includes:
  - Content to support the different areas of the job practice
  - Definitions of terms commonly found on the exam

Please note that the manual has been written using standard American English, except where material has been imported from publications written in International English.

Submit suggestions to enhance the review manual or suggested reference materials to *studymaterials@isaca.org*.

Preparing for the CISA Exam

The CISA exam evaluates a candidate's practical knowledge, experiences and application of the job practice domains as described in this Review Manual. We recommend that the exam candidate look to multiple resources to prepare for the exam, including this Review Manual, along with external publications. This section covers some tips for studying for the exam.

©ISACA. All Rights Reserved.

Read to understand the areas that need more knowledge. Then, see reference sources to expand those areas and, also, gain experience in those areas.

Getting Started

Having adequate time to prepare for the CISA exam is critical. Most candidates spend between three and six months studying prior to taking the exam. Set aside a designated time each week to study, and perhaps increase study time as the exam date approaches.

It helps to develop a plan for studying to prepare for the exam.

Using the CISA Official Review Manual

The *CISA® Official Review Manual* is divided into five chapters, each corresponding with a domain in the CISA Job Practice. While the manual does not include every concept that could be tested on the CISA exam, it does cover a breadth of knowledge that provides a solid base for the exam candidate. The manual is one source of preparation for the exam and should not be thought of as the only source nor viewed as a comprehensive collection of all the information and experience required to pass the exam.

Features in the Review Manual

The *CISA® Official Review Manual* includes several features to help you navigate the job practice and enhance your learning and retaining the material.

Review Manual Features	Description
Overview	The Overview provides the context of the domain, including the job practice areas and applicable learning objectives and task statements.
Suggested Resources for Further Study	Refer to external sources to supplement your understanding of the concepts. Use the suggested resources to enhance your study efforts as they relate to each chapter.
Self-Assessment Questions and Answers	The self-assessment questions in each chapter are not intended to measure the candidate's ability to answer questions correctly on the CISA exam for that area. The questions are intended to familiarize the candidate with the question structure and may or may not be similar to questions that appear on the actual examination.
Glossary	A glossary is included at the end of the manual which contains terms that apply to: • The material included in the chapters • To related areas not specifically discussed in the manual Since the glossary is an extension of the text in the manual, it can serve as other areas the candidate may want to seek additional references.
Acronym List	A list of commonly used acronyms related to IS auditing is included to help the candidate understand the material in the chapter as well as concepts covered on the CISA exam.

Types of Questions on the CISA Exam

CISA exam questions are developed with the intent of measuring and testing practical knowledge and the application of IS auditing and assurance principles. All questions are presented in a multiple-choice format and are designed for one best answer.

The candidate is cautioned to read each question carefully. Knowing that these types of questions are asked and how to study to answer them will go a long way toward answering them correctly. The best answer is of the choices provided. There can be many potential solutions to the scenarios posed in the questions, depending on industry, geographical location, etc. It is advisable to consider the information provided in the question and to determine the best answer of the options provided.

Each CISA question has a stem (question) and four options (answer choices). The candidate is asked to

 ©ISACA. All Rights Reserved.

choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement.

A helpful approach to these questions includes the following:

- Read the entire stem and determine what the question is asking. Look for key words such as "BEST," "MOST," "FIRST," etc., and key terms that may indicate what domain or concept that is being tested.
- Read all of the options, and then read the stem again to see if you can eliminate any of the options based on your immediate understanding of the question.
- Re-read the remaining options and bring in any personal experience to determine which is the best answer to the question.

Preparing for the Exam

When preparing for the exam, the candidate should recognize that information security is a global profession, and the candidate's perceptions and experiences may not reflect the more global position. Because the exam and CISA manuals are written for the international information security management community, the candidate must be flexible when reading a condition that may be contrary to the candidate's experience.

Note that the CISA exam questions are written by experienced information security professionals from around the world. Each question on the exam is reviewed by ISACA's CISA Exam Item Development Working Group, which consists of international members. This geographic representation ensures that all exam questions are understood equally in every country and language.

Using ISACA Exam Preparation Resources

The *CISA® Official Review Manual* can be used in conjunction with other CISA exam preparation activities. The following products are based on the CISA job practice, and referenced job practice areas can be used to find related content within the *CISA® Official Review Manual*. These resources include:

- CISA Official Questions, Answers & Explanations Database—12 Month Subscription
- CISA Official Online Review Course
- CISA review courses (provided by local ISACA chapters and accredited training organizations)

About the CISA Official Questions, Answers & Explanations Database

The CISA® Review Questions, Answers & Explanations Database–12 Month Subscription. The online database consists of the 1,000 questions, answers and explanations organized by knowledge areas in the CISA Job Practice. With this product, CISA candidates can quickly identify their strengths and weaknesses by taking random sample exams of varying lengths and breaking the results down by domain. Sample exams also can be chosen by domain, allowing for concentrated study, one domain at a time, and other sorting features, such as the omission of previous correctly answered questions, are available.

The CISA Official Questions, Answers & Explanations Database can be used in conjunction with the *CISA® Official Review Manual 28th Edition* to help candidates prepare for the exam and review topics and areas where they need additional knowledge.

Note

When using the CISA review materials to prepare for the exam, it should be noted that they cover a broad spectrum of IS auditing and assurance topics. **Again, candidates should not assume that reading these manuals and answering review questions will fully prepare them for the examination.** Since actual exam questions often relate to practical experiences, candidates should refer to their own experiences and other reference sources and draw on the experiences of colleagues and others who have earned the CISA designation.

©ISACA. All Rights Reserved.

Page intentionally left blank

 ©ISACA. All Rights Reserved.

Chapter 1

Information System Auditing Process

Overview

Domain 1 Exam Content Outline 24
Learning Objectives/Task Statements 24
Suggested Resources for Further Study 24
Self-Assessment Questions 24
Chapter 1 Answer Key 28

Part A: Planning

1.1 IS Audit Standards, Guidelines, Functions and Codes of Ethics 31
1.2 Types of Audits, Assessments and Reviews 34
1.3 Risk-Based Audit Planning 38
1.4 Types of Controls and Considerations 43

Part B: Execution

1.5 Audit Project Management 53
1.6 Audit Testing and Sampling Methodology 60
1.7 Audit Evidence Collection Techniques 63
1.8 Audit Data Analytics 66
1.9 Reporting and Communication Techniques 73
1.10 Quality Assurance and Improvement of the Audit Process 77

Case Study

Case Study 79
Chapter 1 Answer Key 82

©ISACA. All Rights Reserved.

Overview

The information systems (IS) auditing process encompasses the standards, principles, methods, guidelines, practices and techniques that an IS auditor uses to plan and execute audits of information systems supporting critical business processes.

An IS auditor must have a thorough understanding of this auditing process and of IS processes, business processes and controls designed to achieve organizational objectives.

This domain represents 18 percent of the CISA exam (approximately 27 questions).

Domain 1 Exam Content Outline

Part A: Planning

1. IS Audit Standards, Guidelines, Function and Codes of Ethics
2. Types of Audits, Assessments and Reviews
3. Risk-based Audit Planning
4. Types of Controls

Part B: Execution

1. Audit Project Management
2. Audit Testing and Sampling Methodology
3. Audit Evidence Collection Techniques
4. Audit Data Analytics (including audit algorithms)
5. Reporting and Communication Techniques
6. Quality Assurance and Improvement of Audit Process

Learning Objectives/Task Statements

Within this domain, the IS auditor should be able to:

- Plan an audit to determine whether information systems are protected, controlled and provide value to the organization.
- Conduct audits in accordance with IS audit standards and a risk based IS audit strategy.
- Apply project management methodologies to the audit process.
- Communicate and collect feedback on audit progress, findings, results and recommendations with stakeholders.
- Conduct post-audit follow up to evaluate whether identified risk has been sufficiently addressed.
- Utilize data analytics tools to enhance audit processes.
- Evaluate the role and/or impact of automatization and/or decision-making systems for an organization.
- Evaluate audit processes as part of quality assurance and improvement programs.
- Evaluate the organization's enterprise risk management (ERM) program.
- Evaluate the readiness of information systems for implementation and migration into production.
- Evaluate potential opportunities and risks associated with emerging technologies, regulations and industry practices.

Suggested Resources for Further Study

ISACA Audit Programs and Tools, *https://www.isaca.org/resources/insights-and-expertise/audit-programs-and-tools*

ISACA Frameworks, Standards and Models, *https://www.isaca.org/resources/frameworks-standards-and-models*

ISACA, *IT Audit Framework (ITAF™): A Professional Practices Framework for IT Audit, 4th Edition*, *https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko91EAC*

ISACA IT Audit, *https://www.isaca.org/resources/it-audit*

ISACA White Papers, *https://www.isaca.org/resources/insights-and-expertise/white-papers*

Self-Assessment Questions

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see section About This Manual for more guidance regarding practice questions.

1. Which of the following outlines the overall authority to perform an information systems (IS) audit?

   A. The audit scope with goals and objectives
   B. A request from management to perform an audit
   C. The approved audit charter
   D. The approved audit schedule

 ©ISACA. All Rights Reserved.

2. Which of the following is the key benefit of a control self-assessment (CSA)?

   A. Management ownership of the internal controls supporting business objectives is reinforced.
   B. Audit expenses are reduced when the assessment results are an input to external audit work.
   C. Fraud detection is improved because internal business staff are engaged in testing controls.
   D. Internal auditors can use the results of the assessment to shift to a consultative approach.

3. Which of the following would an information systems (IS) auditor **MOST** likely focus on when developing a risk-based audit program?

   A. Business processes
   B. Administrative controls
   C. Environmental controls
   D. Business strategies

4. Which of the following types of audit risk assumes an absence of compensating controls in the area being reviewed?

   A. Control risk
   B. Detection risk
   C. Inherent risk
   D. Sampling risk

5. An information systems (IS) auditor performing a review of an application's controls finds a weakness in system software that could materially impact the application. In this situation, an IS auditor should:

   A. disregard these control weaknesses because a system software review is beyond the scope of this review.
   B. conduct a detailed system software review and report the control weaknesses.
   C. include a statement in the report that the audit was limited to a review of the application's controls.
   D. review the relevant system software controls and recommend a detailed system software review.

6. Which of the following is the **MOST** important reason for reviewing an audit planning process at periodic intervals?

   A. To plan for deployment of available audit resources
   B. To consider changes to the risk environment
   C. To provide inputs for documentation of the audit charter
   D. To identify the applicable IS audit standards

7. Which of the following is a **KEY** benefit of a control self-assessment (CSA)?

   A. Management ownership of the internal controls supporting business objectives is reinforced.
   B. Audit expenses are reduced when the assessment results are an input to external audit work.
   C. Fraud detection is improved because internal business staff are engaged in testing controls.
   D. Internal auditors can use the results of the assessment to shift to a consultative approach.

8. Which of the following is the **MOST** critical step when planning an information systems (IS) audit?

   A. Review of prior audit findings
   B. Executive management's approval of the audit plan
   C. Review of information security policies and procedures
   D. Performance of a risk assessment

9. The approach an information systems (IS) auditor should use to plan IS audit coverage should be based on:

   A. risk.
   B. materiality.
   C. fraud monitoring.
   D. sufficiency of audit evidence.

©ISACA. All Rights Reserved.

10. An organization performs a daily backup of critical data and software files and stores backup media at an offsite location. The backup media are used to restore the files in case of a disruption. This is an example of a:

    A. preventive control.
    B. management control.
    C. corrective control.
    D. detective control.

Answers on page 28

Page intentionally left blank

©ISACA. All Rights Reserved.

Chapter 1 Answer Key

Self-Assessment Questions

1. A. The audit scope is specific to a single audit and does not grant authority to perform an audit.
   B. A request from management to perform an audit is not sufficient because it relates to a specific audit.
   C. The approved audit charter outlines the auditor's responsibility, authority and accountability.
   D. The approved audit schedule does not grant authority to perform an audit.

2. **A. The objective of control self-assessment (CSA) is to have business managers become more aware of the importance of internal control and their responsibility in terms of corporate governance.**
   B. Reducing audit expenses is not a key benefit of CSA.
   C. Improved fraud detection is important but not as important as control ownership. It is not a principal objective of CSA.
   D. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

3. **A. A risk-based audit approach focuses on understanding the nature of the business and being able to identify and categorize risk. Business risk impacts the long-term viability of a specific business. Thus, an information systems (IS) auditor using a risk-based audit approach must be able to understand business processes.**
   B. Administrative controls, while an important subset of controls, are not the primary focus needed to understand the business processes within the scope of an audit.
   C. Like administrative controls, environmental controls are an important control subset; however, they do not address high-level overarching business processes under review.
   D. Business strategies are the drivers for business processes; however, in this case, an IS auditor is focusing on the business processes that were put in place to enable the organization to implement its strategies.

4. A. Control risk is the risk that a material error exists that will not be prevented or detected in a timely manner by the system of internal controls.
   B. Detection risk is the risk that a material misstatement with a management assertion will not be detected by an audit and assurance professional's substantive tests. It consists of two components: sampling risk and non-sampling risk.
   C. Inherent risk is the risk level or exposure assessed without considering the actions that management has taken or might take.
   D. Sampling risk is the risk that incorrect assumptions are made about the characteristics of a population from which a sample is taken. Non-sampling risk is detection risk that is unrelated to sampling; it can be due to a variety of reasons, including human error.

5. A. An information systems (IS) auditor is not expected to ignore control weaknesses just because they are outside the scope of a current review.
   B. The conduct of a detailed systems software review may hamper the audit's schedule, and an IS auditor may not be technically competent to do such a review at the time of the audit.
   C. If there are control weaknesses that have been discovered by an IS auditor, they should be disclosed. By issuing a disclaimer, this responsibility would be waived.
   D. The appropriate option would be to review the relevant systems software and recommend a detailed systems software review for which additional resources may be recommended.

6. A. Deployment of available audit resources is determined by the audit assignments, which are influenced by the planning process.
   B. Short- and long-term issues that drive audit planning can be heavily impacted by changes to the risk environment, technologies and business processes of the enterprise.
   C. The audit charter reflects the mandate of top management to the audit function and resides at a more abstract level.
   D. Applicability of information systems (IS) audit standards, guidelines and procedures is universal to any audit engagement and is not influenced by short- and long-term issues.

 ©ISACA. All Rights Reserved.

7. **A. The objective of control self-assessment (CSA) is to have business managers become more aware of the importance of internal control and their responsibility in terms of corporate governance.**
   B. Reducing audit expenses is not a key benefit of CSA.
   C. Improved fraud detection is important but not as important as control ownership. It is not a principal objective of CSA.
   D. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

8. A. The findings of a previous audit are of interest to the auditor, but they are not the most critical step. The most critical step involves finding the current issues or high-risk areas, not reviewing the resolution of older issues. A review of historical audit findings could indicate that management is not resolving the risk items identified or that the recommendations were ineffective.
   B. Executive management is not required to approve the audit plan. It is typically approved by the audit committee or board of directors. Management could recommend areas to audit.
   C. Reviewing information security policies and procedures is normally conducted during fieldwork, not planning.
   D. Of all the steps listed, performing a risk assessment is the most critical. Risk assessment is required by ISACA IS Audit and Assurance Standard 1201 (Risk Assessment in Planning), statement 1201.2: "IT audit and assurance practitioners shall identify and assess risk relevant to the area under review when planning individual engagements." In addition to the standards requirement, if a risk assessment is not performed, then high-risk areas of the auditee systems or operations may not be identified for evaluation.

9. **A. Audit planning requires a risk-based approach.**
   B. Materiality pertains to potential weaknesses or absences of controls while planning a specific engagement, and whether such weaknesses or absences of controls could result in a significant deficiency or a material weakness.
   C. Fraud monitoring pertains to the identification of fraud-related transactions and patterns and may play a part in audit planning but only as it pertains to organizational risk.
   D. Sufficiency of audit evidence pertains to the evaluation of the sufficiency of evidence obtained to support conclusions and achieve specific engagement objectives.

10. A. Preventive controls are those that avert problems before they arise. Backup media cannot be used to prevent damage to files and, therefore, cannot be classified as preventive controls.
    B. Management controls modify processing systems to minimize repeat occurrences of the problem. Backup media do not modify processing systems and, therefore, do not fit the definition of management controls.
    C. A corrective control helps to correct or minimize the impact of a problem. Backup media can be used for restoring the files in case of damage to the files, thereby reducing the impact of a disruption.
    D. Detective controls help to detect and report problems as they occur. Backup media do not aid in detecting errors.

©ISACA. All Rights Reserved.

Page intentionally left blank

 ©ISACA. All Rights Reserved.

Part A: Planning

Audits are conducted for a variety of reasons. An audit can help an organization ensure effective operations, affirm its compliance with various regulations and confirm that the business is functioning well and is prepared to meet potential challenges. An audit can also help to gain assurance on the level of protection available for information assets. Most significantly, an audit can assure stakeholders of the financial, operational and ethical well-being of the organization. IS audits support all those outcomes, with a special focus on the information and related systems upon which most businesses and public institutions depend for competitive advantage.

IS audit is the formal examination and/or testing of information systems to determine whether:

- Information systems are in compliance with applicable laws, regulations, contracts and/or industry guidelines.
- Information systems and related processes comply with governance criteria and related and relevant policies and procedures.
- Confidentiality, integrity and availability of IS data meet appropriate levels based on measurable metrics.
- IS operations are being accomplished efficiently and effectiveness targets are being met.

During the audit process, an IS auditor reviews the control framework, gathers evidence, evaluates the strengths and weaknesses of internal controls based on the evidence and prepares an audit report that presents findings and recommendations for remediation to stakeholders in an objective manner.

In general terms, the typical audit process consists of three major phases (**figure 1.1**):

- Planning
- Fieldwork/documentation
- Reporting/follow-up

Figure 1.1—Typical Audit Process Phases



Source: ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016

These main phases can be further broken down into subphases; for example, the reporting phase can be broken down into report writing and issuance, issue follow-up and audit closing. The organization and naming conventions of these phases can be customized as long as the procedures and outcomes comply with applicable audit standards such as an IT Assurance Framework (ITAF).

Note

Information systems are defined as the combination of strategic, managerial and operational activities and related processes involved in gathering, processing, storing, distributing and using information and its related technologies. Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the people and process components. IT is defined as the hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form. The terms "IS" and "IT" will be used according to these definitions throughout this manual.

1.1 IS Audit Standards, Guidelines, Functions and Codes of Ethics

The credibility of any IS audit activity is largely determined by its adherence to commonly accepted standards. The fundamental elements of IS audit are defined and provided within ISACA's IS audit and assurance standards and guidelines. ISACA's code of professional ethics guides the professional and personal conduct of ISACA members and certification holders.

1.1.1 ISACA IS Audit and Assurance Standards

ISACA IS Audit and Assurance Standards define mandatory requirements for IS auditing and reporting and inform a variety of audiences of critical information, such as:

- For IS auditors, the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- For management and other interested parties, the profession's expectations concerning the work of practitioners
- For holders of the CISA designation, their professional performance requirements

The framework for the ISACA IS Audit and Assurance Standards provides for multiple levels of documents:

- Standards define mandatory requirements for IS audit and assurance and reporting.

©ISACA. All Rights Reserved.

- Guidelines provide guidance in applying IS audit and assurance standards. The IS auditor should consider guidelines in determining how to achieve implementation of standards, use professional judgment in their application and be prepared to justify any departures.
- Tools and techniques provide examples of processes an IS auditor might follow in an audit engagement. The tools and techniques documents provide information on how to meet standards when completing IS auditing work, but they do not set requirements.

ISACA IS Audit and Assurance Standards are divided into general, performance and reporting categories:

- **General**—Provide the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments and deal with an IS auditor's ethics, independence, objectivity, due care, knowledge, competency and skill.
- **Performance**—Deal with the conduct of the assignment, such as planning and supervision; scoping; risk and materiality; resource mobilization; supervision and assignment management; audit and assurance evidence and the exercising of professional judgment and due care
- **Reporting**—Address the types of reports, means of communication and the information communicated

1.1.2 ISACA IS Audit and Assurance Guidelines

ISACA IS Audit and Assurance Guidelines provide guidance and information on how to comply with the ISACA IS Audit and Assurance Standards. An IS auditor should:

- Consider the guidelines in determining how to implement ISACA Audit and Assurance Standards
- Use professional judgment in applying them to specific audits
- Be able to justify any departure from the ISACA Audit and Assurance Standards

Note

The CISA candidate is not expected to know specific ISACA standard and guidance numbering or memorize any specific ISACA IS audit and assurance standard or guideline. However, the exam will test a CISA candidate's ability to apply these standards and guidelines within the audit process.

1.1.3 ISACA Code of Professional Ethics

ISACA's Code of Professional Ethics guides the professional and personal conduct of ISACA members and certification holders.

ISACA members and certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including audit, control, security and risk management.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.
4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
6. Inform appropriate parties of the results of work performed, including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including audit, control, security and risk management.

Note

A CISA candidate is not expected to memorize the ISACA Code of Professional Ethics.[1] The exam will test a candidate's understanding and application of the code.

[1] ISACA, "Code of Professional Ethics," *https://www.isaca.org/credentialing/code-of-professional-ethics*

1.1.4 ITAF TM

ITAF is a comprehensive and best practice-setting reference model that:

- Establishes standards that address IS auditor roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements
- Defines terms and concepts specific to IS assurance
- Provides guidance and tools and techniques on the planning, design, conduct and reporting of IS audit and assurance assignments

Note

A CISA candidate will not be tested on the organization or arrangement of the ITAF framework. However, the application of audit and assurance standards is tested.

1.1.5 IS Internal Audit Function

The role of the IS internal audit function should be established by an audit charter approved by the board of directors and the audit committee (or by senior management if these entities do not exist). Professionals should have a clear mandate to perform the IS audit function, which may be expressed in the audit charter.

Audit Charter

IS audit can be a part of internal audit, or function as an independent group or be integrated within a financial and operational audit to provide IT-related control assurance to the financial or management auditors. Therefore, the audit charter may include IS audit as an audit support function. Additionally, the audit charter should include the IS audit function's role with consulting-related services that it may perform.

The charter should clearly state management's responsibility and objectives for, and delegation of authority to, the IS audit function. The highest level of management and the audit committee, if one exists, should approve the charter. Once established, the charter should be changed only if the change is thoroughly justified.

The responsibility, authority and accountability of the IS audit function should be appropriately documented in an audit charter or engagement letter. An audit charter is an overarching document that covers the entire scope of audit activities in an entity while an engagement letter is more focused on a particular audit exercise to be initiated in an organization with a specific objective in mind. If IS audit services are provided by an external firm, the scope and objectives of the services should be documented in a formal contract or statement of work between the contracting organization and the service provider. In either case, the internal audit function should be independent and report to an audit committee, if one exists, or to the highest management level, such as the board of directors.

Note

For additional guidance, see standard 1001 Audit Charter and guideline 2001 Audit Charter.

Management of the IS Audit Function

The IS audit function should be managed and led in a manner that ensures that the diverse tasks performed by the audit team will fulfill audit function objectives, while preserving audit independence and competence. Furthermore, managing the IS audit function should ensure value-added contributions to senior management in the efficient management of IT and achievement of business objectives.

Note

For additional guidance, see standards 1002 Organizational Independence, 1003 Auditor Objectivity, 1004 Reasonable Expectation and 1005 Due Professional Care. Also see the related guidelines: 2002, 2003, 2004 and 2005.

IS Audit Resource Management

IS technology is constantly changing. Therefore, it is important that IS auditors maintain their competency through updates of existing skills and obtain training directed toward new audit techniques and technological areas. An IS auditor must have the technical skills and knowledge necessary to perform audit work. Further, an IS auditor must maintain technical competence through appropriate continuing professional education. Skills and knowledge should be taken into consideration when planning audits and assigning staff to specific audit assignments.

Preferably, a detailed staff training plan should be drawn up for the year based on the organization's direction in terms of technology and related risk that needs to be addressed. The plan should be reviewed periodically to ensure that training efforts and results are aligned with the direction the audit organization is taking. Additionally, IS audit management should provide the necessary IT resources to properly perform IS audits of a

©ISACA. All Rights Reserved.

highly specialized nature (e.g., tools, methodology, work programs).

Note

For additional guidance, see standard 1006 Proficiency and guideline 2006 Proficiency.

Using the Services of Other Auditors and Experts

Due to the scarcity of IS auditors and the need for IT security specialists and other subject matter experts to conduct audits of highly specialized areas, the audit department or auditors entrusted with providing assurance may require the services of other auditors or experts. Outsourcing of IS assurance and security services is increasingly becoming a common practice.

Note

The IS auditor should be familiar with ISACA Audit and Assurance Standard 1204 Performance and Supervision and the IS Audit and Assurance Guideline 2206 Using the Work of Other Experts, which focus on the rights of access to the work of other experts.

External experts could include experts in technologies such as networking, systems integration and digital forensics, or subject matter experts who specialize in a particular industry or area such as banking, securities trading, insurance, privacy or the law.

When there is a proposal to outsource a part or all of IS audit services to other auditors and experts or external service providers, the IS auditor should consider:

- Restrictions on outsourcing of audit/security services provided by laws and regulations
- Audit charter or contractual stipulations
- Impact on overall and specific IS audit objectives
- Impact on IS audit risk and professional liability
- Independence and objectivity of other auditors and experts
- Professional competence, qualifications and experience
- Scope and approach of work to be outsourced
- Supervisory and audit management controls
- Method and modalities of communication of results of audit work
- Compliance with legal and regulatory stipulations
- Compliance with applicable professional standards

Based on the nature of assignment, the IS auditor may also need to consider:

- Testimonials/references and background checks
- Access to systems, premises and records
- Confidentiality restrictions to protect customer-related information
- Use of computer-assisted auditing techniques (CAATs) and other tools to be used by the external audit service provider
- Standards and methodologies for performance of work and documentation
- Nondisclosure agreements

The IS auditor or entity outsourcing the auditing services should monitor the relationship to ensure objectivity and independence throughout its duration. It is important to understand that although a part or the whole of the audit work may be delegated to an external service provider, the related professional liability is not necessarily delegated. Therefore, it is the responsibility of the IS auditor or entity employing the services of external service providers to:

- Clearly communicate the audit objectives, scope and methodology through a formal engagement letter
- Establish a monitoring process for regular review of the work of the external service provider with regard to planning, supervision, review and documentation. For example, the work papers of other IS auditors or experts should be reviewed to confirm the work was appropriately planned, supervised, documented and reviewed and to consider the appropriateness and sufficiency of the audit evidence provided. Likewise, the reports of other IS auditors or experts should be reviewed to confirm the scope specified in the audit charter, terms of reference or letter of engagement has been observed, the reports were performed within the defined auditable period, any significant assumptions used by other IS auditors or experts have been identified and the findings and conclusions reported have management approval.
- Assess the usefulness and appropriateness of such external providers' reports and assess the impact of significant findings on the overall audit objectives

1.2 Types of Audits, Assessments and Reviews

An IS auditor should understand the various types of audits, assessments and reviews that can be performed along with the basic associated audit procedures, which may be carried out by internal or external groups.

An audit includes formal inspection and verification to check whether standards or guidelines are being followed, records are accurate, or efficiency and effectiveness targets are met. Formal audits provide a

higher level of assurance than broader assessments and reviews. In general, assessments and reviews may be perceived with less negative stigma than audits and may focus on opportunities for reducing the costs of poor quality, employee perceptions on quality aspects, proposals to senior management on policy, goals, etc.

Some examples of audits, assessment and reviews include:

- **IS audit**—An IS audit is designed to collect and evaluate evidence to determine whether an information system and related resources are adequately safeguarded and protected; maintain data and system integrity and availability; provide relevant and reliable information; achieve organizational goals effectively; consume resources efficiently; and have, in effect, internal controls that provide reasonable assurance not only that business, operational and control objectives will be met but also that undesired events will be prevented or detected and corrected in a timely manner.
- **Compliance audit**—A compliance audit includes tests of controls to demonstrate adherence to specific regulations or industry-specific standards or practices. These audits often overlap other types of audits but may focus on particular systems or data.
- **Financial audit**—A financial audit assesses the accuracy of financial reporting. A financial audit will often involve detailed, substantive testing, although IS auditors are increasingly placing more emphasis on a risk- and control-based audit approach. A financial audit relates to financial information integrity and reliability.
- **Operational audit**—An operational audit is designed to evaluate the internal control structure in a given process or area. IS audits of application controls or logical security systems are examples of operational audits.
- **Integrated audit**—There are different types of integrated audits, but typically an integrated audit combines financial and operational audit steps and may or may not include the use of an IS auditor. An integrated audit is performed to assess the overall objectives within an organization, related to financial information and to safeguarding assets, maximizing efficiency and ensuring compliance. An integrated audit can be performed by external or internal auditors and includes compliance tests of internal controls and substantive audit steps. See section 1.10 Quality Assurance and Improvement of the Audit Process for more information.
- **Administrative audit**—An administrative audit is designed to assess issues related to the efficiency of operational productivity within an organization.
- **Specialized audit**—Many different types of specialized audits are conducted. Within the category of IS audit, specialized reviews may examine areas such as fraud or services performed by third parties.
  - **Third-party service audit**—A third-party service audit addresses the audit of outsourced financial and business processes to third-party service providers that may operate in different jurisdictions. A third-party service audit issues an opinion on a service organization's description of controls through a service auditor's report, which then can be used by the IS auditor of the entity that engages the service organization.
  - **Fraud audit**—A fraud audit is a specialized audit designed to discover fraudulent activity. Auditors often use specific tools and data analysis techniques to discover fraud schemes and business irregularities.
  - **Forensic audit**—A forensic audit is a specialized audit to discover, disclose and follow up on fraud and crime. The primary purpose of such an audit is the development of evidence for review by law enforcement and judicial authorities.
- **Computer forensic audit**—A computer forensic audit is an investigation that includes the analysis of electronic computing devices with the intent to gather and preserve evidence. An IS auditor possessing the necessary skills can assist an information security manager or forensic specialist in performing forensic investigations and can conduct an audit of the system to ensure compliance with the evidence collection procedures for forensic investigation.
- **Functional audit**—A functional audit provides an independent evaluation of software products, verifying that its configuration items' actual functionality and performance are consistent with the requirement specifications. Specifically, a functional audit is conducted either prior to software delivery or after implementation.
- **Readiness assessment**—A readiness assessment is a review of an organization's current state of compliance or adherence to documented standards. Readiness assessments generally focus on control design as opposed to operating effectiveness and result in actionable items for an organization to remediate prior to a formal audit.

©ISACA. All Rights Reserved.

1.2.1 Control Self-Assessment

Control self-assessment (CSA) is an assessment of controls made by the staff and management of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal control system of the organization is reliable. It also ensures that employees are aware of the risk to the business and conduct periodic, proactive reviews of controls. It is a methodology used to review key business objectives; to assess risk involved in achieving the business objectives; and to ensure that internal controls are designed to manage business risk through a formal, documented and collaborative process.

An IS auditor acts in the role of facilitator to help business process owners define and assess appropriate controls and to help them understand the need for controls, based on risk to the business processes. The process owners and the personnel who run the processes use their knowledge and understanding of the business function to evaluate the performance of controls against the established control objectives, while considering the risk appetite of the organization. Process owners are in an ideal position to define the appropriate controls because they are knowledgeable about the process objectives.

A CSA program can be implemented through methods such as questionnaires and surveys, facilitated workshops and informal peer reviews. For small business units within organizations, a CSA program can be implemented through facilitated workshops in which functional management and IS auditors come together and deliberate how best to evolve a control structure for the business unit. In a workshop, the role of a facilitator is to support the decision-making process. The facilitator creates a supportive environment to help participants explore their own experiences and those of others; identify control strengths and weaknesses; and share their knowledge, ideas and concerns. If appropriate, the facilitator may also offer their own expertise in addition to facilitating the exchange of ideas and experience.

Objectives of CSA

The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional areas. It is not intended to replace audit's responsibilities but to enhance them. Auditees such as line managers are responsible for controls in their environment; the managers should be responsible for monitoring the controls. CSA programs must educate management about control design and monitoring, particularly concentrating on areas of high risk.

When employing a CSA program, measures of success for each phase (planning, implementation and monitoring) should be developed to determine the value derived from CSA and its future use. One critical success factor (CSF) is a meeting with the business unit representatives (including appropriate and relevant staff and management) to identify the business unit's primary objective and to determine the reliability of the internal control system. Actions that increase the likelihood of achieving the primary objective should be identified.

Benefits of CSA

Some of the benefits of CSA include:

- Early detection of risk
- More effective and improved internal controls
- Creation of cohesive teams through employee involvement
- Development of a sense of control ownership among employees and process owners and reduction of their resistance to control improvement initiatives
- Increased employee awareness of organizational objectives
- Increased employee knowledge of risk and internal controls
- Increased communication between operational and top management
- Increased motivation for employees
- Improved audit rating process
- Reduction in control cost
- Assurance provided to stakeholders and customers
- Necessary assurance given to top management about the adequacy of internal controls relative to regulations and laws

Disadvantages of CSA

CSA contains some disadvantages, including:

- It could be mistaken as an audit function replacement.
- It may be regarded as an additional workload (e.g., one more report to be submitted to management).
- Failure to act on improvement suggestions could damage employee morale.
- Lack of audit knowledge may limit effectiveness in the detection of weak controls.

The IS Auditor's Role in CSA

When CSA programs are established, auditors become internal control professionals and assessment facilitators. Their value in these roles is evident when management takes ownership and responsibility for internal

control systems under its authority through process improvements in control structures, including an active monitoring component.

To be effective in this facilitative and innovative role, the IS auditor must understand the business process being assessed. It is important to remember that in the CSA process, IS auditors are the facilitators and the management client is the participant. For example, during a CSA workshop, instead of performing detailed audit procedures, the IS auditor will lead and guide the auditees in assessing their environment by providing insight into the objectives of controls based on risk assessment. The managers, with a focus on improving the productivity of the process, might suggest replacement of preventive controls. In this case, the IS auditor is better positioned to explain the risk associated with such changes.

To provide higher-quality audits and make use of internal and/or external audits or subject matter expertise, an integrated audit approach is used to perform risk-based assessments of internal controls over an operation, process or entity.

1.2.2 Integrated Auditing

The dependence of business processes on IT requires that all auditors develop an understanding of IT control structures. In addition, IS auditors must develop an understanding of the business control structures. This type of integrated auditing can be defined as the process whereby appropriate audit disciplines are combined to assess key internal controls over an operation, process or entity with a focus on risk. A risk assessment aims to understand and identify risk arising from the entity and its environment, including relevant internal controls. At this stage, the role of an IS auditor is typically to understand and identify risk under topical areas such as information management, IT infrastructure, IT governance and IT operations. Other audit and assurance specialists will seek to understand the organizational environment, business risk and business controls. A key element of the integrated approach is a discussion among the whole audit team of emerging risk, with consideration of impact and likelihood.

Detailed audit work focuses on the relevant controls in place to manage risk. IT systems frequently provide a first line of preventive and detective controls, and the integrated audit approach depends on a sound assessment of their efficiency and effectiveness.

The integrated audit process typically involves:

- Identification of risk faced by the organization for the area being audited
- Identification of relevant key controls
- Review and understanding of the design of key controls
- Testing IT system support for key controls
- Testing operational effectiveness of management controls
- A combined report or opinion on control risk, design and weaknesses

An integrated audit demands a focus on business risk and a drive for creative control solutions. It is a team effort of audit and assurance professionals with different skill sets. Using this approach permits a single audit of an entity with one comprehensive report. An additional benefit is that this approach assists in staff development and retention by providing variety and the ability to see how all the elements (functional and IT) mesh to form the complete picture. See **figure 1.2** for an integrated auditing approach.

Figure 1.2—An Integrated Audit



The integrated audit concept has radically changed the way audits are accepted and valued by different stakeholders. For example:

- Employees or process owners better understand the objectives of an audit because they can see the linkage between controls and audit procedures.
- Top management better understands the linkage between increased control effectiveness and corresponding improvements in the allocation and utilization of IT resources.

©ISACA. All Rights Reserved.

- Shareholders better understand the linkage between the push for a greater degree of corporate governance and its impact on the generation of financial statements that can be relied on.

All these developments have contributed to the growing popularity of integrated audits.

1.3 Risk-Based Audit Planning

Audit planning is conducted at the beginning of the audit process to establish the overall audit strategy and detail the specific procedures to be carried out to implement the strategy and complete the audit. It includes both short- and long-term planning. Short-term planning considers audit issues that will be covered during the year, whereas long-term planning considers risk-related issues regarding changes in the organization's IT strategic direction that will affect the organization's IT environment.

All of the relevant processes that represent the blueprint of the enterprise's business should be included in the audit universe. The audit universe ideally lists all the processes that may be considered for audit. Each process may undergo a qualitative or quantitative risk assessment carried out by evaluating the risk in the context of defined, relevant risk factors. The risk factors are those that influence the frequency and/or business impact of risk scenarios. For example, for a retail business, reputation can be a critical risk factor. The evaluation of risk should ideally be based on inputs from the business process owners. Evaluation of the risk factors should be based on objective criteria, although subjectivity cannot be completely avoided. For example, with respect to the reputation factor, the criteria (based on which inputs can be solicited from the business) may be rated as:

- **High**—A process issue may result in reputational damage that will take the organization more than six months to recover.
- **Medium**—A process issue may result in reputational damage that will take the organization less than six months but more than three months to recover.
- **Low**—A process issue may result in reputational damage that will take the organization less than three months to recover.

In this example, the defined time frame represents the objective aspect of the criteria, and the subjective aspect of the criteria can be found in the business process owners' determination of the time frame—whether it is more than six months or less than three months. After the risk is evaluated for each relevant factor, a criterion may be defined to determine the overall risk for each of the processes.

The audit plan can then be constructed to include all of the processes that are rated "high," which would represent the ideal annual audit plan. However, in practice, often the available resources are not sufficient to execute the entire ideal plan. This analysis will help the audit function demonstrate the gap in resourcing and give top management a good idea of the amount of risk that it is accepting if it does not add to or augment the existing audit resources.

Analysis of short- and long-term issues should occur at least annually. This frequency is necessary to consider new control issues, enhanced evaluation techniques, and changes in the risk environment, technologies and business processes. The results of this analysis should be reviewed by senior audit management and approved by the audit committee, if available, or alternatively by the board of directors, and communicated to relevant levels of management. The annual planning should be updated if any key aspects of the risk environment have changed (e.g., acquisitions, new regulatory issues, market conditions).

Note

For additional guidance, see standards 1007 Assertions and 1008 Criteria and related guidelines 2007 and 2008.

1.3.1 Individual Audit Assignments

In addition to overall annual planning, each individual audit assignment must be adequately planned. An IS auditor should understand that other considerations —such as the results of periodic risk assessments, changes in the application of technology and evolving privacy issues and regulatory requirements—may impact the overall approach to the audit. An IS auditor should take into consideration system implementation/ upgrade deadlines, current and future technologies, requirements from business process owners and IS resource limitations.

When planning an audit, an IS auditor must understand the overall environment under review. This should include gaining a general understanding of the various business practices and functions relating to the audit subject, as well as the types of information systems and technology supporting the activity. For example, an IS auditor should be familiar with the regulatory environment in which the business operates.

To perform audit planning, an IS auditor should perform the steps indicated in **figure 1.3**.

Note

For additional guidance, see standard 1201 Risk Assessment in Planning and guideline 2201 Risk Assessment in Planning.

Figure 1.3—Steps to Perform Audit Planning

- Gain an understanding of the organization's mission, objectives, purpose and processes, which include information and processing requirements such as availability, integrity, security and business technology and information confidentiality.
- Gain an understanding of the organization's governance structure and practices related to the audit objectives.
- Understand changes in the business environment of the auditee.
- Review prior work papers.
- Identify stated contents such as policies, standards and required guidelines, procedures and organization structure.
- Perform a risk analysis to help in designing the audit plan.
- Set the audit scope and audit objectives.
- Develop the audit approach or audit strategy.
- Assign personnel resources to the audit.
- Address engagement logistics.
- Identify opportunities for continuous audit or audit automation using computer-assisted audit tools (CAATs).

1.3.2 Effect of Laws and Regulations on IS Audit Planning

Each organization, regardless of its size or the industry within which it operates, will need to comply with a number of governmental and external requirements related to IS practices and controls and the manner in which data is used, stored and secured. Additionally, industry regulations can impact the way data is processed, transmitted and stored (e.g., stock exchange, central banks, etc.). Special attention should be given to compliance issues in industries that are closely regulated.

Because of the dependency on information systems and related technology, several countries are making efforts to add legal regulations concerning IS audit and assurance. The content of these legal regulations pertains to:

- Establishment of regulatory requirements
- Responsibilities assigned to corresponding entities
- Financial, operational and IS audit functions

Management at all levels should be aware of the external requirements relevant to the goals and plans of the organization and to the responsibilities and activities of the information services department/function/activity.

There are two major areas of concern:

1. Legal requirements (i.e., laws, regulations and contractual agreements) applicable to audit or IS audit
2. Legal requirements placed on the auditee regarding its systems, data management, reporting, etc.

These areas impact the audit scope and audit objectives, which are important to internal and external audit and assurance professionals. Legal issues related to ergonomic regulations may also impact the organization's business operations.

An IS auditor would perform the following steps to determine an organization's level of compliance with external requirements:

- Identify government or other relevant external requirements dealing with:
  - Electronic data, personal data, copyrights, ecommerce, e-signatures, etc.
  - IS practices and controls
  - The manner in which computers, programs and data are stored
  - The organization or the activities of information technology services
  - IS audits
- Document applicable laws and regulations.
- Assess whether the management of the organization and the IT function have considered the relevant external requirements in making plans and in setting policies, standards and procedures and business application features.
- Review internal IT department/function/activity documents that address adherence to laws applicable to the industry.
- Determine adherence to established procedures that address external requirements.
- Determine if there are procedures in place to ensure that contracts or agreements with external IT services providers reflect any legal requirements related to responsibilities.

©ISACA. All Rights Reserved.

Note

A CISA candidate will not be asked about any specific laws or regulations but may be questioned about how one would audit for compliance with laws and regulations.

Risk-based audit planning is the deployment of audit resources to areas within an organization that represent the greatest risk. It requires an understanding of the organization and its environment, specifically:

- External and internal factors affecting the organization
- The organization's selection and application of policies and procedures
- The organization's objectives and strategies
- Measurement and review of the organization's performance

As part of obtaining this understanding, an IS auditor must also gain an understanding of the key components of the organization's:

- Strategy management
- Business products and services
- Corporate governance process
- Transaction types, transaction partners and transaction flows within information systems

Effective risk-based auditing uses risk assessment to drive the audit plan and minimize the audit risk during the execution of an audit.

A risk-based audit approach is used to assess risk and to assist an IS auditor in making the decision to perform either compliance testing or substantive testing. It is important to stress that the risk-based audit approach efficiently assists an IS auditor in determining the nature and extent of testing.

Within this concept, inherent risk, control risk or detection risk should not be of major concern, despite some resulting weaknesses. In a risk-based audit approach, IS auditors do not rely solely on risk assessment; they also rely on internal and operational controls and knowledge of the organization or the business. This type of risk assessment decision-making can help relate the cost-benefit analysis of the control to the known risk, allowing the organization to make practical choices.

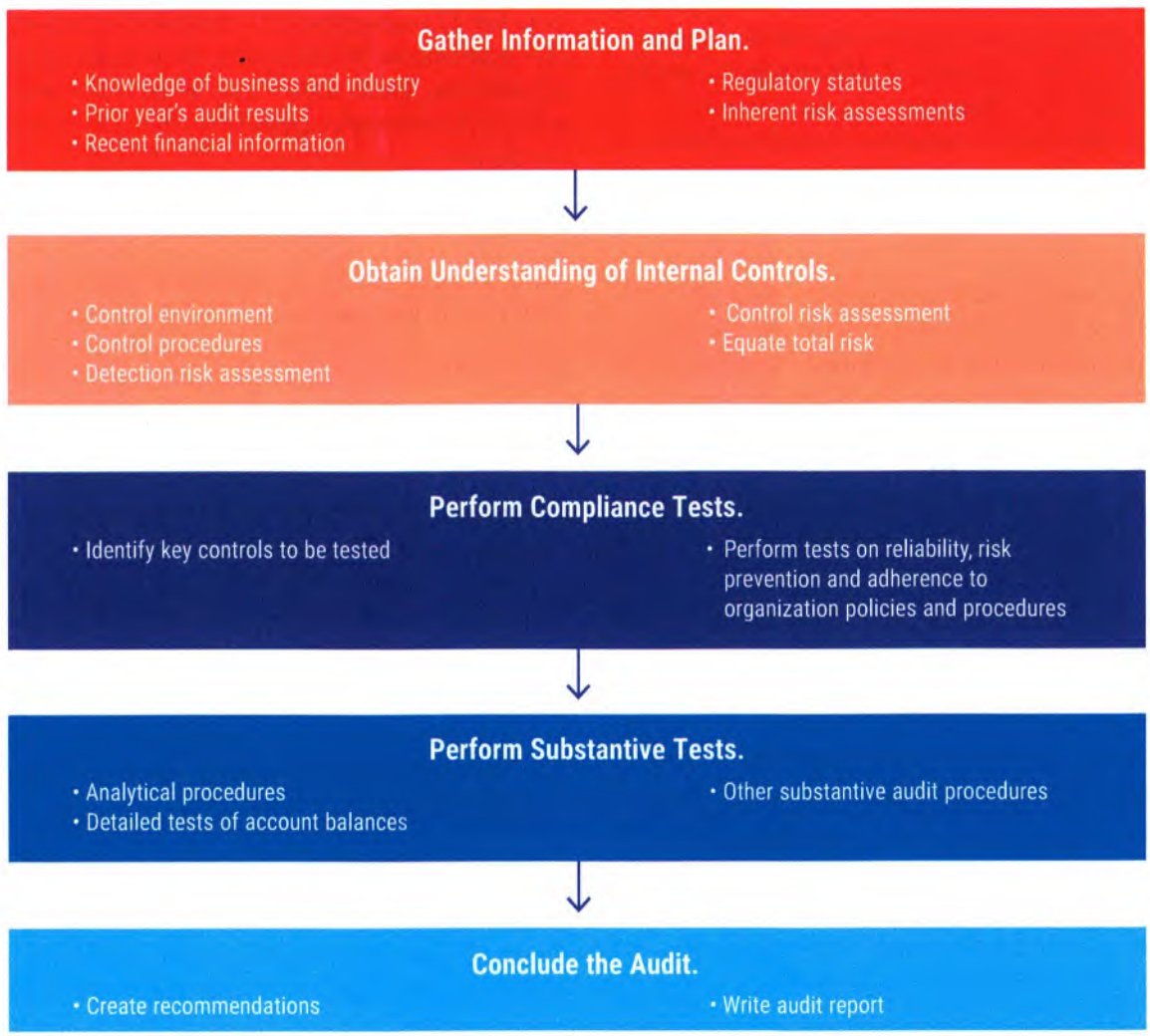
Business risk includes concerns about the probable effects of an uncertain event on achieving established business objectives. The nature of business risk may be financial, regulatory or operational. Risk may also be derived from specific technologies. For example, an airline company is subject to extensive safety regulations and economic changes, both of which impact the continuing operations of the company. In this context, the availability of IT services and their reliability are critical. Risk also includes measures an organization is willing to take to achieve or advance its objectives even though the results may be unproven or uncertain.

By understanding the nature of the business, an IS auditor can identify and categorize types of risk and can better determine the appropriate risk model or approach in conducting the audit. The risk model assessment can be as simple as creating weights for the types of risk associated with the business and identifying the risk in an equation. On the other hand, risk assessment can be a scheme in which risk is given elaborate weights based on the nature of the business or the significance of the risk. A simplistic overview of a risk-based audit approach is shown in **figure 1.4**.

Note

For further guidance, see standard 1204 Materiality.

Figure 1.4—Risk-Based Audit Approach



1.3.3 Audit Risk and Materiality

Audit risk can be defined as the risk that information collected may contain a material error that may go undetected during the audit. An IS auditor should also consider, if applicable, other factors relevant to the organization: customer data; privacy; availability of provided services; and corporate and public image, as in the case of public organizations or foundations.

Audit risk is influenced by:

- **Inherent risk**—As it relates to audit risk, inherent risk is the risk level or exposure of the process/entity to be audited without regard to the controls management has implemented. Inherent risk exists independent of an audit and can occur because of the nature of the business.
- **Control risk**—This is the risk of a material error that would not be prevented or detected on a timely basis by the system of internal controls. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often overlooked due to the volume of logged information. The control risk associated with computerized data validation procedures is ordinarily low if the processes are consistently applied.
- **Detection risk**—This is the risk that material errors or misstatements will not be detected by an IS auditor.
- **Overall audit risk**—This is the risk that the auditor may not detect a material error in information or financial reports. An objective in formulating the audit approach is to limit the audit risk in the area under scrutiny so the overall audit risk is at

©ISACA. All Rights Reserved.

a sufficiently low level at the completion of the examination.

An internal control weakness or set of combined internal control weaknesses may leave an organization highly susceptible to the occurrence of a threat (e.g., financial loss, business interruption, loss of customer trust, economic sanction). An IS auditor should be concerned with assessing the materiality of the items in question through a risk-based audit approach to evaluating internal controls.

Materiality refers to the importance of a piece of information with regard to its impact or effect on the functioning of the entity being audited. Materiality is the expression of the relative significance or importance of a particular matter in the context of the enterprise as a whole. There is an inverse relationship between materiality and the level of audit risk acceptable to the IS auditor (i.e., the higher the materiality level, the lower the acceptability of the audit risk and vice versa).

An IS auditor should have a good understanding of audit risk when planning an audit. An audit sample may not reflect every potential error in a population. However, by using proper statistical sampling procedures or a strong quality control process, the probability of detection risk can be reduced to an acceptable level.

Similarly, when evaluating internal controls, an IS auditor should realize that a given system may not detect a minor error. However, that specific error, combined with others, could become material to the overall system.

Note

A CISA candidate should understand audit risk and not confuse it with statistical sampling risk, which is the risk that incorrect assumptions are made about the characteristics of a population from which a sample is selected.

1.3.4 Risk Assessment

An IS auditor should understand how the organization being audited approaches risk assessment. Risk assessments should identify, quantify and prioritize risk against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action, priorities for managing information security risk and priorities for implementing controls selected to protect against risk.

Risk assessments should be performed by management periodically to address changes in the environment, security requirements and the risk landscape (e.g., in the assets, threats, vulnerabilities and impacts) and whenever significant changes occur. It is important to note that IT management is responsible for conducting risk assessments. If expertise is not present within the organization, the IS auditor may assist in risk assessment efforts. However, management is ultimately responsible for the risk assessment process. The IS auditor may perform a separate risk assessment to supplement the needs of risk-based audit planning.

Refer to section 2.5 Enterprise Risk Management for additional details on risk assessments.

1.3.5 IS Audit Risk Assessment Techniques

When determining which functional areas should be audited, an IS auditor may face a large variety of audit subjects. Each of these subjects may incur different types of risk. An IS auditor should evaluate risk candidates to determine the high-risk areas that should be audited.

There are many risk assessment methodologies available to an IS auditor, ranging from simple classifications based on the auditor's judgment of high, medium and low, to complex scientific calculations that provide numeric risk ratings.

One such risk assessment approach is a scoring system that is useful in prioritizing audits based on an evaluation of risk factors. The system considers variables such as technical complexity, level of control procedures in place and level of financial loss. These variables may or may not be weighted. The risk values are then compared to each other, and audits are scheduled accordingly.

Another form of risk assessment is subjective, in which an independent decision is based on business knowledge, executive management directives, historical perspectives, business goals and environmental factors. A combination of techniques can be used. Risk assessment methods may change and develop over time to best serve the needs of the organization. An IS auditor should consider the level of complexity and detail appropriate for the organization being audited.

IS auditors should leverage the results of management risk assessments to supplement their own risk assessment procedures. A degree of professional skepticism should be leveraged when reviewing or leveraging management assessments of risk due to potential independence impairment.

Using risk assessment to determine areas to be audited:

- Enables audit management to effectively allocate limited audit resources
- Ensures that relevant information has been obtained from all levels of management, including boards of directors, IS auditors and functional area managers. Generally, this information assists management in effectively discharging its responsibilities and ensures that the audit activities are directed to high-risk areas, which will add value for management.
- Establishes a basis for effectively managing the audit department
- Provides a summary of how the individual audit subject is related to the overall organization as well as to the business plans

1.3.6 Risk Analysis

Risk analysis, a subset of risk assessment, is used during audit planning to help identify risk and vulnerabilities so an IS auditor can determine the controls needed to mitigate risk. Risk assessment procedures provide a basis for the identification and assessment of risk of material vulnerabilities; however, they do not provide sufficient appropriate audit evidence to support the audit opinion.

In evaluating IT-related business processes applied by an organization, it is important to understand the relationship between risk and control. IS auditors must be able to identify and differentiate risk types and the controls used to mitigate risk. They should have knowledge of common business risk areas, related technology risk and relevant controls. They should also be able to evaluate the risk assessment and management processes and techniques used by business managers, and to make assessments of risk to help focus and plan audit work. In addition to understanding business risk and control, IS auditors must understand that risk exists within the audit process.

1.4 Types of Controls and Considerations

Every organization has controls in place. An effective control is one that prevents, detects and/or contains an incident and enables recovery from a risk event. Organizations design, develop, implement and monitor information systems through policies, procedures, practices and organizational structures to address various types of risk.

Controls are normally composed of policies, procedures, practices and organizational structures that are implemented to reduce risk to the organization. Internal controls are developed to provide reasonable assurance to management that the organization's business objectives will be achieved, and that risk events will be prevented or detected and corrected. Internal control activities and supporting processes may be manual or automated.

1.4.1 Internal Controls

Internal controls operate at all levels within an organization to mitigate risk exposures that potentially could prevent it from achieving its business objectives. The board of directors and senior management are responsible for establishing the appropriate culture to facilitate an effective and efficient internal control system and for continuously monitoring the effectiveness of the internal control system, although each individual within an organization must take part in this process.

There are two key aspects that controls should address:

1. What should be achieved
2. What should be avoided

Internal controls or control activities help ensure that management directives are carried out. They help ensure that necessary actions are taken to address risk and to achieve the enterprise's business objectives. Control activities occur throughout the enterprise, at all levels and in all functions, such as granting approvals and authorizations, implementing verifications and reconciliations, reviewing operating performance, securing assets and ensuring separation of duties.

1.4.2 Control Objectives and Control Measures

A control objective is defined as an objective of one or more operational areas or roles, which is designed to contribute to the fulfillment of the company's strategic goals. That is, the control objective is explicitly related to the company's overall strategy.

Control objectives are statements of the desired result or purpose to be achieved by implementing control activities (procedures). For example, control objectives may relate to:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Safeguarding information assets

Control objectives apply to all controls, whether they are manual, automated or both (e.g., review of system logs). Control objectives in an IS environment do not differ from those in a manual environment; however, the way the controls are implemented may be different.

©ISACA. All Rights Reserved.

Thus, control objectives need to be addressed relevant to specific IS-related processes.

A control measure is defined as an activity contributing to the fulfillment of a control objective. Both the control objective and control measure serve the decomposition of the strategic-level goals into such lower-level goals and activities that can be assigned as tasks to the staff. This assignment can take the form of a role specified in a job description.

IS Control Objectives

IS control objectives include a complete set of high-level requirements to be considered by management for effective control of each IT process area. IS control objectives are:

- Statements of the desired result or purpose to be achieved by implementing controls around IS processes
- Policies, procedures, practices and organizational structures
- Requirements designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected

Organizational management needs to make choices relative to control objectives by:

- Selecting those that are applicable
- Deciding on those that will be implemented
- Choosing how to implement them (i.e., frequency, span, automation, etc.)
- Accepting the risk of not implementing others that may apply

Specific IS control objectives include:

- Safeguarding information assets, including ensuring that information on automated systems is up to date and secure from improper access
- Ensuring that system development life cycle (SDLC) processes are established, in place and operating effectively to provide reasonable assurance that development of business, financial and/or industrial software systems and applications is repeatable, reliable and aligned to business objectives
- Ensuring integrity of general operating system (OS) environments, including network management and operations
- Ensuring integrity of sensitive and critical application system environments, including accounting/financial and management information (information objectives) and customer data, through:
  - **Authorization of the input**—Each transaction is authorized and entered only once.
  - **Validation of the input**—Each input is validated and will not have a negative impact on the processing of transactions.
  - **Accuracy and completeness of transaction processing**—All transactions are recorded accurately and entered into the system for the proper period.
  - **Reliability of overall information processing activities**—All programmatic actions taken by the system during processing are sound.
  - **Accuracy, completeness and security of the output**—Outputs can be relied upon and countermeasures are implemented to enable security of information assets generated.
  - **Database confidentiality, integrity and availability**—The underlying systems of record have general IS security controls.
- Ensuring appropriate identification and authentication of users of IS resources (end users and infrastructure support)
- Ensuring the efficiency and effectiveness of operations (operational objectives)
- Complying with users' requirements, organizational policies and procedures and applicable laws and regulations (compliance objectives)
- Ensuring availability of IT services by developing efficient business continuity plans (BCPs) and disaster recovery plans (DRPs) that include backup and recovery processes
- Enhancing protection of data and systems by developing an incident response plan
- Ensuring integrity and reliability of systems by implementing effective change management procedures
- Ensuring that outsourced IS processes and services have clearly defined service level agreements (SLAs) and contract terms and conditions designed to protect the organization's assets and meet business goals and objectives

General Control Methods

General control methods apply to all areas of an organization as seen in **figure 1.5**.

 ©ISACA. All Rights Reserved.

Figure 1.5—General Control Methods

Category	Description	Example
Managerial (administrative)	Controls related to the oversight, reporting, procedures and operations of a process	• Policies and procedures • Accounting controls (e.g., balancing) • Employee training and development • Compliance reporting
Technical	Also known as logical controls, controls that are provided through the use of technology, equipment or devices. A technical control requires proper managerial (administrative) controls to operate correctly.	• Firewall rulesets • Network or host-based intrusion detection systems (IDSs) • Passwords • Antimalware solutions
Physical	Controls that are installed to physically restrict access to a facility or hardware. Physical controls require maintenance, monitoring and the ability to address and react to an alert.	• Physical access badges and locks • Closed-circuit TV (CCTV)

Often operational and administrative controls that concern day-to-day operations, functions and activities are included within managerial controls. Technical controls and physical controls, respectively, relate to the use of technology and the use of physical equipment or devices to regulate access.

An enterprise should maintain a proper balance of control types in order to meet its specific needs and help achieve its business objectives. For example, the implementation of a technical control, such as a firewall, requires training for the staff who manage or operate it, correct procedures for its configuration, assignment of responsibilities for its monitoring and schedules for regular testing. If these coinciding controls are not in place, stakeholders may develop a false sense of security, resulting in unidentified vulnerabilities, an ineffective use of resources and greater risk than anticipated or intended.

IS-Specific Controls

Each general control method can be translated into an IS-specific control. A well-designed information system should have controls built in for all its sensitive or critical functions. For example, there should be a general procedure to ensure that adequate safeguards over access to assets and facilities can be translated into an IS-related set of control procedures, covering access safeguards over computer programs, data and equipment.

Examples of IS-specific control procedures include:

- Strategy and direction of the IT function
- General organization and management of the IT function
- Access to IT resources, including data and programs
- Systems development methodologies and change control
- Operations procedures
- Systems programming and technical support functions
- Quality assurance (QA) procedures
- Physical access controls
- BCP/DRP
- Networks and communication technology (e.g., local area networks, wide area networks, wireless)
- Database administration
- Protective and detective mechanisms against internal and external attacks

Note

A CISA candidate should understand concepts regarding IS controls and how to apply them in planning an audit.

Business Process Applications and Controls

In an integrated application environment, controls are embedded and designed into the business application that supports the processes. Business process control assurance involves evaluating controls at the process and activity levels, which may be a combination of management, programmed and manual controls. In addition to evaluating general controls that affect the processes, an IS auditor should evaluate business process owner-specific controls—such as proper security and separation of duties (SoD), periodic reviews, and approvals of access and application controls within the business process.

©ISACA. All Rights Reserved.

To effectively audit business application systems, an IS auditor must obtain a clear understanding of the application system under review. Numerous financial and operational functions are computerized for the purpose of improving efficiency and increasing the reliability of information. These applications range from traditional (including general ledger, accounts payable and payroll) to industry-specific (such as bank loans, trade clearing and material requirements planning). Given their unique characteristics, computerized application systems add complexity to audit efforts. These characteristics may include limited audit trails, instantaneous updating and information overload.

Figure 1.6 describes sample risk and controls for common business applications in an enterprise.

Figure 1.6—Business Application Controls

Business Application System	Description	Example Risk(s) and related Control(s)
Ecommerce	Ecommerce is the buying and selling of goods online.	Due to their exposure to the Internet, ecommerce applications are subject to a high risk of Structured Query Language (SQL) injection attacks. IS-specific controls such as secure coding training for developers, system development life cycle (SDLC) code reviews and form input validity checks could be used to mitigate applicable risk.
Electronic data interchange (EDI)	EDI replaced the traditional paper document exchange, such as medical claims and records, purchase orders, invoices or material release schedules.	Transmitted data is at risk of being intercepted and potentially manipulated or compromised. Appropriate encryption controls should be used to ensure the confidentiality and integrity of transmitted data.
Email	Email services are used by an enterprise to communicate electronically with internal or external parties.	Email provides an avenue for attackers to manipulate end users through social engineering. Spam filtering, hyperlink verification and phishing training for email users can decrease the likelihood of phishing-related social engineering attacks.
Industrial control systems (ICSs)	ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs) and other control system configurations such as programmable logic controllers (PLCs), which are often found in industrial sectors and critical infrastructures.	Systems like SCADA are highly sensitive and if compromised can have a direct impact on human life. Organizations should consider adding perimeter security controls, such as network segmentation and multifactor authentication, to get into and administer high-risk SCADA environments.
Artificial intelligence (AI) and expert systems	Expert systems are an area of AI and perform a specific function or are prevalent in certain industries. An expert system allows the user to specify certain basic assumptions or formulas and then uses those assumptions or formulas to analyze arbitrary events.	AI systems rely on learned data and associated decision trees that can be inherently biased. An IS auditor should ensure that the proper level of expertise was used in developing the basic assumptions and formulas.

 ©ISACA. All Rights Reserved.

Note

A CISA candidate should be familiar with different types of business application systems and architectures, processes, risk and related controls and IS audit implications and practices. The IS auditor should consult industry- or technology-specific guidance and apply applicable IS-specific controls as necessary. For example, when reviewing an ecommerce application, an IS auditor might consider applicable guidance from authoritative sources such as the Open Web Application Security Project (OWASP).[2] Where specific skillsets are not present within an IS audit department, external experts should be brought in to perform applicable reviews.

1.4.3 Control Classifications

Controls are implemented to provide reasonable assurance to management that the organization's business objectives will be achieved, and risk events will be prevented or detected and corrected. Elements of controls that should be considered when evaluating control strength are classified as preventive, detective or corrective in nature.

Figure 1.7 describes control categories.

Figure 1.7—Control Categories

Category	Description
Preventive	Inhibit or impede attempts to violate security policy and practices. Encryption, user authentication and vault-construction doors are examples of preventive controls.
Deterrent	Provide guidance or warnings that may dissuade intentional or unintentional attempts at compromise. Warning banners on login screens, acceptable use policies, security cameras and rewards for the arrest of hackers are examples of deterrent controls.
Detective	Provide warnings of violations or attempted violations of security policy and practices without inhibiting or impeding the questionable actions. Audit trails, intrusion detection systems (IDSs) and checksums are examples of detective controls.
Corrective	Remediate errors, omissions, unauthorized uses and intrusions when detected. Data backups, error correction and automated failover are examples of corrective controls.
Compensating	Offset a deficiency or weakness in the control structure of the enterprise, often because the baseline controls cannot meet a stated requirement due to legitimate technical or business constraints. Placing unsecured systems on isolated network segments with strong perimeter security and adding third-party challenge-response mechanisms to devices that do not support individual login accounts are examples of compensating controls that, while not directly addressing vulnerabilities, make it harder to exploit them.

Source: ISACA, *CRISC Official Review Manual 7th Edition Revised*, USA, 2023

Preventive controls are generally stronger at mitigating risk because they prevent threat events from occurring. For example, if a malicious threat actor attempts to log into a system that is accessible from the Internet with a compromised password, multifactor authentication requirements could prevent the threat actor from successfully accessing the system.

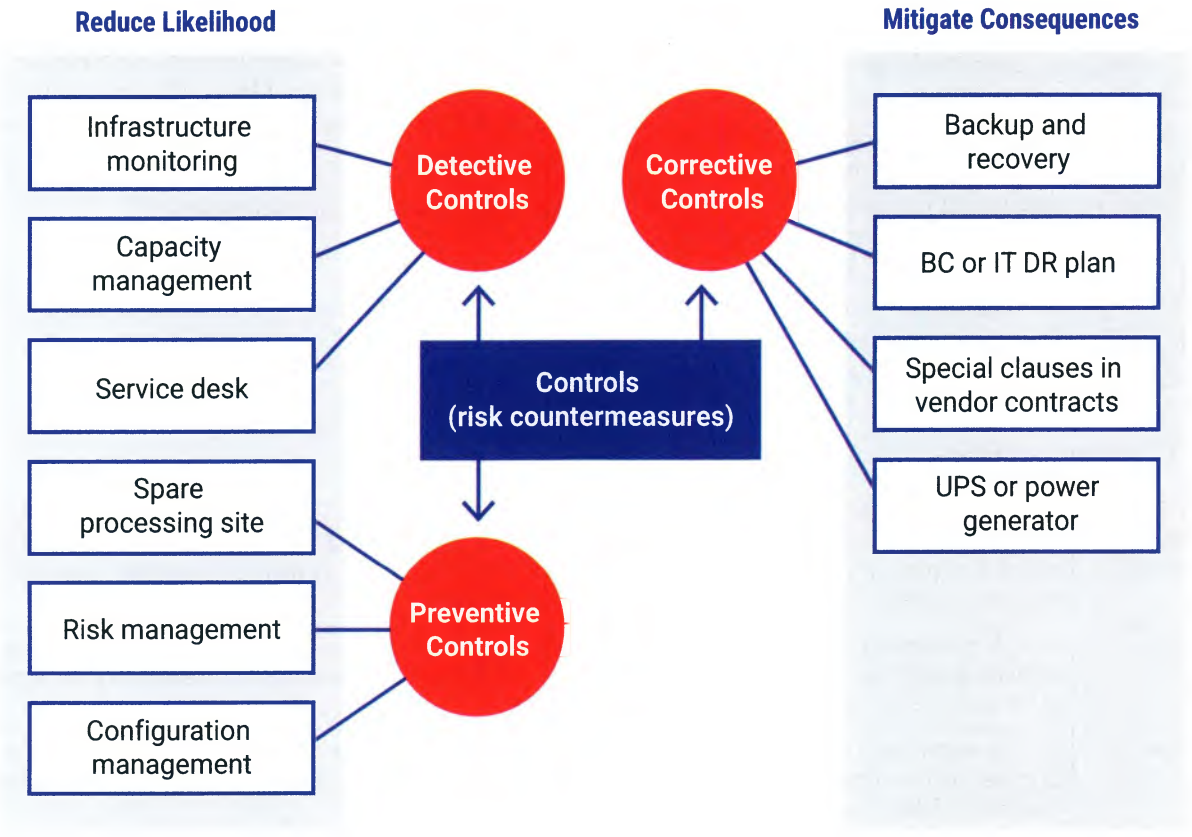
By contrast, a detective control does not stop unauthorized uses or entries from occurring, but it indicates that a threat event took place or is in progress. If a threat event occurs, a corrective control helps an enterprise recover from the effects of an attack. For example, if unauthorized access has been gained to a specific enterprise computer, a procedure is initiated to protect the rest of the network.

Organizations must implement a variety of control types based on applicable risk and cost-benefit analysis. In summary, detective and preventive controls are used to reduce the likelihood of a threat event (the probability of something happening), while corrective controls are intended to mitigate the consequences (**figure 1.8**).

[2] Open Web Application Security Project, *https://owasp.org/about/*

©ISACA. All Rights Reserved.

Figure 1.8—Control Purpose



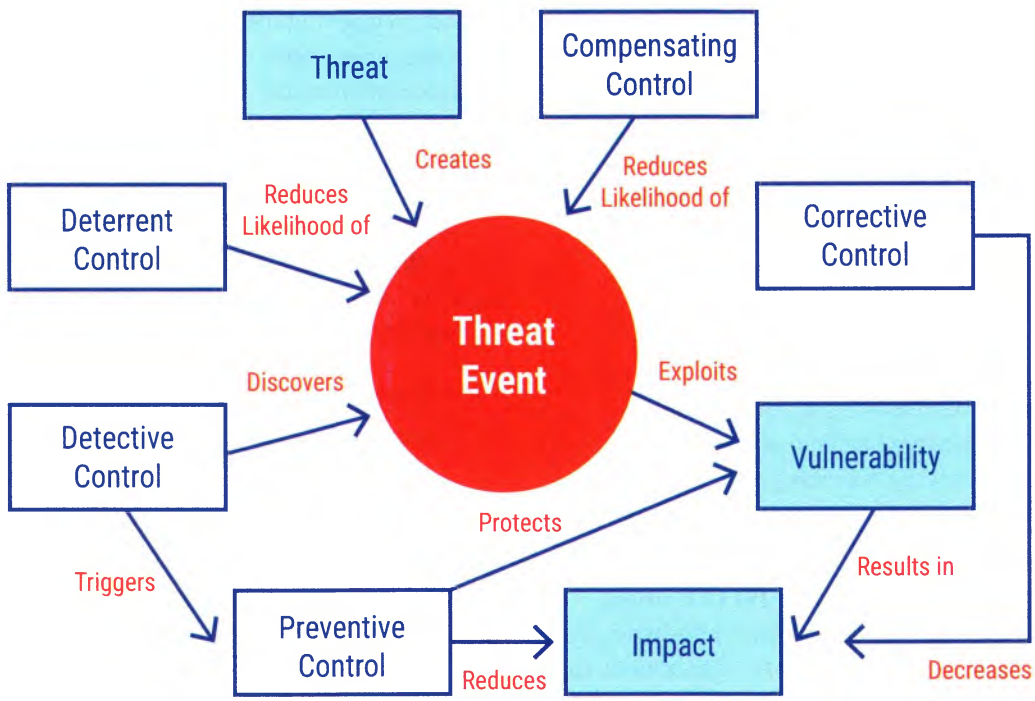
Source: ISACA, *Fundamentals of Information Systems Audit and Assurance* (Facilitator Guide), USA, 2018

An adequate mix of controls with different classifications is important not only to reduce the likelihood of threat events occurring but also to identify and mitigate consequences. Different types of controls can complement one another to help ensure that each is working effectively and addressing unique threat events as outlined in **figure 1.9**.

Note

A CISA candidate should understand the purpose of and differences between preventive, detective and corrective controls and be able to recognize examples of each.

Figure 1.9—Interaction of Control Types and Threat Events



Source: Adapted from ISACA, *CRISC® Review Manual, 7th Edition* Revised, USA, 2023

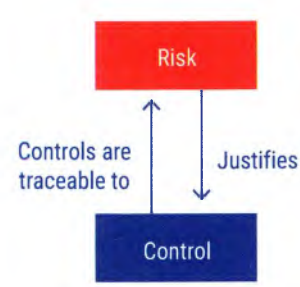
1.4.4 Control Relationship to Risk

There is a direct relationship between risk and control that demonstrates that risk is addressed through control and control is justified by the risk it addresses. **Figure 1.10** shows this relationship.

The IS auditor should have a solid understanding of the applicable risk to controls being evaluated. This not only informs the overall audit procedures that will be used but also helps determine overall materiality of any control weaknesses that may be identified during the performance of an IS audit.

When evaluating controls, the IS auditor should ensure that management's identified controls are mapped back to applicable risk. It is management's responsibility to ensure controls are documented and implemented per its assessment of risk.

Figure 1.10—Control Relationship to Risk



Source: ISACA, *IT Risk Fundamentals Study Guide*, USA, 2020

If controls implemented do not mitigate risk to an acceptable level (per the organization's risk tolerance), additional controls should be implemented. If appropriate or required countermeasures cannot be implemented based on system or business restrictions, compensating controls may be considered. However, any compensating control must achieve the same result the underperforming

©ISACA. All Rights Reserved.

control was designed to achieve. Placing unsecured systems on isolated network segments with strong perimeter security and adding third-party challenge-response mechanisms to devices that do not support individual login accounts are examples of compensating controls. Although the examples in the following sections are IT-specific, it is possible for non-IT compensating controls to exist.

1.4.5 Prescriptive Controls and Frameworks

In some instances, authoritative sources provide a prescriptive set of controls or control objectives for an organization to implement and assess. Prescriptive control sets or control frameworks attempt to provide a standard set of controls an organization should implement to mitigate applicable risk to the organization as a whole or to a specific business process.

Examples of sets of prescriptive controls or control objectives include:

- **Center for Internet Security (CIS) 18 Critical Security Controls**[3]—A prescriptive, prioritized and simplified set of best practices that organizations can use to strengthen their cybersecurity postures
- **OWASP Software Assurance Maturity Model (SAMM)**[4]—An open framework to help organizations formulate and implement strategies for software security that are tailored to the specific risk they face
- **Service Organization Controls (SOC) reports**[5]—A framework developed by the American Institute of Certified Public Accountants (AICPA) meant to be used by organizations to process data related to services they provide
- **Payment Card Industry (PCI) Data Security Standard (DSS)**[6]—A set of requirements that must be met by organizations that store, process, transmit or in any way affect the security of credit card data
- **Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)**[7]—A cybersecurity control framework for cloud computing encompassing various key practices to ensure cloud security across different cloud models and designed to provide fundamental security principles to guide cloud vendors and assist prospective cloud customers in assessing the overall security risk of a cloud provider

Organizations leveraging prescriptive control frameworks must identify applicable countermeasures in place to meet outlined control objectives. In some instances, prescriptive controls may not be applicable to an organization based on unique business practices. For example, if an organization accepting credit cards does not store credit card data as a part of its business process, then controls applicable to the protection of stored credit card information are likely not applicable. Where prescriptive controls do not apply to an organization, the organization should ensure the reasons and validation on non-applicability are formally documented.

1.4.6 Evaluation of the Control Environment

The control environment should be reviewed in accordance with the risk-based audit plan. Although IS audit will execute its risk-based audit plan, it is important to note that IS management should also evaluate the effectiveness of the control environment.

Management Control Monitoring

Management may perform its own monitoring of control effectiveness within a given audit cycle. This process helps to identify control deviations prior to a potentially less frequent audit and allows management to take corrective action.

Control monitoring ensures that:

- Control requirements are being met.
- Standards are being followed.
- Employees are complying with enterprise policies, practices and procedures.

Management can use the results of its own control monitoring efforts to continuously improve the organization's security program. An IS auditor may leverage these results as reassurance that controls were effectively working over a period of time. When

[3] Center for Internet Security, "The 18 CIS Critical Security Controls," *https://www.cisecurity.org/controls/cis-controls-list*
[4] OWASP Project, "OWASP SAMM," *https://owasp.org/www-project-samm/*
[5] American Institute of Certified Public Accountants, "SOC 2® - SOC for Service Organizations: Trust Services Criteria," *https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report*
[6] Payment Card Industry Security Standards Council, "PCI DSS: v4.0," *https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf*
[7] Cloud Security Alliance, "Cloud Controls Matrix," *https://cloudsecurityalliance.org/research/cloud-controls-matrix/*

reviewing management's control monitoring processes, an IS auditor should ensure the following:

- Identified control exceptions are remediated and lessons learned are considered for security program enhancement.
- Metrics are established for critical processes or control monitoring and are based on management's risk assessment.
- Metrics identify specific, quantifiable outputs for reporting.
- Independence considerations are made regarding potential completeness and accuracy concerns.
- Reporting establishes expected thresholds for control effectiveness and tracks success over time.

Independent Evaluation of the Control Environment

Once the applicable risk and controls are understood, the IS auditor can perform an evaluation of the control environment. An IS auditor reviews evidence gathered during the audit to determine if the operations reviewed are well controlled and effective. This is an area that requires judgment and experience. An IS auditor also assesses the strengths and weaknesses of the controls evaluated and determines if they are effective in meeting the control objectives established as part of the audit planning process.

©ISACA. All Rights Reserved.

Page intentionally left blank

Part B: Execution

Once an audit is planned and the scope and objectives are defined, the IS auditor is ready to execute the audit. The following sections provide guidance for executing an audit.

1.5 Audit Project Management

Several steps are required to perform an audit. Adequate planning is a necessary first step in performing an effective IS audit. To efficiently use IS audit resources, audit organizations must assess the overall risk for the general and application areas and related services being audited, and then develop an audit program that consists of objectives and audit procedures to satisfy the audit objectives. The audit process requires an IS auditor to gather evidence, evaluate the strengths and weaknesses of controls based on the evidence gathered through audit tests, and prepare an audit report that presents those issues (i.e., areas of control weaknesses with recommendations for remediation) to management in an objective manner.

Audit management must ensure the availability of adequate audit resources and a schedule for performing the audit procedures and, in the case of an internal IS audit, for conducting follow-up reviews on the status of corrective actions taken by management. The process of auditing includes defining the audit scope, formulating audit objectives, identifying audit criteria, performing audit procedures, reviewing and evaluating evidence, forming audit conclusions and opinions, and reporting to management after discussion with key process owners.

Project management techniques for audit projects include:

- **Plan the audit engagement**—Plan the audit, considering project-specific risk.
- **Build the audit plan**—Chart the necessary audit tasks across a timeline, optimizing resource use. Make realistic estimates of the time requirements for each task with proper consideration given to the availability of the auditee.
- **Execute the plan**—Execute audit tasks against the plan.
- **Monitor project activity**—Report actual progress against planned audit steps to ensure challenges are managed proactively and the scope is completed within time and budget.

1.5.1 Audit Objectives

Audit objectives refer to the specific goals that must be accomplished by the audit. In contrast, a control objective refers to how an internal control should function. An audit generally incorporates several audit objectives.

Audit objectives often focus on confirming that internal controls exist to minimize business risk and function as expected. These audit objectives include ensuring compliance with legal and regulatory requirements and ensuring the confidentiality, integrity, reliability and availability of information and IT resources. Audit management may give an IS auditor a general control objective to review and evaluate when performing an audit.

A key element in planning an IS audit is to translate basic and wide-ranging audit objectives into specific IS audit objectives. For example, in a financial/operational audit, a control objective could be to ensure that transactions are properly posted to the general ledger accounts. However, in an IS audit, the objective could be extended to ensure that editing features are in place to detect errors in the coding of transactions that may impact account-posting activities.

An IS auditor must understand how general audit objectives can be translated into specific IS control objectives. Determining an audit's objectives is a critical step in planning an IS audit.

One of the primary purposes of an IS audit is to identify control objectives and the related controls that address the objective. For example, an IS auditor's initial review of an information system should identify key controls. It should then be determined whether to test those controls for compliance. An IS auditor should identify both key general and application controls after developing an understanding and documenting the business processes and the applications/functions that support those processes and general support systems. Based on that understanding, an IS auditor should identify the key control points.

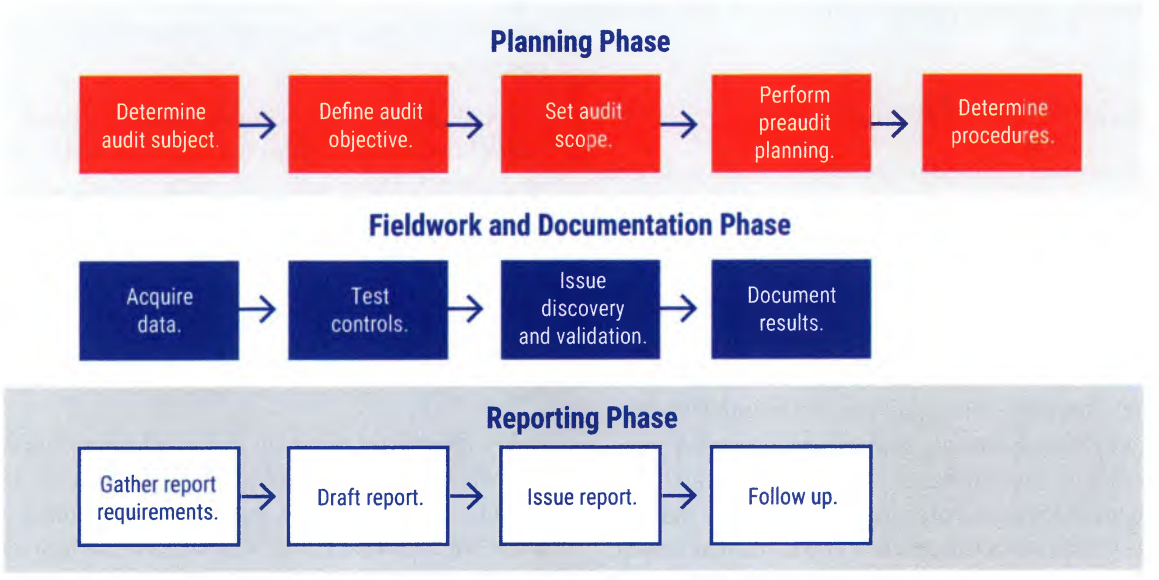
Alternatively, an IS auditor may assist in assessing the integrity of financial reporting data, referred to as substantive testing, through CAATs.

1.5.2 Audit Phases

Each phase in the execution of an audit can be divided into key steps to plan, define, perform and report the results, as shown in **figure 1.11**.

©ISACA. All Rights Reserved.

Figure 1.11—Typical Audit Process Steps by Phase



Source: ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016

Planning

Planning steps can be further broken down into more specific activities, as shown in **figure 1.12**.

Figure 1.12—Audit Process Activities for the Planning Phase

Audit Step	Description
1. Determine audit subject.	Identify the area to be audited (e.g., business function, system, physical location).
2. Define audit objective.	Identify the purpose of the audit. For example, an objective might be to determine whether program source code changes occur in a well-defined and controlled environment.
3. Set audit scope.	Identify the specific systems, function or unit of the organization to be included in the review. In the case of the program changes example, the scope statement might limit the review to a single application, system or a limited period of time. This step is very important because the information systems (IS) auditor will need to understand the IT environment and its components to identify the resources that will be required to conduct a comprehensive evaluation. A clear scope will help the IS auditor define a set of testing points that are relevant to the audit and to further determine the technical skills and resources necessary to evaluate different technologies and their components.

Figure 1.12—Audit Process Activities for the Planning Phase (cont.)

Audit Step	Description
4. Perform preaudit planning.	Conduct a risk assessment, which is critical in setting the final scope of a risk-based audit. For other types of audits (e.g., compliance), conducting a risk assessment is a good practice because the results can help the IS audit team justify the engagement and further refine the scope and preplanning focus. • Interview the auditee to inquire about activities or areas of concern that should be included in the scope of the engagement. • Identify regulatory compliance requirements. • Once the subject, objective and scope are defined, the audit team can identify the resources needed to perform the audit. Some of the necessary resources to be defined: ▪ Technical skills and resources ▪ Budget and effort to complete the engagement ▪ Locations or facilities to be audited ▪ Roles and responsibilities among the audit team ▪ Time frame for the various stages of the audit ▪ Sources of information for test or review, such as functional flowcharts, policies, standards, procedures and prior audit work papers ▪ Points of contact for administrative and logistics arrangements ▪ A communication plan that identifies whom to inform, when, how often and for what purposes
5. Determine audit procedures and steps for data gathering.	At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit program. Some of the specific activities in this step are: • Identify and obtain departmental policies, standards and guidelines for review. • Identify any regulatory compliance requirements. • Identify a list of individuals to interview. • Identify methods and tools to perform the evaluation. • Develop audit tools and methodology to test and verify controls. • Develop test scripts. • Identify criteria for evaluating the test. • Define a methodology to evaluate whether the test and its results are accurate (and repeatable if necessary).

Source: ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016

Fieldwork/Documentation

Fieldwork/documentation steps can be further broken down into more specific activities, as shown in **figure 1.13**.

©ISACA. All Rights Reserved.

Figure 1.13—Audit Process Activities for the Fieldwork/Documentation Phase

Audit Step	Description
1. Acquire data.	Establish a process to acquire audit-related data. An advance request list can be used to identify key evidence or interviews/observations that need to be gathered or performed during an audit. The IS auditor should establish a process to collect evidence in a secure manner (e.g., through fileshare). A governance, risk and compliance (GRC) tool may help facilitate audit data collection for more advanced audit functions.
2. Test controls.	Use testing techniques (e.g., interviews, observations, inspections, etc.) to evaluate controls applicable to the acquired data. In some instances, sampling may be required to review a subset of an overall population. For example, an IS auditor may select a sample of servers and perform an observation to confirm that antimalware solutions are installed per policy.
3. Discover and validate issues.	Identify potential issues throughout the audit process. Issues are deviations from expected audit outcomes (e.g., policy requirements) and are the basis for recommendations the auditor will provide for management action.
4. Document results.	Document the results within the audit program and work papers per document audit standards for the IS auditor's organization.

Reporting/Follow Up

Reporting/follow-up phase steps can be broken down into specific activities, as shown in **figure 1.14**.

Figure 1.14—Audit Process Activities for the Reporting/Follow-Up Phase

Audit Step	Description
1. Gather report requirements.	Reporting requirements are identified prior to drafting an audit report. These requirements may be derived from internal audit standards for the organization or through external reporting requirements.
2. Draft report.	A draft report is created and reviewed by information systems (IS) audit leadership prior to review by the auditee. The report includes the overall results of the audit and potential findings and recommendations for management. Prior to issuing a final report, the auditee should review and respond to recommendations identifying planned actions for any recommended remediations.
3. Issue report.	Once a report is finalized, it is issued. The final report is retained per internal or external retention requirements. Audit reports are presented to the oversight function of the organization (e.g., audit committee).
4. Follow up.	A process is established to follow up on management's remediation progress for issues identified during an IS audit.

1.5.3 Audit Programs

An audit program is a step-by-step set of audit procedures and instructions that should be performed to complete an audit. It is based on the scope and objective of the particular assignment.

The main purposes of developing an audit program are:

- Formal documentation of audit procedures and sequential steps
- Creation of procedures that are repeatable and easy to use by internal or external audit and assurance professionals who need to perform similar audits
- Documentation of the type of testing that will be used (compliance and/or substantive)
- Meeting generally accepted audit standards that relate to the planning phase in the audit process

An IS auditor often evaluates IT functions and systems from different perspectives, such as security (confidentiality, integrity and availability), quality

 ©ISACA. All Rights Reserved.

(effectiveness, efficiency), fiduciary (compliance, reliability), service and capacity. The audit work program is the audit strategy and plan—it identifies scope, audit objectives and audit procedures to obtain sufficient, relevant and reliable evidence to draw and support audit conclusions and opinions.

General audit procedures are the basic steps in the performance of an audit and usually include:

- Obtaining and recording an understanding of the audit area/subject
- Creating a risk assessment and general audit plan and schedule
- Performing detailed audit planning that includes the necessary audit steps and a breakdown of the work planned across an anticipated timeline
- Conducting a preliminary review of the audit area/subject
- Evaluating the audit area/subject
- Verifying and evaluating the appropriateness of controls designed to meet control objectives
- Conducting compliance testing (tests of the implementation of controls and their consistent application)
- Conducting substantive testing (confirming the accuracy of information)
- Reporting (communicating results)
- Following up in cases that rely on an internal audit function

Minimum Skills to Develop an Audit Program

The development of meaningful audit and assurance programs depends on the auditor's ability to customize procedures according to the nature of the subject under review and the specific risk that must be addressed in the audit area/organization. Skills that can assist an IS auditor in creating an audit program include:

- Sufficient understanding of the nature of the enterprise and its industry to identify and categorize types of risk and threat
- Good understanding of the IT space and its components and sufficient knowledge of the technologies that affect them
- Understanding of the relationship between business risk and IT risk
- Basic knowledge of risk assessment practices
- Understanding of testing procedures for evaluating IS controls and identifying the best method of evaluation, such as:
  - The use of generalized audit software (GAS) to survey the contents of data files (e.g., system logs, user access list)
  - The use of specialized software to assess the contents of operating systems, databases and application parameter files
  - Flowcharting techniques for documenting business processes and automated controls
  - The use of audit logs and reports to evaluate parameters
  - Review of documentation
  - Inquiry and observations
  - Walk-throughs
  - Reperformance of controls

Note

For additional guidance, see standard 1204 Performance and Supervision and guideline 2204 Performance and Supervision.

1.5.4 Audit Work Papers

All audit plans, programs, activities, tests, findings and incidents should be properly documented in work papers. The format and media of work papers can vary, depending on the specific needs of the department. IS auditors should particularly consider how to maintain the integrity and protection of audit test evidence in order to preserve its value as substantiation in support of audit results.

Work papers can be considered the bridge or interface between the audit objectives and the final report. Work papers should provide a seamless transition—with traceability and support for the work performed—from objectives to report and from report to objectives. In this context, the audit report can be viewed as a particular work paper.

IS auditors should ensure that the same security-related requirements they may be assessing are considered for the audit work papers they collect. IS audit reports and related work papers can contain sensitive information that could be leveraged by malicious actors. A retention and destruction process should be established based on legal requirements for each audit type.

1.5.5 Fraud, Irregularities and Illegal Acts

Management is primarily responsible for establishing, implementing and maintaining an internal control system that enables the deterrence and/or timely detection of fraud. Internal controls may fail due to exploitation of vulnerabilities, management-perpetrated control weaknesses or collusion among people.

©ISACA. All Rights Reserved.

The presence of internal controls does not altogether eliminate fraud. IS auditors should observe and exercise due professional care in all aspects of their work and be alert to opportunities that may allow fraud to materialize. They should be aware of the possibilities and means of perpetrating fraud, especially through exploitation of vulnerabilities and overriding controls in the IT-enabled environment. They should have knowledge of fraud and fraud indicators and be alert to the possibility of fraud and errors while performing an audit.

During the course of regular assurance work, an IS auditor may come across instances or indicators of fraud. After careful evaluation, an IS auditor may communicate the need for a detailed investigation to appropriate authorities. In the case of an IS auditor identifying a major fraud or if the risk associated with the detection is high, audit management should consider communicating the issue to the audit committee in a timely manner.

Regarding fraud prevention, an IS auditor should be aware of potential legal requirements concerning the implementation of specific fraud detection procedures and the reporting of fraud to appropriate authorities.

Note

For additional guidance, see standard 1207 Irregularity and Illegal Acts and guideline 2207 Irregularity and Illegal Acts.

1.5.6 Agile Auditing

A goal for any IS audit function is to provide faster and more efficient ways to conduct an IS audit to demonstrate the value provided to stakeholders. One method to achieve this is leveraging Agile concepts.

Agile Auditing Overview

The term "agile" usually refers to software development and emphasizes individuals and interactions over processes and tools, working software over comprehensive documentation, customer collaboration over contract negotiation and responding to change over following a plan.[8] Traditional IS audit, on the other hand, has used strict standards and frameworks, resulting in rather rigid audit engagement constraints that, essentially, represented projects. IT projects have similarly inflexible models. However, they have evolved from the formal Waterfall model to less formal, but very often more efficient, models that are usually collectively known as "Agile."

In Agile models, design and specification documentation are kept to the bare minimum required, and a major part of documentation is created at the operations and support levels (e.g., user manuals), which occur much later in the system life cycle. In the context of an IS audit, this would result in blurring or altogether abolishing the temporal separation between planning and fieldwork phases. Agile audits, thus, address major bottlenecks in many audits.

For example, necessary data—such as lists of system users from the system itself or an authorization database or file—can be requested and prepared by the auditees while the auditors are still trying to finalize remaining audit program steps. In addition, auditors can analyze data already collected while waiting for the audit team to schedule planning phase meetings with other auditees or the team members. Elimination of the requirement for strict temporal separation between planning and fieldwork makes audit more efficient. Tasks run in parallel (i.e., planning may be going on as the auditees collect requested data, or fieldwork may be occurring while meetings to address remaining planning issues are taking place).

Benefits of Agile Auditing

Agile methodologies benefit audit departments through production of rapid audit results, avoidance of siloed audit and customer teams, communications in near real time and effective collaboration with auditees. Agile also ensures that IT audit engagements are more successful through:

- **Reduced end-to-end planning**—Instead of audit engagements being planned over several months, Agile reduces the planning process to weeks or even days due to condensed sprint cycles and a small-scale, iterative approach.
- **Streamlined audit engagements**—Combining the planning, fieldwork and reporting phases into a single cohesive engagement avoids the execution of disparate audit phases with long lead times.
- **Direct customer collaboration**—Involving customers in the Agile scrum (i.e., daily standup meeting) at the beginning of the audit engagement sprint gives them a seat at the table. This involvement further facilitates their input in guiding the engagement to both valid and highly beneficial audit outcomes for all parties.
- **Flexible audit scope**—As new information is provided to or discovered by auditors, Agile facilitates real-time audit scope adjustments. Auditors should continue to obtain audit management approval

[8] "Manifesto for Agile Software Development," *http://agilemanifesto.org/*

as potential scope adjustments are identified and be prepared to adjust testing focus as new information is discovered or provided by audit customers.

- **Real-time assurance**—Direct customer collaboration means customers are informed of audit findings or control weaknesses as they are discovered by auditors versus receiving a draft audit report toward the end of an audit engagement. Auditors should provide audit customers with updates on potential findings or control weaknesses as testing uncovers them.
- **Frequent audit plan updates**—The increased velocity of engagements produced by Agile IT audits provides an opportunity to revisit the audit backlog and annual plan and make revisions more frequently. Unlike audit plans that are reviewed annually, Agile audit plans are reviewed every quarter (or more frequently in some instances) due to the Agile iterative approach to conducting an audit engagement.

Agile Auditing Compared to Established Assurance Standards

Figure 1.15 shows how Agile complements general, performance and reporting standards and guidelines found in the ISACA ITAF standard. The comparison in **figure 1.15** shows how Agile audit techniques complement adherence to the standard.

Figure 1.15—Complementary Relationship of Agile Audit Techniques and ITAF

ITAF Standard or Guideline Reference	How Agile Complements or Satisfies ITAF
General Standard 1002—Organizational Independence The IT audit and assurance function shall be free from conflicts of interest and undue influence in all matters related to audit and assurance engagements.	• Agile encourages more direct levels of communication and involvement with audit customers, which reflects auditors' organizational independence. • The collaborative approach used in Agile (and facilitated by organizational independence) allows audit to leverage subject matter expertise to allow expedient agreement on audit findings and minimize remediation timelines.
General Standard 1003—Auditor Objectivity IT audit and assurance practitioners shall be objective in all matters related to audit and assurance engagements.	• While differing from the traditional approach to audit, Agile does not compromise auditor objectivity, which may be impaired if conflicts of interest arise. • Agile audit functions retain their professional skepticism and ability to make final decisions throughout the audit engagement.
General Standard 1005—Due Professional Care Auditors will exercise due diligence and professional care. They will maintain high standards of conduct and character, and they will refrain from engaging in acts that may discredit themselves or the profession. Privacy and confidentiality of information obtained during the course of the auditor's duties should be maintained.	• The audit backlog is prioritized more often under Agile, which considers the required resources, establishment of proper audit scope, proper audit objectives and adequate levels of diligence and discretion. • With Agile, audit management retains its right to conclude on key matters of each audit engagement.
General Standard 1006—Proficiency IT audit and assurance practitioners, collectively with others assisting with the audit and assurance engagement, shall possess the professional competence to perform the work required.	• Daily standup scrum meetings and two-week sprint cycles greatly enhance development of audit staff at the junior and senior levels. • Increased collaboration with audit customers allows audit staff to learn the business more completely.
Reporting Standard 1402.3—Follow-Up Activities and Acceptance of Risk Where it is determined that the risk related to a finding has been accepted and is greater than the enterprise's risk appetite, this risk acceptance should be discussed with senior management.	• The collaborative and frequent communication processes leveraged by Agile seek to ensure full disclosure to executive management of any accepted risk taken by audit customers.

©ISACA. All Rights Reserved.

Figure 1.15—Complementary Relationship of Agile Audit Techniques and ITAF (cont.)

ITAF Standard or Guideline Reference	How Agile Complements or Satisfies ITAF
General Guideline 2001.2.6—Performance of Quality Assurance (QA) Accountability of the audit and assurance function includes but is not limited to the QA Process (e.g., interviews, customer satisfaction surveys, assignment performance surveys) that establishes an understanding of the auditees' needs and expectations relevant to the audit function.	• The Agile sprint retrospective is a tool the audit team uses to analyze how the last sprint delivered with regard to individuals, interactions among customers and the audit team, executed processes, audit tools and the definition of "done."

Source: ISACA, *Destination: Agile Auditing*, USA, 2021

1.6 Audit Testing and Sampling Methodology

Valid conclusions can be reached using audit sampling. When using either statistical or nonstatistical sampling methods, IS auditors should design and select an audit sample, perform audit procedures and evaluate sample results to obtain sufficient and appropriate evidence to form a conclusion. When using sampling methods to draw a conclusion about the entire population, professionals should use statistical sampling.

An IS auditor should consider the purpose of the sample:

- **Compliance testing/test of controls**—An audit procedure designed to evaluate the operating effectiveness of controls in preventing, or detecting and correcting, material weaknesses
- **Substantive testing/test of details**—An audit procedure designed to detect material weaknesses at the assertion level

1.6.1 Compliance Versus Substantive Testing

Compliance testing is evidence gathering for the purpose of testing an organization's compliance with control procedures. This differs from substantive testing, in which evidence is gathered to evaluate the integrity of individual transactions, data or other information.

A compliance test determines whether controls are being applied in a manner that complies with management policies and procedures. For example, if an IS auditor is concerned about whether production program library controls are working properly, the IS auditor might select a sample of programs to determine whether the source and object versions are the same. The broad objective of any compliance test is to provide reasonable assurance of a particular control as perceived in the preliminary evaluation.

It is important that an IS auditor understands the specific objective of a compliance test and of the control being tested. Compliance tests can be used to test the existence and effectiveness of a defined process, which may include a trail of documentary and/or automated evidence (e.g., to provide assurance that only authorized modifications are made to production programs).

A substantive test substantiates the integrity of actual processing. It provides evidence of the validity and integrity of the balances in the financial statements and the transactions that support those balances. An IS auditor could use substantive tests to check for monetary errors directly affecting financial statement balances or other relevant data of the organization. Additionally, an IS auditor might develop a substantive test to evaluate the completeness and accuracy of report data. To perform this test, the IS auditor might use a statistical sample, which will allow the IS auditor to develop a conclusion regarding the accuracy of all the data.

A direct correlation exists between the level of internal controls and the amount of substantive testing required. If the results of testing controls (compliance tests) reveal the presence of adequate internal controls, then minimizing the substantive procedures could be justified. Conversely, if the control testing reveals weaknesses in controls that may raise doubts about the completeness, accuracy or validity of the accounts, substantive testing can alleviate those doubts.

Examples of compliance testing of controls where sampling could be considered include user access rights, program change control procedures, documentation procedures, program documentation, follow-up of exceptions, review of logs and software license audits.

Examples of substantive tests where sampling could be considered include performance of a complex calculation (e.g., interest) on a sample of accounts or a sample of transactions to vouch for supporting documentation.

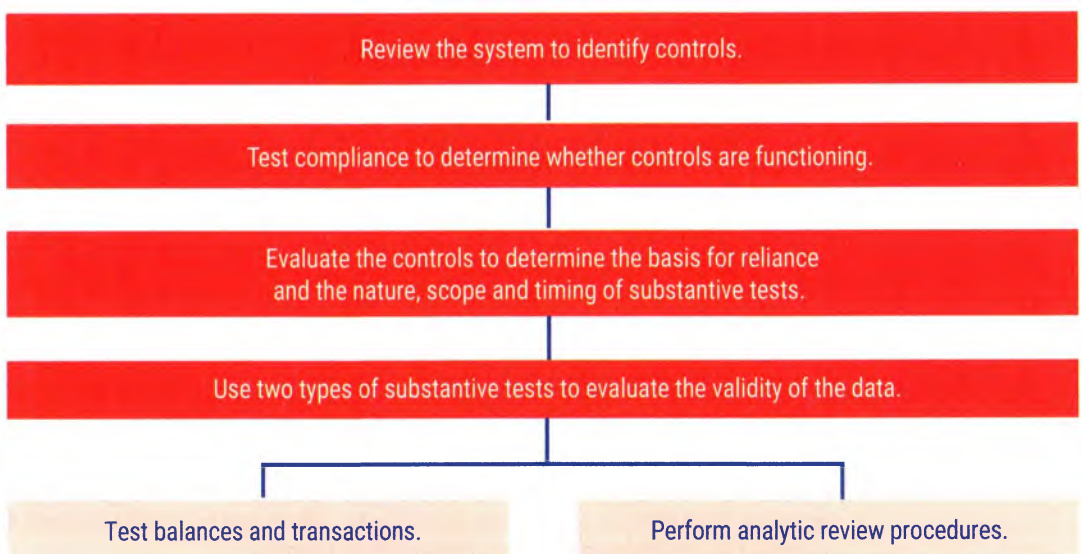
An IS auditor could decide during the preliminary assessment of the controls to include some substantive testing if the results of the preliminary evaluation indicate that implemented controls are not reliable or do not exist.

Figure 1.16 shows the relationship between compliance and substantive tests and describes the two categories of substantive tests.

Note

A CISA candidate should be knowledgeable about when to perform compliance tests or substantive tests.

Figure 1.16—Understand the Control Environment and Flow of Transactions



1.6.2 Sampling

Sampling is performed when time and cost considerations preclude a total verification of all transactions or events in a predefined population. The population consists of the entire group of items that need to be examined. The subset of population members used to perform testing is called a sample. Sampling is used to infer characteristics about a population based on the characteristics of a sample.

The two general approaches to audit sampling are statistical and nonstatistical:

- **Statistical sampling**—An objective method of determining the sample size and selection criteria
  - Statistical sampling uses the mathematical laws of probability to: (1) calculate the sampling size, (2) select the sample items and (3) evaluate the sample results and make inferences.
  - With statistical sampling, an IS auditor quantitatively decides how closely the sample should represent the population (assessing sample precision) and the number of times in 100 that the sample should represent the population (the reliability or confidence level). This assessment is represented as a percentage. The results of a valid statistical sample are mathematically quantifiable.
- **Nonstatistical sampling (often referred to as judgmental sampling)**—Uses audit judgment to determine the method of sampling, the number of items that will be examined from a population (sample size) and which items to select (sample selection)
  - These decisions are based on subjective judgment as to which items/transactions are the most material and most risky.

The IS auditor should be familiar with the statistical sampling concepts described in **figure 1.17**.

When using either statistical or nonstatistical sampling methods, an IS auditor should design and select an audit sample, perform audit procedures and evaluate sample results to obtain sufficient, reliable, relevant

©ISACA. All Rights Reserved.

and useful audit evidence. These methods of sampling require an IS auditor to use judgment when defining the population characteristics and, thus, are subject to the risk that incorrect conclusions could be drawn from the sample (sampling risk). However, statistical sampling permits an IS auditor to quantify the probability of error (confidence coefficient). To be a statistical sample, each item in the population should have an equal opportunity or probability of being selected. Within these two general approaches to audit sampling, there are two primary methods of sampling used—attribute sampling and variable sampling. Attribute sampling, generally applied in compliance testing, deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence.

Figure 1.17—Statistical Sampling Terminology

Term	Definition
Confidence coefficient (confidence level or reliability factor)	A percentage expression (90 percent, 95 percent, 99 percent, etc.) of the probability that the characteristics of the sample are a true representation of the population. Generally, a 95 percent confidence coefficient is considered a high degree of assurance. If an information systems (IS) auditor knows internal controls are strong, the confidence coefficient may be lowered. The greater the confidence coefficient, the larger the sample size.
Level of risk	Equal to one minus the confidence coefficient. For example, if the confidence coefficient is 95 percent, the level of risk is five percent (100 percent minus 95 percent).
Precision	Set by an IS auditor, the acceptable range difference between the sample and the actual population. For attribute sampling, this figure is stated as a percentage. For variable sampling, this figure is stated as a monetary amount or a number. The higher the precision amount, the smaller the sample size and the greater the risk of fairly large total error amounts going undetected. The smaller the precision amount, the greater the sample size. A very low precision level may lead to an unnecessarily large sample size.
Expected error rate	An estimate stated as a percentage of the errors that may exist. The greater the expected error rate, the greater the sample size. This figure is applied to attribute sampling formulas but not to variable sampling formulas.
Sample mean	The sum of all sample values divided by the size of the sample. The sample mean measures the average value of the sample.
Sample standard deviation	The variance of the sample values from the mean of the sample. Sample standard deviation represents the spread or dispersion of the sample values.
Tolerable error rate	Describes the maximum misstatement or number of errors that can exist without an account being materially misstated. Tolerable rate is used for the planned upper limit of the precision range for compliance testing. The term is expressed as a percentage. "Precision range" and "precision" have the same meaning when used in substantive testing.
Population standard deviation	A mathematical concept that measures the relationship to the normal distribution. The greater the standard deviation, the larger the sample size. This figure is applied to variable sampling formulas but not to attribute sampling formulas.

Attribute sampling refers to three different, but related, types of proportional sampling:

- **Attribute sampling (fixed sample-size attribute sampling or frequency-estimating sampling)**—A sampling model used to estimate the rate (percent) of occurrence of a specific quality (attribute) in a population. Attribute sampling answers the question, "How many?"
  - An example of an attribute that might be tested is approval signatures on computer access request forms.
- **Stop-or-go sampling**—A sampling model that helps prevent excessive sampling of an attribute by allowing an audit test to be stopped at the earliest possible moment. Stop-or-go sampling is used when

an IS auditor believes that relatively few errors will be found in a population.

- **Discovery sampling**—A sampling model most often used when the objective of the audit is to seek out (discover) fraud, circumvention of regulations or other irregularities. For example, if the sample is found to be error free, it is assumed that no fraud/irregularity exists; however, if a single error is found, the entire sample is believed to be fraudulent/irregular.

Variable sampling (dollar estimation or mean estimation sampling) is a technique used to estimate the monetary value or some other unit of measure (such as weight) of a population from a sample portion. An example of variable sampling is a review of an organization's balance sheet for material transactions and an application review of the program that produced the balance sheet.

Variable sampling refers to three types of quantitative sampling models:

- **Stratified mean per unit**—A statistical model in which the population is divided into groups and samples are drawn from the various groups; used to produce a smaller overall sample size relative to unstratified mean per unit
- **Unstratified mean per unit**—A statistical model in which a sample mean is calculated and projected as an estimated total
- **Difference estimation**—A statistical model used to estimate the total difference between audited values and book (unaudited) values based on differences obtained from sample observations

Variable sampling, generally applied in substantive testing, deals with population characteristics that vary, such as monetary values and weights (or any other measurement), and provides conclusions related to deviations from the norm.

Key steps in the construction and selection of a sample for an audit test are shown in **figure 1.18**.

Figure 1.18—Steps in the Selection of a Sample for an Audit Test



Sampling Risk

Sampling risk arises from the possibility that an IS auditor's conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure. There are two types of sampling risk:

- **The risk of incorrect acceptance**—A material weakness is assessed as unlikely when, in fact, the population is materially misstated.
- **The risk of incorrect rejection**—A material weakness is assessed as likely when, in fact, the population is not materially misstated.

Note

A CISA candidate is not expected to be a sampling expert. However, a CISA candidate should have a foundational understanding of the general principles of sampling and how to design a sample that is reliable. A CISA candidate should also be familiar with the different types of sampling terms and techniques and know when it is appropriate to use each technique.

1.7 Audit Evidence Collection Techniques

Evidence is any information used by an IS auditor to determine whether the entity or data being audited follows the established criteria or objectives and supports audit conclusions. It is a requirement that conclusions be based on sufficient, relevant and competent evidence.

©ISACA. All Rights Reserved.

When planning the IS audit, the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability should be considered.

Audit evidence may include:
- An IS auditor's observations (presented to management)
- Notes taken from interviews
- Results of independent and qualified third-party assessors
- Material extracted from correspondence and internal documentation or contracts with external partners
- The results of audit test procedures

While all evidence will assist an IS auditor in developing audit conclusions, some types of evidence are more reliable than others. The rules of evidence and sufficiency and the competency of evidence must be considered as required by audit standards.

Determinants for evaluating the reliability of audit evidence include:
- **Independence of the provider of the evidence**—Evidence obtained from outside sources is more reliable than evidence from within the organization. This is why confirmation letters are used for verification of accounts receivable balances. Additionally, signed contracts or agreements with external parties can be considered reliable if the original documents are made available for review.
- **Qualifications of the individual providing the information/evidence**—Whether the providers of the information/evidence are inside or outside of the organization, an IS auditor should always consider the qualifications and functional responsibilities of the persons providing the information. This can also be true of an IS auditor. If an IS auditor does not have a good understanding of the technical area under review, the information gathered from testing that area may not be reliable, especially if the IS auditor does not fully understand the test.
- **Objectivity of the evidence**—Objective evidence is more reliable than evidence that requires considerable judgment or interpretation. An IS auditor's review of media inventory is direct, objective evidence. An IS auditor's analysis of the efficiency of an application, based on discussions with certain personnel, may not be objective audit evidence.
- **Timing of the evidence**—An IS auditor should consider the time during which information exists or is available in determining the nature, timing and extent of compliance testing and, if applicable, substantive testing. For example, audit evidence processed by dynamic systems, such as spreadsheets, may not be retrievable after a specified period of time if changes to the files are not controlled or the files are not backed up.

An IS auditor gathers a variety of evidence during an audit. Some evidence may be relevant to the objectives of the audit, while other evidence may be considered peripheral. An IS auditor should focus on the overall objectives of the review and not the nature of the evidence gathered.

The quality and quantity of evidence must be assessed. These two characteristics are referred to by the International Federation of Accountants (IFAC) as appropriate (quality) and sufficient (quantity). Evidence is competent when it is both reliable and relevant. Audit judgment is used to determine when sufficiency is achieved in the same manner that it is used to determine the appropriateness of evidence.

An understanding of the rules of evidence is important for IS auditors because they may encounter a variety of evidence types.

Note

A CISA candidate, given an audit scenario, should be able to determine which evidence-gathering technique would be best in a given situation.

Techniques for gathering evidence include:
- **Reviewing IS organization structures**—An organizational structure that provides adequate SoD is a key general control in an IS environment. An IS auditor should understand general organizational controls and be able to evaluate those controls in the organization under audit. Where there is a strong emphasis on cooperative distributed processing or on end-user computing, IT functions may be organized somewhat differently from the classic IS organization, which consists of separate systems and operations functions. An IS auditor should be able to review organizational structures and assess the level of control they provide.
- **Reviewing IS policies and procedures**—An IS auditor should review whether appropriate policies and procedures are in place, determine whether personnel understand the implemented policies and procedures and ensure that policies and procedures are being followed. An IS auditor should verify that management assumes full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims

and directives. Periodic reviews of policies and procedures for appropriateness should be carried out.

- **Reviewing IS standards**—An IS auditor should first understand the existing standards in place within the organization.
- **Reviewing IS documentation**—A first step in reviewing the documentation for an information system is to understand the existing documentation in place within the organization. This documentation could be a hard copy or a copy stored electronically. If the latter, controls to preserve the document integrity should be evaluated by an IS auditor. An IS auditor should look for a minimum level of IS documentation. Documentation may include:
  - Systems development initiating documents (e.g., feasibility studies)
  - Documentation provided by external application suppliers
  - SLAs with external IT providers
  - Functional requirements and design specifications
  - Tests plans and reports
  - Program and operations documents
  - Program change logs and histories
  - User manuals
  - Operations manuals
  - Security-related documents (e.g., security plans, risk assessments)
  - BCPs
  - QA reports
  - Reports on security metrics
- **Interviewing appropriate personnel**—See section 1.7.1 Interviewing and Observing Personnel in Performance of Their Duties.
- **Observing processes and employee performance**—The observation of processes is a key audit technique for many types of review. An IS auditor should be unobtrusive while making observations and should document everything in sufficient detail to be able to present it, if required, as audit evidence. In some situations, the release of the audit report may not be timely enough to use observations as evidence, which may necessitate the issuance of an interim report to management of the area being audited. An IS auditor may wish to consider whether documentary evidence would be useful as evidence (e.g., photograph of a server room with doors fully opened).
- **Reperformance**—The reperformance process is a key audit technique that generally provides better evidence than the other techniques and is, therefore, used when a combination of inquiry, observation and examination of evidence does not provide sufficient assurance that a control is operating effectively. This technique involves the actual performance of the control under assessment in real time.
- **Walk-throughs**—The walk-through is an audit technique to confirm the understanding of controls. A walkthrough can help ensure the control owner and IS auditor clearly understand the controls to be assessed and assist in the identification of evidence to be collected to validate control effectiveness.

While these evidence-gathering techniques are part of an audit, an audit is not limited to review work. It includes examination, which incorporates the testing of controls and audit evidence and, therefore, includes the results of audit tests.

An IS auditor should recognize that with systems development techniques, such as computer-aided software engineering (CASE) or prototyping, traditional systems documentation will not be required or will be provided in an automated form. However, an IS auditor should look for documentation standards and practices within the IS organization.

An IS auditor should be able to review documentation for a given system and determine whether it follows the organization's documentation standards. In addition, an IS auditor should understand the current approaches to developing systems—such as object orientation, CASE tools or prototyping—and how the documentation is constructed. An IS auditor should recognize other components of IS documentation, such as database specifications, file layouts or self-documented program listings.

1.7.1 Interviewing and Observing Personnel in Performance of Their Duties

Interviewing techniques are an important skill for an IS auditor. Interviews should be organized in advance with objectives clearly communicated, follow a fixed outline and be documented by interview notes. Using an interview form or checklist prepared by an IS auditor is a good approach.

Remember that the purpose of such an interview is to gather audit evidence using techniques, such as inquiry, observation, inspection, confirmation, performance and monitoring. Personnel interviews are discoveries by nature and should never be accusatory; the interviewer should help people feel comfortable, encouraging them to share information, ideas, concerns and knowledge. An IS auditor should verify the accuracy of the notes with the interviewee.

©ISACA. All Rights Reserved.

Observing personnel in the performance of their duties assists an IS auditor in identifying:

- **Actual functions**—Observation can be an adequate test to ensure that the individual who is assigned and authorized to perform a particular function is the person who is actually doing the job. It allows an IS auditor an opportunity to witness how policies and procedures are understood and practiced. Depending on the specific situation, the results of this type of test should be compared with the respective logical access rights.
- **Actual processes/procedures**—Performing a walk-through of the process/procedure allows an IS auditor to obtain evidence of compliance and observe deviations, if any. This type of observation can prove useful for physical controls.
- **Security awareness**—Security awareness should be observed to verify an individual's understanding and practice of good preventive and detective security measures to safeguard the enterprise's assets and data. This type of information can be supported with an examination of previous and planned security training.
- **Reporting relationships**—Reporting relationships should be observed to ensure that assigned responsibilities and adequate SoD are being practiced. Often, the results of this type of test should be compared with the respective logical access rights.
- **Observation drawbacks**—The observer may interfere with the observed environment. Personnel, upon noticing that they are being observed, may change their usual behavior. Interviewing information processing personnel and management should provide adequate assurance that the staff has the required technical skills to perform the job. This is an important factor that contributes to an effective and efficient operation.

1.8 Audit Data Analytics

Data analytics is an important tool for an IS auditor. Through the use of technology, an IS auditor can select and analyze full data sets to continuously audit or monitor key organizational data for abnormalities or variances that can be used to identify and evaluate organizational risk and achieve compliance with control and regulatory requirements.

An IS auditor can use data analytics to:

- Determine the operational effectiveness of the current control environment
- Determine the effectiveness of antifraud procedures and controls
- Identify business process errors
- Identify business process improvements and inefficiencies in the control environment
- Identify exceptions or unusual business rules
- Identify fraud
- Identify areas where poor data quality exists
- Conduct a risk assessment at the planning phase of an audit

The process used to collect and analyze data includes:

- Setting the scope (e.g., determining audit/review objectives; defining data needs, sources and reliability)
- Identifying and obtaining the data (e.g., requesting data from responsible sources, testing a sample of data, extracting the data for use)
- Validating the data (e.g., determining if the data is sufficient and reliable to perform audit tests) by:
  - Validating balances independent of the data set extracted
  - Reconciling detailed data to report control totals
  - Validating numeric, character and date fields
  - Verifying the time period of the data set (i.e., determining that it meets scope and purpose)
  - Verifying that all necessary fields identified in the scope are actually included in the acquired data set
- Executing the tests (e.g., running scripts and performing other analytical tests)
- Documenting the results (e.g., recording the testing purpose, data sources and conclusions reached)
- Reviewing the results (e.g., ensuring that the testing procedures have been adequately performed and reviewed by a qualified person)
- Retaining the results (e.g., maintaining important test elements), such as:
  - Program files
  - Scripts
  - Macros/automated command tests
  - Data files

Data analytics can be effective for an IS auditor in both the planning and fieldwork phases of an audit.

Analytics can be used to:

- Combine logical access files with human resources employee master files for authorized users
- Combine file library settings with data from the change management systems and dates of file changes that can be matched to dates of authorized events
- Match ingress with egress records to identify tailgating in physical security logs
- Review table or system configuration settings
- Review system logs for unauthorized access or unusual activities

 ©ISACA. All Rights Reserved.

- Test system conversion
- Test logical access SoD (e.g., analysis of Active Directory data combined with job descriptions)

1.8.1 Computer-Assisted Audit Techniques

CAATs are important tools that an IS auditor uses to gather and analyze data during an IS audit or review. When systems have different hardware and software environments, data structures, record formats or processing functions, it is almost impossible for an IS auditor to collect certain evidence without using such a software tool.

CAATs also enable an IS auditor to gather information independently. They provide a means to gain access and analyze data for a predetermined audit objective and to report the audit findings with emphasis on the reliability of the records produced and maintained in the system. The reliability of the source of the information used provides reassurance on findings generated.

CAATs include many types of tools and techniques such as GAS, utility software, debugging and scanning software, test data, application software tracing and mapping and expert systems.

GAS refers to standard software that can directly read and access data from various database platforms, flat-file systems and American Standard Code for Information Interchange (ASCII) formats. GAS provides an IS auditor with an independent means to gain access to data for analysis and the ability to use high-level, problem-solving software to invoke functions to be performed on data files. Features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recomputations. Functions commonly supported by GAS include:

- **File access**—Enables the reading of different record formats and file structures
- **File reorganization**—Enables indexing, sorting, merging and linking with another file
- **Data selection**—Enables global filtration conditions and selection criteria
- **Statistical functions**—Enables sampling, stratification and frequency analysis
- **Arithmetical functions**—Enables arithmetic operators and functions

Utility software is a subset of software—such as report generators of the database management system (DBMS)—that provides evidence about system control effectiveness. Test data involves an IS auditor using a sample set of data to assess whether logic errors exist in a program and whether the program meets its objectives. The review of an application system will provide information about internal controls built into the system. The audit-expert system will provide direction and valuable information to all levels of auditors while carrying out the audit because the query-based system is built on the knowledge base of senior auditors or managers.

Utility software tools and techniques can be used in performing various audit procedures such as:

- Tests of the details of transactions and balances
- Analytical review procedures
- Compliance tests of IS general controls
- Compliance tests of IS application controls
- Network and OS vulnerability assessments
- Penetration testing
- Application security testing and source code security scans

An IS auditor should have a thorough understanding of CAATs and know where and when to apply them. For example, an IS auditor should review the results of engagement procedures to determine whether there are indications that irregularities or illegal acts may have occurred. Using CAATs could aid significantly in the effective and efficient detection of irregularities or illegal acts.

An IS auditor should weigh the costs and benefits of using CAATs before going through the effort, time and expense of purchasing or developing them. Issues to consider include:

- Ease of use for existing and future audit staff
- Training requirements
- Complexity of coding and maintenance
- Flexibility of uses
- Installation requirements
- Processing efficiencies
- Effort required to bring the source data into the CAATs for analysis
- Ensuring the integrity of imported data by safeguarding its authenticity
- Recording the time stamp of data downloaded at critical processing points to sustain the credibility of the review
- Obtaining permission to install the software on the auditee servers
- Reliability of the software
- Confidentiality of the data being processed

When developing CAATs, the following are examples of documentation to be retained:

- Online reports detailing high-risk issues for review

©ISACA. All Rights Reserved.

- Commented program listings
- Flowcharts
- Sample reports
- Record and file layouts
- Field definitions
- Operating instructions
- Description of applicable source documents

CAATs documentation should be referenced to the audit program and clearly identify the audit procedures and objectives being served. When requesting access to production data for use with CAATs, an IS auditor should request read-only access. Any data manipulation by an IS auditor should be applied to copies of production files in a controlled environment to ensure that production data is not exposed to unauthorized updating. Most CAATs allow for production data to be downloaded from production systems to a standalone platform and then analyzed from the standalone platform, thereby insulating the production systems from any adverse impact.

CAATs as a Continuous Online Audit Approach

An important advantage of CAATs is the ability to improve audit efficiency through continuous online auditing techniques. To this end, an IS auditor must develop audit techniques that are appropriate for use with advanced information systems.

In addition, the IS auditor must be involved in the creation of advanced systems at the early stages of development and implementation and must make greater use of automated tools that are suitable for the organization's automated environment. This takes the form of the continuous audit approach.

1.8.2 Continuous Auditing and Monitoring

Continuous auditing is an approach used by IS auditors to monitor system reliability on a continuous basis and gather selective audit evidence through the computer. A distinctive characteristic of continuous auditing is the short time lapse between the facts to be audited, the collection of evidence and audit reporting. To properly understand the implications and requirements of continuous auditing, a distinction is made between continuous auditing and continuous monitoring:

- **Continuous auditing**—Enables an IS auditor to perform tests and assessments in a real-time or near-real-time environment. Continuous auditing is designed to enable an IS auditor to report results on the subject matter being audited within a much shorter time frame than under a traditional audit approach.
- **Continuous monitoring**—Enables an organization to observe the performance of one or many processes, systems or types of data. For example, real-time antivirus or intrusion detection systems may operate in a continuous monitoring fashion.

Continuous auditing should be independent of continuous control or monitoring activities. When both continuous monitoring and auditing take place, continuous assurance can be established. In practice, continuous auditing is the precursor to management adopting continuous monitoring as a process on a day-to-day basis. Often, the audit function will hand over the techniques used in continuous auditing to the business, which will then run the continuous monitoring. This collaboration has led to increased appreciation among process owners of the value that the audit function brings to the organization, leading to greater confidence and trust between the business and the audit function. Nevertheless, the lack of independence and objectivity inherent in continuous monitoring should not be overlooked, and continuous monitoring should never be considered as a substitute for the audit function.

Continuous auditing efforts often incorporate new IT developments; increased processing capabilities of current hardware, software, standards and AI tools; and attempts to collect and analyze data at the moment of the transaction. Data must be gathered from different applications working within different environments, transactions must be screened, the transaction environment has to be analyzed to detect trends and exceptions, and atypical patterns (i.e., a transaction with significantly higher or lower value than typical for a given business partner) must be exposed. If all this must happen in real time, perhaps even before final sign-off of a transaction, it is mandatory to adopt and combine various top-level IT techniques. The IT environment is a natural enabler for the application of continuous auditing because of the intrinsic automated nature of its underlying processes.

Continuous auditing aims to provide a more secure platform to avoid fraud and a real-time process aimed at ensuring a high level of financial control. Continuous auditing and monitoring tools are often built into many enterprise resource planning packages and most OS and network security packages. These environments, if appropriately configured and populated with rules, parameters and formulas, can output exception lists on request while operating against actual data. Therefore, they represent an instance of continuous auditing. The difficulty, but significant added value, of using these features is that they postulate a definition of what would

be a "dangerous" or exception condition. For example, whether a set of granted IS access permissions is to be deemed risk-free will depend on having well-defined SoD. On the other hand, it may be much harder to decide if a given sequence of steps taken to modify and maintain a database record points to a potential risk.

It is important to validate the source of the data used for continuous auditing and note the possibility of manual changes.

1.8.3 Continuous Auditing Techniques

Continuous auditing techniques are important IS audit tools, particularly when they are used in time-sharing environments that process a large number of transactions but leave a scarce paper trail. By permitting an IS auditor to evaluate operating controls on a continuous basis without disrupting the organization's usual operations, continuous auditing techniques improve the security of a system. When a system is misused by someone withdrawing money from an inoperative account, a continuous auditing technique will report this withdrawal in a timely fashion to an IS auditor. Thus, the time lag between the misuse of the system and the detection of that misuse is reduced. The realization that failures, improper manipulation and lack of controls will be detected on a timely basis by the use of continuous auditing procedures gives an IS auditor and management greater confidence in a system's reliability.

There are five types of automated evaluation techniques applicable to continuous auditing:

1. **Systems control audit review file and embedded audit modules (SCARF/EAM)**—The use of this technique involves embedding specially written audit software in the organization's host application system so the application systems are monitored on a selective basis.
2. **Snapshots**—This technique involves taking what might be termed "pictures" of the processing path that a transaction follows, from the input to the output stage. With the use of this technique, transactions are tagged by applying identifiers to input data and recording selected information about what occurs for an IS auditor's subsequent review.
3. **Audit hooks**—This technique involves embedding hooks (e.g., logging and monitoring triggers) in application systems to function as red flags and induce IS security and auditors to act before an error or irregularity gets out of hand.
4. **Integrated test facility (ITF)**—With this technique, dummy entities are set up and included in an auditee's production files. An IS auditor can make the system either process live transactions or test transactions during regular processing runs and have the transactions update the records of the dummy entity. The operator enters the test transactions simultaneously with the live transactions that are entered for processing. An auditor then compares the output with the data that has been independently calculated to verify the correctness of the computer-processed data.
5. **Continuous and intermittent simulation (CIS)**—During a process run of a transaction, the computer system simulates the instruction execution of the application. As each transaction is entered, the simulator decides whether the transaction meets certain predetermined criteria and, if so, audits the transaction. If not, the simulator waits until it encounters the next transaction that meets the criteria.

In **figure 1.19**, the relative use cases of the various continuous auditing tools are presented.

Figure 1.19—Continuous Auditing Tools—Use Cases

	SCARF/EAM	Snapshots	Audit Hooks	ITF	CIS
Complexity	**Very high**	**Medium**	**Low**	**High**	**Medium**
Useful when:	Regular processing cannot be interrupted.	An audit trail is required.	Only select transactions or processes need to be examined.	It is not beneficial to use test data.	Transactions meeting certain criteria need to be examined.

The use of each of the continuous auditing techniques has advantages and disadvantages. Their selection and implementation depend, to a large extent, on the complexity of an organization's computer systems and

©ISACA. All Rights Reserved.

applications and an IS auditor's ability to understand and evaluate the system with and without the use of continuous auditing techniques. In addition, an IS auditor must recognize that continuous auditing techniques are not a cure for all control problems and that the use of these techniques provides only limited assurance that the information processing systems examined are operating as they were intended to function.

Techniques that are used to operate in a continuous auditing environment must work at all data levels—single input, transaction and databases—and include:

- Transaction logging
- Query tools
- Statistics and data analysis
- DBMSs
- Data warehouses, data marts, data mining
- Intelligent agents
- EAM
- Neural network technologies
- Standards such as Extensible Business Reporting Language (XBRL)

Intelligent software agents may be used to automate the evaluation processes and allow for flexibility and dynamic analysis capabilities. The configuration and application of intelligent agents (bots) allow for continuous monitoring of systems settings and the delivery of alert messages when certain thresholds are exceeded or certain conditions are met.

Full continuous auditing processes have to be carefully built into applications and work in layers. The auditing tools must operate in parallel with normal processing—capturing real-time data, extracting standardized profiles or descriptors and passing the result to the auditing layers.

Continuous auditing has an intrinsic edge over point-in-time or periodic auditing because it captures internal control problems as they occur, preventing negative effects. Implementation can also reduce possible or intrinsic audit inefficiencies such as delays, planning time, inefficiencies of the audit process, overhead due to work segmentation, multiple quality or supervisory reviews or discussions concerning the validity of findings.

Full top management support, dedication and extensive experience and technical knowledge are all necessary to accomplish continuous auditing, while minimizing the impact on the underlying audited business processes. The auditing layers and settings may also need continual adjustment and updating.

Besides difficulty and cost, continuous auditing has an inherent disadvantage in that internal control experts and auditors might be hesitant to trust an automated tool in lieu of their personal judgment and evaluation. Also, mechanisms have to be put in place to eliminate false negatives and false positives in the reports generated by such audits so that the report generated continues to inspire stakeholders' confidence in its accuracy.

1.8.4 Artificial Intelligence in IS Audit

Artificial intelligence (AI) is increasingly being used in many business functions. Detecting fraudulent transactions, performing data quality checks, screening for negative news and data processing have all been successfully automated via AI/machine learning (ML) techniques. Implementing AI or ML for large multinational corporate banks leads to big savings in manual overhead and reconciliation efforts.

IS auditors may benefit from using AI/ML techniques to increase overall audit efficiency or decrease audit risk. Efficiency can be gained through automating tedious manual processes like audit work paper markups or data manipulation. Audit risk may be decreased through the ability to increase audit sample sizes or provide auditors with more time and information to analyze audit results for further testing and follow up.

Figure 1.20 outlines specific tasks and automation opportunities for AI/ML in IS audit.

 ©ISACA. All Rights Reserved.

Figure 1.20—The Role of RPA and AI Within the Audit Life Cycle



Source: Menon, S.; "How Can AI Drive Audits?," *ISACA Journal*, vol. 4, 30 June 2021, *https://www.isaca.org/resources/isaca-journal/issues/2021/volume-4/how-can-ai-drive-audits*

Audit Algorithms

It is important for practitioners, specifically IS auditors, to understand what algorithms are and why they matter, that smart algorithms are not new, and that humans have a decisive role in algorithm design and metrics. It is the auditor's job to ask questions using the correct tools, interpret results and remember that errors are possible even with the most advanced algorithms.

Algorithms as a concept are often associated with mathematics or computer science, which can make them seem intimidating and difficult to understand. However, algorithms are simply ways to solve a specific problem. For example, babies cry when they need nourishment, pain management or attention. An algorithm can be as simple as "If hungry, then cry."[9] Algorithms are used to solve everyday problems—from cooking to driving to troubleshooting to diagnosing a medical condition.

[9] Alexiou, S.; "Algorithms and the Auditor," *ISACA Journal*, vol. 6, 23 November 2021, *https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/algorithms-and-the-auditor*

©ISACA. All Rights Reserved.

Algorithms can be simple or complex, and not all algorithms are effective. Some are more suited to solving a problem than others. The feasibility of using technological advancements, such as AI, is dependent on finding an efficient algorithm that makes computations fast.[10] An example is homomorphic encryption, which enables the manipulation of encrypted data without the need to convert it to cleartext first.[11]

Audits can be considered similarly. For example, audits include checking a current state (as is) versus the desired state (as should be). These checks direct an algorithm to:[12]

- Obtain the "as is" and "as should be" versions.
- Perform whatever operations are needed to enable a comparison.
- Perform the comparison.
- Assess the results and their significance.

A complete algorithm involves a detailed prescription of all the general tasks and how to perform each subtask.[13] Regardless of the complexity, an algorithm is just one way to tackle a problem, and it is important to review and adapt algorithms as changes and needs dictate.

Figure 1.21 further expands on specific applications and use cases for AI/ML techniques in IS audit.

Figure 1.21—Suggested AI/ML Techniques for Use in Auditing

AI or ML Techniques	Application/Use Cases	Usage
Document classification	Application of classification models (e.g., decision trees, Bayesian classifiers, nearest neighbors) to assign documents or text segments to a specific topic or label	• Understanding standard operating procedures, policies and other deliverables reviewed during auditing • Making inferences from previous similar audit reports
Text summarization	The process of combining frequently used words, phrases and topics to generate a natural language summary of a text or a document set	• Generating audit observations and inferences • Auto-generating audit checklists
Topic analysis	Analysis performed across documents, groups of documents or document texts to identify unique topics that link documents or sections of documents	• Analyzing data • Building keyword rule engine for audits
Search and retrieval	The process of searching a database or repository of processed information to retrieve documents that align with the topics or themes entered in the search criteria	• Making similar audit report inferences
Statistical analysis	A basic statistical analysis technique that evaluates term, phrase or topic trends	• Aggregating data • Interpreting data
Sentiment analysis	The ability to extract and analyze text or groups of text in documents to understand author sentiments	• Identifying key issues and risk • Making intelligent inferences and preparing audit reports

Source: Menon, S.; "How Can AI Drive Audits?," *ISACA Journal*, vol. 4, 30 June 2021, *https://www.isaca.org/resources/isaca-journal/issues/2021/volume-4/how-can-ai-drive-audits*

Interpretation of AI/ML Results

AI/ML results should always be interpreted at some point by a person. IS auditors must ensure that testing is designed to answer the question of whether a tool being used is able to answer the question that the auditor is asking. Specific factors to consider include:[14]

- Data inputs must be validated as part of the AI/ML assisted audit process upon implementation and periodically. The use of the AI/ML tool will be

[10] *Ibid.*
[11] Armknecht, F.; C. Boyd; C. Carr et al.; "A Guide to Fully Homomorphic Encryption," 2015, *https://eprint.iacr.org/2015/1192.pdf*
[12] *Op cit* Alexiou
[13] *Ibid.*
[14] *Ibid.*

useless if the data being ingested or analyzed is not complete and accurate. When possible, the IS auditor should ensure raw system data may be obtained for analysis and checking of AI/ML tool conclusions.
- The statistical significance of results should be understood by the IS auditor and results should be representative of the entire audit universe.
- Support for actual conclusions must be based on information. Failure to understand that results include assumptions and caveats can create problems, especially if the need for proof is substituted by computer output. For example, there have been instances of suspects being wrongly identified by facial recognition algorithms run on blurry images.[15]

AI/ML Audit Risk and Considerations

AI/ML techniques are an evolution of CAATs, and the same considerations should be made to ensure they are performing as expected. Specific to AI/ML, the IS auditor should consider:
- Inadequate testing of AI outcomes can produce questionable results or audit outcomes. IS auditors should ensure adequate testing is performed and substantiated by human-led testing. AI/ML programs are often proprietary. Documentation, if available at all, is typically not detailed enough to explain exactly what the algorithm is doing. Even if it is, it may be complex and hard for a nonexpert to understand.
- Training data fed to algorithms, particularly ML algorithms, should be correct and adequate. Such data should be able to cover both usual and unusual cases. In some rare cases, poor training results in algorithms producing incorrect results.
- The tendency to trust the machine's answer is strong, but justified only if the correctness has been exhaustively tested and the machine actually answers the appropriate questions.
- Using AI tools built by humans introduces the ethics and bias of human judgment and stereotyping.

1.9 Reporting and Communication Techniques

Effective and clear communication can significantly improve the quality of audits and optimize their results. Audit findings should be reported and communicated to stakeholders, with appropriate buy-in from the auditees, for the audit process to be successful. An IS auditor should also consider the motivations and perspectives of the recipients of the audit report so their concerns may be properly addressed. Communication skills (both written and verbal) determine the effectiveness of the audit reporting process. Communication and negotiation skills are required throughout the audit. Successful resolution of audit findings with auditees is essential so that auditees will adopt the recommendations in the report and initiate prompt corrective action. To achieve this goal, an IS auditor should be skilled in the use of techniques such as facilitation, negotiation and conflict resolution. An IS auditor should also understand the concept of materiality (i.e., the relative importance of audit findings based on business impact) when reporting audit results.

1.9.1 Communicating Audit Results

The exit interview, conducted at the end of the audit, provides an IS auditor with the opportunity to discuss findings and recommendations with the auditee management. During the exit interview, an IS auditor should:
- Ensure that the facts presented in the report are correct and material
- Ensure that the recommendations are realistic and cost-effective and, if not, seek alternatives through negotiation with auditee management
- Recommend implementation dates for agreed-on recommendations

IS auditors should be aware that, ultimately, they are responsible to senior management and the audit committee, and they should feel free to communicate issues or concerns to them. An attempt to deny access by levels lower than senior management would limit the independence of the audit function.

Before communicating the results of an audit to senior management, an IS auditor should discuss the findings with the auditee management to gain agreement on the findings and develop an agreed-upon course of corrective action. In cases of disagreement, an IS auditor should elaborate on the significance of the findings, risk and effects of not correcting the control weakness. Sometimes the auditee management may request assistance from an IS auditor in implementing the recommended control enhancements. An IS auditor should communicate the difference between an IS auditor's role and that of a consultant and consider how assisting the auditee may adversely affect an IS auditor's independence.

[15] Hill, K.; "Wrongfully Accused by an Algorithm," *The New York Times*, 24 June 2020, *https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html*

©ISACA. All Rights Reserved.

After an agreement has been reached with auditee management, IS audit management should brief senior auditee management. A summary of audit activities should be presented periodically to the audit committee. Audit committees typically are composed of individuals who do not work directly for the organization and, thus, provide an IS audit and assurance professional with an independent route to report sensitive findings.

1.9.2 Audit Report Objectives

The six objectives of audit reporting are to:

1. Formally present the audit results to the auditee (and the audit client, if different from the auditee)
2. Serve as formal closure of the audit engagement
3. Provide statements of assurance and, if needed, identification of areas requiring corrective action and related recommendations
4. Serve as a valued reference for any party researching the auditee or audit topic
5. Serve as the basis for a follow-up audit if audit findings were presented
6. Promote audit credibility, which depends on the report being well developed and well written

The IS audit-specific reporting objectives are developed based on report requirements from auditee management and other users of the report and in compliance with IS audit and assurance standards and audit organization protocols. The auditee or other stakeholders, such as oversight organizations, are identified during audit planning. An IS auditor develops the audit scope and objectives by considering those requirements and other elements of audit planning—such as the assessments of risk, materiality and appropriateness of stated controls—together with regulatory and IT governance requirements. The audit report formally presents the purpose and the results of the audit in line with those requirements. Every audit report should provide unbiased, well-supported responses to the audit's objectives. For example, if the audit objective is to determine whether adequate controls are in effect to provide reasonable assurance that only authorized physical access can be gained to the data center, then the report should state an IS auditor's conclusion or opinion as to the adequacy of the controls to achieve that objective. If controls need to be implemented or strengthened to achieve the objective, then the report should provide a recommendation to meet that need.

1.9.3 Audit Report Structure and Contents

Audit reports are the end product of the IS audit work. The exact format of an audit report will vary by organization; however, an IS auditor should understand the basic components of an audit report and how it communicates audit findings to management.

Note

The CISA candidate should become familiar with the ISACA IS Audit and Assurance Standards 1401 Reporting and 1402 Follow-up Activities.

Audit reports usually include:

- An introduction to the report, stating audit objectives, limitations to the audit and scope, the period of audit coverage, an overview of the nature and extent of audit procedures conducted and processes examined during the audit, and a statement regarding the IS audit methodology and guidelines
- Audit findings, presented in separate sections and often grouped in sections by materiality and/or intended recipient
- An overall conclusion and opinion regarding the adequacy of controls and procedures examined during the audit, and the actual potential risk identified as a consequence of detected deficiencies
- Reservations or qualifications with respect to the audit
  - An IS auditor may state that the controls or procedures examined were found to be adequate or inadequate. The balance of the audit report should support that conclusion, and the overall evidence gathered during the audit should provide an even greater level of support for the audit conclusions.
- Detailed audit findings and recommendations
  - An IS auditor may include specific findings in an audit report, based on the materiality of the findings and the intended recipient of the audit report. For example, an audit report directed to the audit committee of the board of directors may not include findings that are important only to local management and have little control significance to the overall organization. The decision regarding what to include in various levels of audit reports depends on the guidance provided by upper management.

 ©ISACA. All Rights Reserved.

- A variety of findings, some of which may be material while others are minor in nature
  - An IS auditor may choose to present minor findings to management in an alternate format, such as by memorandum.

An IS auditor should make the final decision about what to include or exclude from the audit report. Generally, an IS auditor should be concerned with providing a balanced report, describing not only negative issues in terms of findings but positive constructive comments regarding improved processes and controls or effective controls already in place. Overall, an IS auditor should exercise independence in the reporting process.

Auditee management evaluates the findings, stating corrective actions to be taken and timing for implementing the anticipated corrective actions. Management may not be able to implement all audit recommendations immediately. For example, an IS auditor may recommend changes to an information system that is undergoing other changes or enhancements. An IS auditor should not necessarily expect that the other changes will be suspended until the audit recommendations are implemented. All may be implemented at once.

An IS auditor should discuss the recommendations and any planned implementation dates while in the process of releasing the audit report. Various constraints—such as staff limitations, budgets or other projects—may limit immediate implementation. Management should develop a firm program for taking corrective actions. It is important to obtain a commitment from auditee management on the implementation date for the action plan (implementing the solution can take a long time) and how it will be performed because the corrective action may bring risk that might be avoided if identified while discussing and finalizing the audit report. If appropriate, an IS auditor may want to report to senior management on the progress of implementing recommendations.

The report should include all significant audit findings. When a finding requires explanation, an IS auditor should describe the finding, its cause and risk. When appropriate, an IS auditor should provide the explanation in a separate document and refer to it in the report. For example, this approach may be appropriate for highly confidential matters. An IS auditor should also identify the organizational, professional and governmental criteria applied. The report should be issued in a timely manner to encourage prompt corrective action. When appropriate, an IS auditor should promptly communicate significant findings to the appropriate persons prior to the issuance of the report. However, prior communication of significant findings should not alter the intent or content of the report.

1.9.4 Audit Documentation

Audit documentation is the written record that provides the support for the representations in the auditor's report. It should:

- Demonstrate that the engagement complied with the standards
- Support the basis for the auditor's conclusions

Audit documentation should include, at a minimum:

- Planning and preparation of the audit scope and objectives
- Description and/or walk-throughs on the scoped audit area
- Audit program
- Audit steps performed and audit evidence gathered
- Use of services of other auditors and experts
- Audit findings, conclusions and recommendations
- Audit documentation relation with document identification and dates

It is also recommended that documentation include:

- A copy of the report issued as a result of the audit work
- Evidence of audit supervisory review

Documents should include audit information that is required by laws and regulations, contractual stipulations and professional standards. Audit documentation is the necessary evidence supporting the conclusions reached and should be clear, complete, easily retrievable and sufficiently comprehensible. Audit documentation is generally the property of the auditee and should be accessible only to authorized personnel under specific or general permission. When access to audit documentation is requested by external parties, an IS auditor should obtain appropriate prior approval of senior management and legal counsel before providing it to those external parties.

Policies should be developed regarding custody, retention requirements and release of audit documentation. The documentation format and media are optional, but due diligence and good practices require that work papers be dated, initialed, page-numbered, relevant, complete, clear, self-contained and properly labeled, filed and kept in custody. Work papers may be automated. An IS auditor should consider how to maintain integrity and protection of audit test evidence to preserve its proof value in support of audit results.

©ISACA. All Rights Reserved.

An IS auditor should be able to prepare adequate work papers, narratives, questionnaires and understandable system flowcharts. Audit documentation or work papers can be considered the bridge or interface between the audit objectives and the final report. They should provide a seamless transition—with traceability and accountability—from objectives to report and from report to objectives. The audit report, in this context, can be viewed as a set of particular work papers.

The quest for integrating work papers in the auditor's environment has resulted in all major audit and project management packages, CAATs and expert systems offering a complete array of automated documentation and import-export features.

Audit documentation should support the audit findings and conclusions/opinions. Time of evidence can be crucial to supporting audit findings and conclusions. An IS auditor should take care to ensure that the evidence gathered and documented will be able to support audit findings and conclusions.

The concept of materiality is a key issue when deciding which findings to bring forward in an audit report. Key to determining the materiality of audit findings is the assessment of what would be significant to different levels of management. Assessment requires judging the potential effect of a finding if corrective action is not taken. For example:

- A weakness in information security physical access controls at a remote distributed computer site may be significant to management at the site but would not necessarily be material to upper management at headquarters. However, there may be other matters at the remote site that would be material to upper management.
- A review of access deprovisioning might discover that a terminated user's access was not removed after the user's termination date but show that it was caught during management's review of security access, at which time the terminated user's access was removed. This type of discovery would not likely be brought to the attention of upper management but would be documented and discussed with auditee management.

1.9.5 Follow-Up Activities

Auditing is an ongoing process. An IS auditor is not effective if audits are performed and reports issued, but no follow-up is conducted to determine whether management has taken appropriate corrective actions. IS auditors should have a follow-up program to determine if agreed-on corrective actions have been implemented. Although IS auditors who work for external audit firms may not necessarily follow this process, they may achieve these tasks if they are agreed to by the auditee.

The timing of the follow-up will depend on the criticality of the findings and is subject to an IS auditor's judgment. The results of the follow-up should be communicated to appropriate levels of management. The level of an IS auditor's follow-up review will depend on several factors. In some instances, an IS auditor may merely need to inquire as to the current status. In other instances, an IS auditor who works in an internal audit function may have to perform certain audit steps to determine whether the corrective actions agreed on by management have been implemented.

1.9.6 Types of IS Audit Reports

The IS audit report is driven mainly by the type of audit engagement and the reporting requirements from IS audit and assurance standards. While most IS audits result in a single IS audit report, in some situations, more than one report can be applicable. For example, in addition to a report for a general audience, a separate confidential security report containing detailed technical information may need to be created to ensure that security risk is not disclosed to unintended parties.

The organization and specific content of the report also depend on the scope and objectives of the audit engagement and the degree to which IT processes and systems are examined or require explanation. The format and protocols for audit report presentation can depend on any requirements and expectations set forth between the audit organization and the auditee. Requirements for audit report contents or format may be requested by the audit client who may or may not be from the same organization as the auditee.

Although review, examination and agreed-upon procedure engagements have similar reporting requirements, each type of engagement stipulates different reporting requirements and limitations. The primary distinctions among reviews, examinations and agreed-upon procedures stem from the audit objectives, the nature and extent of audit work and the level of assurance to be provided. While all three types of audits include review work, performing audit tests is far more prevalent in audits or examinations that require stronger evidence for formulation of an opinion. Agreed-upon procedures may also include testing, but because of other limitations, an audit opinion may not be expressed. Although audit scope may be the same for reviews

 ©ISACA. All Rights Reserved.

and examinations, scope is likely to be more narrowly defined for agreed-upon procedure audits.

1.10 Quality Assurance and Improvement of the Audit Process

IS audit plays an important role in improving the quality and control of information systems in an organization. As a critical element to the organization's continued improvement, it is important that the audit process itself improves continuously.

1.10.1 Audit Committee Oversight

If present, the audit committee is responsible for oversight of the IS audit function and interaction with the chief audit executive. If an audit committee does not exist, a designated group or individual assumes the responsibilities of oversight of the audit function. An oversight function and continuous performance monitoring of the audit function (including IS audit) should be established and reviewed through periodic reporting.

1.10.2 Audit Quality Assurance

The quality of individual audits is the responsibility of audit leadership and the assigned project leads. These individuals are responsible for ensuring that documented audit procedures are followed. Documented audit procedures may come in a variety of forms (audit manuals, wikis, sampling guidance, etc.) but should be clearly identified and known to all applicable members of the IS audit function.

IS audit leadership is responsible for the review of audit work papers and final deliverables (e.g., audit reports). A formal review process (detail review, engagement quality review, QA, etc.) should be established for all audit types based on risk and guidance from authoritative sources.

1.10.3 Audit Team Training and Development

A formal development plan should be established for all members of the IS audit function. This plan should include applicable training programs and certifications by role within the IS audit function. IS audit leadership should ensure that a budget is created and supports the needs of training and development for IS audit team members.

1.10.4 Monitoring

Monitoring for compliance with applicable requirements is an important element to ensure that an IS audit function maintains continuation of the audit process within an organization. Examples of monitoring related initiatives include:

- **Audit QA**—The results of audit QA procedures should be periodically reviewed and summarized to identify trends and lessons learned. Actionable items identified during audit QA should be remediated and tracked in a formal manner.
- **Independence monitoring**—A process should be established to allow IS auditors to self-report potential impairments of independence. This process can be integrated into the greater audit function within the organization. Leadership and IS auditors themselves should periodically check to ensure that their independence has not been impaired and report any changes through the established reporting process.
- **Certification and accreditations**—Ownership of applicable certification or accreditation held by an IS audit function should be assigned to appropriate members of IS audit leadership. These individuals should ensure that compliance with certification or accreditation bodies applicable to the IS audit function is maintained.
- **Continued professional education**—Leadership should ensure that a process is in place to monitor the IS auditor's compliance with continued professional education or training requirements. These requirements may be established by an internal development plan or through external certifying bodies.

©ISACA. All Rights Reserved.

Page intentionally left blank

Case Study

Betatronics is a mid-sized manufacturer of electronic goods with headquarters in the United States and factories in Latin America. An IS auditor within the enterprise has been asked to perform preliminary work that will assess the organization's readiness for a review to measure compliance with new US regulatory requirements.

The requirements are designed to ensure that management is taking an active role in setting up and maintaining a well-controlled environment and to assess management's review and testing of the general IT controls. Areas to be assessed include:

- Logical and physical security
- Change management
- Production control and network management
- IT governance
- End-user computing

The IS auditor has been given six months to perform preliminary work. In previous years, repeated problems were identified in the areas of logical security and change management. Logical security deficiencies included the sharing of administrator accounts and failure to enforce adequate controls over passwords. Change management deficiencies included improper segregation of incompatible duties and failure to document all changes. Additionally, the process for deploying OS updates to servers was found to be only partially effective.

The chief information officer (CIO) requested direct reports to develop narratives and process flows describing major activities for which IT was responsible. Those tasks were completed, approved by the various process owners and the CIO, and then forwarded to the IS auditor for examination. Following the completion of the preliminary audit work, Betatronics decides to plan audits for the next two years. After accepting the appointment, the IS auditor notes that:

- The entity has an audit charter that details the scope and responsibilities of the IS audit function and specifies the audit committee as the overseeing body for audit activity.
- The entity is subject to regulatory compliance requirements that require its management to certify the effectiveness of the internal control system as it relates to financial reporting.
- The entity has been recording consistent growth over the last two years at double the industry average.
- The entity has seen increased employee turnover.

1. What should the IS auditor do **FIRST**?

   A. Perform a survey audit of logical access controls.
   B. Revise the audit plan to focus on risk-based auditing.
   C. Perform an IT risk assessment.
   D. Begin testing controls that the IS auditor feels are most critical.

2. When auditing the logical security, the IS auditor is **MOST** concerned when observing:

   A. the system administrator account is known by everybody.
   B. the passwords are not enforced to change frequently.
   C. the network administrator is given excessive permissions.
   D. the IT department does not have a written policy on privilege management.

3. When testing program change management in this case, how should the sample be selected?

   A. Change management documents should be selected at random and examined for appropriateness.
   B. Changes to production code should be sampled and traced to appropriate authorizing documentation.
   C. Change management documents should be selected based on system criticality and examined for appropriateness.
   D. Changes to production code should be sampled and traced back to system-produced logs indicating the date and time of the change.

4. List three general IT controls the IS auditor would use for substantive testing when planning audits for the next two years.

5. The **FIRST** priority of the IS auditor in year one should be to study the:

   A. Previous IS audit reports in order to plan the audit schedule
   B. Audit charter in order to plan the audit schedule
   C. Impact of the increased employee turnover
   D. Impact of the implementation of a new enterprise resource plan on the IT environment

©ISACA. All Rights Reserved.

6. How should the IS auditor evaluate backup and batch processing within computer operations?

   A. Rely on the service auditor's report of the service provider
   B. Study the contract between the entity and the service provider
   C. Compare the service delivery report to the SLA
   D. Plan and carry out an independent review of computer operations

7. During the day-to-day work, the IS auditor advises there is a risk that log review may not result in timely detection of errors. This is an example of which of the following?

   A. Inherent risk
   B. Residual risk
   C. Control risk
   D. Material risk

8. The IS auditor advised the CIO and team to improve the general IT control environment, and adapting COBIT was proposed for that purpose. What recommendations should the IS auditor make when considering this framework?

Answers on page 82

 ©ISACA. All Rights Reserved.

Page intentionally left blank

©ISACA. All Rights Reserved.

Chapter 1 Answer Key

Case Study

1. A. Performing a survey audit of logical access controls would occur after an IT risk assessment.
   B. Revising the audit plan to focus on risk-based auditing would occur after an IT risk assessment.
   C. An IT risk assessment should be performed first to ascertain which areas present the greatest risk and which controls mitigate that risk. Although narratives and process flows have been created, the organization has not yet assessed which controls are critical.
   D. Testing controls that the IS auditor feels are most critical would occur after an IT risk assessment.

2. **A. The system administrator account being known by everybody is most dangerous. In that case, any user could perform any action in the system, including accessing files and making permission and parameter adjustments.**
   B. Infrequent password changing would present a concern but would not be as serious as everyone knowing the system administrator account.
   C. The network administrator being given excessive permissions would present a concern, but it would not be as serious as everyone knowing the system administrator account.
   D. The absence of a privilege management policy would be a concern, but it would not be as serious as everyone knowing the system administrator account.

3. A. When a sample is chosen from a set of control documents, there is no way to ensure that every change is accompanied by appropriate control documentation.
   B. When testing a control, it is advisable to trace from the item being controlled to the relevant control documentation. When a sample is chosen from a set of control documents, there is no way to ensure that every change is accompanied by appropriate control documentation. Accordingly, changes to production code provide the most appropriate basis for selecting a sample.
   C. When a sample is chosen from a set of control documents, there is no way to ensure that every change is accompanied by appropriate control documentation.
   D. When testing a control, it is advisable to trace from the item being controlled to the relevant control documentation.

4. Some possible answers include:
   - The IS auditor can check which account was recently used for executing a particular system administrator task.
   - The IS auditor can check if there was a change record for any selected system changes (e.g., server reboot and patching).
   - The IS auditor can check the transactions to see if they separated the incompatible duties.

5. A. Previous IS audit reports will be revisited to save redundant work and to use as references when doing the IS audit work.
   B. The audit charter defines the purpose, authority and responsibility of the IS audit activities. It also sets the foundation for upcoming activities.
   C. Impact of employee turnover would be addressed when negotiating follow-up activities for respective areas if there is any gap to close.
   D. Impact of the implementation of a new ERP would be addressed when negotiating the follow-up activities for respective areas if there is any gap to close.

6. A. The service auditor's report cannot ensure the discovery of control inefficiencies.
   B. Review of the contract cannot ensure the discovery of control inefficiencies.
   C. Comparing the service delivery report and the service level agreement cannot ensure the discovery of control inefficiencies.
   D. IS audit should conduct an independent review of the backup and batch processing. All other choices cannot ensure the discovery of control inefficiencies in the process.

7. A. This is not an example of inherent risk. Inherent risk is the risk level or exposure without considering the actions that management has taken or might take (e.g., implementing controls).
   B. This is not an example of residual risk. Residual risk is the remaining risk after management has implemented a risk response.
   C. Control risk exists when a risk cannot be prevented or detected on a timely basis by the system of IS controls, which is described in this instance.

 ©ISACA. All Rights Reserved.

D. This is not an example of material risk. Material risk is any risk large enough to threaten the overall success of the business in a material way.

8. Possible answer: The COBIT framework can be leveraged and adapted. Each process can be classified as fully addressed, partially addressed and not applicable by comparing the standard COBIT framework to the organization's reality. Further frameworks, standards and practices can be included in each respective process, as COBIT guidance suggests.

©ISACA. All Rights Reserved.

Page intentionally left blank

 ©ISACA. All Rights Reserved.

Chapter 2

Governance and Management of IT

Overview

Domain 2 Exam Content Outline 86
Learning Objectives/Task Statements 86
Suggested Resources for Further Study 87
Self-Assessment Questions 87
Chapter 2 Answer Key 90

Part A: IT Governance

2.1 Laws, Regulations and Industry Standards 93
2.2 Organizational Structure, IT Governance and IT Strategy 95
2.3 IT Policies, Standards, Procedures and Guidelines 117
2.4 Enterprise Architecture and Considerations 121
2.5 Enterprise Risk Management 122
2.6 Data Privacy Program and Principles 127
2.7 Data Governance and Classification 131

Part B: IT Management

2.8 IT Resource Management 137
2.9 IT Vendor Management 143
2.10 IT Performance Monitoring and Reporting 150
2.11 Quality Assurance and Quality Management of IT 155

Case Study

Case Study 157
Chapter 2 Answer Key 160

©ISACA. All Rights Reserved.

Overview

Governance and management of IT are integral parts of enterprise governance.

Effective governance and management of IT consist of the leadership, organizational structures and processes to ensure the enterprise's IT function sustains and extends the enterprise's strategy and objectives.

Knowledge of IT governance is fundamental to the work of the information systems (IS) auditor. It forms the foundation for developing sound control practices and management oversight and review mechanisms.

This domain represents 18 percent of the CISA examination (approximately 27 questions).

Domain 2 Exam Content Outline

Part A: IT Governance

1. Laws, Regulations and Industry Standards
2. Organizational Structure, IT Governance and IT Strategy
3. IT Policies, Standards, Procedures and Practices
4. Enterprise Architecture (EA) and Considerations
5. Enterprise Risk Management (ERM)
6. Privacy Program and Principles
7. Data Governance and Classification

Part B: IT Management

1. IT Resource Management
2. IT Vendor Management
3. IT Performance Monitoring and Reporting
4. Quality Assurance and Quality Management of IT

Learning Objectives/Task Statements

Within this domain, the IS auditor should be able to:

- Conduct audits in accordance with IS audit standards and a risk-based IS audit strategy.
- Communicate and collect feedback on audit progress, findings, results and recommendations with stakeholders.
- Conduct post-audit follow-up to evaluate whether the identified risk has been sufficiently addressed.
- Evaluate the role and/or impact of automatization and/or decision-making systems for an organization.
- Evaluate the IT strategy for alignment with the organization's strategies and objectives.
- Evaluate the effectiveness of IT governance structure and IT organizational structure.
- Evaluate the organization's management of IT policies and practices, including compliance with legal and regulatory requirements.
- Evaluate IT resources and project management for alignment with the organization's strategies and objectives.
- Evaluate the organization's enterprise risk management (ERM) program.
- Determine whether the organization has defined ownership of IT risk, controls and standards.
- Evaluate the monitoring and reporting of IT key performance indicators (KPIs) and IT key risk indicators (KRIs).
- Evaluate the organization's ability to continue business operations.
- Evaluate the organization's storage, backup and restoration policies and processes.
- Evaluate whether the business cases related to information systems meet business objectives.
- Evaluate whether IT vendor selection and contract management processes meet business, legal and regulatory requirements.
- Evaluate whether effective processes are in place to support end users.
- Evaluate whether IT service management practices align with organizational requirements.
- Conduct periodic reviews of information systems and enterprise architecture (EA) to determine alignment with organizational objectives.
- Evaluate whether IT operations and maintenance practices support the organization's objectives.
- Evaluate the organization's database management practices.
- Evaluate the organization's data governance program.
- Evaluate the organization's privacy program.
- Evaluate data classification practices for alignment with the organization's data governance program, privacy program and applicable external requirements.
- Evaluate the organization's problem and incident management program.
- Evaluate the organization's change, configuration, release and patch management programs.
- Evaluate the organization's log management program.
- Evaluate the organization's policies and practices related to asset life cycle management.
- Evaluate the organization's information security program.
- Evaluate the organization's threat and vulnerability management program.

 ©ISACA. All Rights Reserved.

- Evaluate the organization's security awareness training program.
- Evaluate potential opportunities and risk associated with emerging technologies, regulations and industry practices.

Suggested Resources for Further Study

Hales, A.; *The Definitive Handbook of Business Continuity Management, 3rd Edition*, John Wiley & Sons Inc., USA, 2011

International Organization for Standardization (ISO), *ISO/IEC 38500:2015: Information technology—Governance of IT for the Organization*, Switzerland, 2015

ISACA, *COBIT*, *https://www.isaca.org/resources/cobit*

ISACA, *Getting Started with Governance of Enterprise IT (GEIT)*, USA, 2015

ISACA, *The Risk IT Framework, 2nd Edition*, USA, 2021

ISACA, White Papers, *https://www.isaca.org/resources/insights-and-expertise/white-papers*

Self-Assessment Questions

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often, a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Note that these questions are not actual or retired exam items. See section About This Manual at the beginning of this manual for more guidance regarding practice questions.

1. For management to effectively monitor the compliance of processes and applications, which of the following would be the **MOST** ideal?

   A. A central document repository
   B. A knowledge management system
   C. A dashboard
   D. Benchmarking

2. Which of the following would be included in an information systems (IS) strategic plan?

   A. Specifications for planned hardware purchases
   B. Analysis of future business objectives
   C. Target dates for development projects
   D. Annual budgetary targets for the IT department

3. Which of the following **BEST** describes an IT department's strategic planning process?

   A. The IT department will have either short- or long-range plans depending on the organization's broader plans and objectives.
   B. The IT department's strategic plan must be time- and project-oriented but not so detailed that it addresses and helps determine priorities to meet business needs.
   C. Long-range planning for the IT department should recognize enterprise goals, technological advances and regulatory requirements.
   D. Short-range planning for the IT department does not need to be integrated into the short-range plans of the enterprise, because technological advances will drive the IT department plans much quicker than enterprise plans.

4. Which of the following is the **MOST** important responsibility of a data security officer in an enterprise?

   A. Recommending and monitoring data security policies
   B. Promoting security awareness within the enterprise
   C. Establishing procedures for IT security policies
   D. Administering physical and logical access controls

5. What is considered the **MOST** critical element for successfully implementing an information security program?

   A. An effective enterprise risk management (ERM) framework
   B. Senior management commitment
   C. An adequate budgeting process
   D. Meticulous program planning

6. An IS auditor should ensure that IT governance performance measures:

   A. evaluate the activities of IT oversight committees.
   B. provide strategic IT drivers.
   C. adhere to regulatory reporting standards and definitions.
   D. evaluate the IT department.

©ISACA. All Rights Reserved.

7. Which of the following tasks may be performed by the same person in a well-controlled information processing computer center?

   A. Security administration and change management
   B. Computer operations and system development
   C. System development and change management
   D. System development and system maintenance

8. Which of the following is the **MOST** critical control over database administration (DBA)?

   A. Approval of DBA activities
   B. Separation of duties regarding access rights granting/revoking
   C. Review of access logs and activities
   D. Review of the use of database tools

9. When complete separation of duties (SoD) cannot be achieved in an online system environment, which of the following functions should be separated from the others?

   A. Origination
   B. Authorization
   C. Recording
   D. Correction

10. In a small enterprise, where separation of duties (SoD) is not practical, an employee performs the functions of computer operator and application programmer. Which of the following controls should the information systems (IS) auditor recommend?

    A. Automated logging of changes to development libraries
    B. Additional staff to provide SoD
    C. Procedures that verify that only approved program changes are implemented
    D. Access controls to prevent the operator from making program modifications

Answers on page 90

Page intentionally left blank

©ISACA. All Rights Reserved.

Chapter 2 Answer Key

Self-Assessment Questions

1. A. A central document repository hosts a great deal of data but not necessarily the specific information that would be useful for monitoring and compliance.
   B. A knowledge management system provides valuable information but generally is not used by management for compliance purposes.
   C. A dashboard provides information that illustrates compliance with the processes, applications and configurable elements and keeps the enterprise on course.
   D. Benchmarking provides information to help managers adapt the enterprise promptly, according to trends and environment.

2. A. Specifications for planned hardware purchases are not strategic items.
   B. Information systems (IS) strategic plans must address the needs of the business and meet future business objectives. Hardware purchases may be outlined, but not specified, and neither budget targets nor development projects are appropriate choices.
   C. Target dates for development projects are not strategic items.
   D. Annual budgetary targets for the IT department are not strategic items.

3. A. Typically, the IT department will have short- or long-range plans that are consistent and integrated with the organization's plans.
   B. Plans must be time- and project-oriented and address the enterprise's broader plans toward attaining its goals.
   C. Long-range planning for the IT department should recognize enterprise goals, technological advances and regulatory requirements.
   D. Short-range planning for the IT department should be integrated into the short-range plans of the enterprise to better enable the IT department to be agile and responsive to needed technological advances that align with enterprise goals and objectives.

4. **A. A data security officer's prime responsibility is recommending and monitoring data security policies.**
   B. Promoting security awareness within the enterprise is one of the responsibilities of a data security officer. However, it is less important than recommending and monitoring data security policies.
   C. The IT department, not the data security officer, is responsible for establishing procedures for IT security policies recommended by the data security officer.
   D. The IT department, not the data security officer, is responsible for the administration of physical and logical access controls.

5. A. An effective enterprise risk management (ERM) framework is not a key success factor for an information security program.
   B. Senior management's commitment provides the basis for success in implementing an information security program.
   C. Although an effective information security budgeting process will contribute to success, senior management commitment is the key element.
   D. Program planning is important but will not be sufficient without senior management commitment.

6. **A. Evaluating the activities of boards and committees providing oversight is an important aspect of governance and should be measured.**
   B. Providing strategic IT drivers is irrelevant to evaluating IT governance performance measures.
   C. Adhering to regulatory reporting standards and definitions is irrelevant to evaluating IT governance performance measures.
   D. Evaluating the IT department is irrelevant to evaluating IT governance performance measures.

7. A. The roles of security administration and change management are incompatible functions. The level of security administration access rights could allow changes to go undetected.
   B. Computer operations and system development is the incorrect choice because this would make it possible for an operator to run a program they had amended.
   C. The combination of system development and change control would allow program modifications to bypass change control approvals.
   D. It is common for system development and maintenance to be undertaken by the same

 ©ISACA. All Rights Reserved.

person. In both, the programmer requires access to the source code in the development environment but should not be allowed access in the production environment.

8. A. Approval of database administration (DBA) activities does not prevent the combination of conflicting functions. Review of access logs and activities is a detective control.
   B. Separation of duties (SoD) will prevent the combination of conflicting functions. This is a preventive control, and it is the most critical control over DBA.
   C. Reviewing access logs and activities may not reduce the risk if DBA activities are improperly approved.
   D. Reviewing the use of database tools does not reduce the risk because this is only a detective control and does not prevent the combination of conflicting functions.

9. A. Origination, in conjunction with recording and correction, does not enable the transaction to be authorized for processing and committed within the system of record.
   B. Authorization should be separated from all aspects of record keeping (origination, recording and correction). Such a separation enhances the ability to detect the recording of unauthorized transactions.
   C. Recording, in conjunction with origination and correction, does not enable the transaction to be authorized for processing and committed within the system of record.
   D. Correction, in conjunction with origination and recording, does not enable the transaction to be authorized for processing and committed within the system of record.

10. A. Logging changes to development libraries would not detect changes to production libraries.
    B. In smaller enterprises, it generally is not appropriate to recruit additional staff to achieve a strict separation of duties. The IS auditor must look at alternatives.
    C. The information systems (IS) auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so that the changes can be reviewed by a third party regularly. This would be a compensating control process.
    D. Access controls to prevent the operator from making program modifications require a third party to make the changes, which may not be practical in a small enterprise.

©ISACA. All Rights Reserved.

Page intentionally left blank

Part A: IT Governance

IT governance is not an isolated discipline. Rather, IT governance is an integral part of a comprehensive enterprise/corporate governance program that typically includes organizational functions such as audit, compliance, legal and risk management. All functions within the governance program share the responsibility for providing strategic direction, ensuring organizational objectives are achieved, ascertaining whether risk is managed appropriately and verifying the responsible deployment of resources.

The IT governance process generally starts with setting objectives for an enterprise's IT function, assessing risk to achieving those objectives and establishing controls to mitigate that risk before monitoring the IT function's performance against the objectives and making adjustments as needed.

Note

The *CISA Official Review Manual* uses the terms governance of enterprise information and technology (GEIT), enterprise governance of information and technology (EGIT), governance of IT and IT governance (ITG) interchangeably.

2.1 Laws, Regulations and Industry Standards

IT governance must consider the laws, regulations and industry standards that apply to the enterprise. The laws and regulations applicable to the geographic location and industry of the enterprise will impact the enterprise's performance of functions within the information life cycle, including the receipt, processing, storage, transmission, distribution and destruction of data. A wide variety of statutory requirements have been enacted to protect stakeholder interests. These laws and regulations constantly evolve, requiring IS auditors to remain current on which ones apply to their enterprise.

Regulatory drivers require developing and implementing well-maintained, timely, relevant and actionable organizational business policies, procedures and processes related to IT governance. The major compliance requirements that are considered globally recognized include the protection of privacy and confidentiality of personal data, intellectual property rights and the reliability of financial information produced by enterprises. In addition, some compliance requirements are industry-specific, such as regulations over electronic communication in US brokerage firms.

The IT organization should assess how effectively it protects all IT assets and manages associated risk. Compliance with legislative and regulatory requirements on accessing and using IT resources, systems and data should be reviewed regularly. Like with any risk, enterprises may also weigh the option of compliance with a legal or regulatory requirement and decide to accept noncompliance risk and penalties.

Note

For the CISA exam, the IS auditor must be aware of these globally recognized concepts; however, knowledge of specific legislation and regulations will not be tested.

2.1.1 Impact of Laws, Regulations and Industry Standards on IS Audit

Enterprises may be subject to audits related to specific applicable laws, regulations and industry standards. The audits generally are to ascertain compliance with statutory requirements. Examples of laws that may require an audit include:

- United States laws:
  - Gramm-Leach-Bliley Act (GLBA)
  - Family Educational Rights and Privacy Act (FERPA)
  - Children's Online Privacy Protection Act (COPPA)
  - Children's Internet Protection Act (CIPA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Federal Information Security Management Act of 2002 (FISMA)
  - Sarbanes-Oxley Act (SOX) of 2002
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- South Korea's Personal Information Protection Act (PIPA)
- Japan's Financial Instruments and Exchange Act (FIEA) of 2006
- South Africa's Protection of Personal Information (POPI) Act
- The UK Ministry of Defence's DEFCON 658
- The UK Data Protection Act
- The EU's General Data Protection Act (GDPR)
- Saudi Arabia's Personal Data Protection Law (PDPL)
- Australia's Privacy Act 1988

©ISACA. All Rights Reserved.

In addition, enterprises operating in multiple jurisdictions must be aware of the legal and regulatory requirements in those areas in which they operate. Some laws and regulations may apply to enterprises, even those not headquartered in the jurisdiction where the law or regulation was created. For example, GDPR requires enterprises within the European Union and enterprises that handle protected data related to individuals in the European Union to follow specific guidelines related to the transmission, storage and destruction of that data. As a result, GDPR compliance applies to enterprises globally if they do business with anyone in the European Union.

According to The Institute of Internal Auditors (IIA)[16], the auditor should consider the following when auditing regulatory compliance:

- **Standards and procedures**—Compliance standards and procedures should be established, which employees and other entities should follow to reduce the risk of criminal activity.
- **Assignment of responsibility to senior personnel**—Overall responsibility for compliance with standards and procedures should be assigned to a specific individual(s) within the enterprise senior management.
- **Reliable staff background**—The enterprise should conduct background checks on staff members before establishing access or authority roles to ensure that such power is not delegated to individuals who have conducted illegal activity.
- **Communication of procedures**—Enterprise standards and procedures should be communicated effectively to all employees and other agents via training or documentation.
- **Compliance monitoring and auditing**—The enterprise should take reasonable steps to achieve compliance with its standards (e.g., monitoring and reporting).
- **Consistent enforcement**—Compliance should be enforced consistently throughout the enterprise, with appropriate disciplinary action toward offenders.
- **Appropriate response to an offense and prevention of similar offenses**—Enterprises should act appropriately (i.e., reporting to proper authorities and/or law enforcement) when an offense is detected/occurs and act to prevent future offenses promptly.

The United Nations Conference on Trade and Development (UNCTAD) Global Cyberlaw Tracker[17] is the first global mapping of cyberlaws. It tracks the state of ecommerce legislation in the field of etransactions, consumer protection, data protection/privacy and cybercrime adoption in the 194 UNCTAD member states. It indicates whether a given country has adopted legislation or has a draft law pending adoption.

2.1.2 Governance, Risk and Compliance

The rise of the term governance, risk and compliance (GRC) comes from a growing recognition within enterprises that assurance processes cannot exist in a silo. At a high level, each of the three components can be defined as follows:

- **Governance**—Managing the enterprise's policies, processes and decisions
- **Risk (management)**—Identifying, assessing and treating potential risk
- **Compliance**—Adhering to laws, regulations, standards and policies

According to OCEG, the organization that created the acronym GRC, the term captures "the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity—to achieve Principled Performance."[18] GRC is often referred to as a single business activity because the components include overlapping and related assurance activities within an enterprise. The assurance functions may include governance, internal audit, compliance programs, enterprise risk management (ERM), operational risk management (ORM), incident management and other activities.

Although a GRC program can be implemented in any area of an organization, it is usually focused on financial, IT and legal areas. Financial GRC ensures proper operation of financial processes and compliance with regulatory requirements, such as SOX in the United States. Similarly, IT GRC seeks to ensure proper operation and policy compliance of IT processes. An enterprise may implement legal GRC to focus on overall regulatory compliance for their location and industry.

Although it may be practiced differently across enterprises or even among business units, the overall goal for GRC is to promote a combined, holistic view

[16] The Institute of Internal Auditors, *https://www.theiia.org/*

[17] United Nations Conference on Trade and Development, "Global Cyberlaw Tracker," UNCTAD, *https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide*

[18] Open Compliance and Ethics Group, "What is GRC (Governance, Risk and Compliance)?" OCEG, *https://www.oceg.org/ideas/what-is-grc/*

 ©ISACA. All Rights Reserved.

of risk that can prevent an enterprise from achieving its objectives.

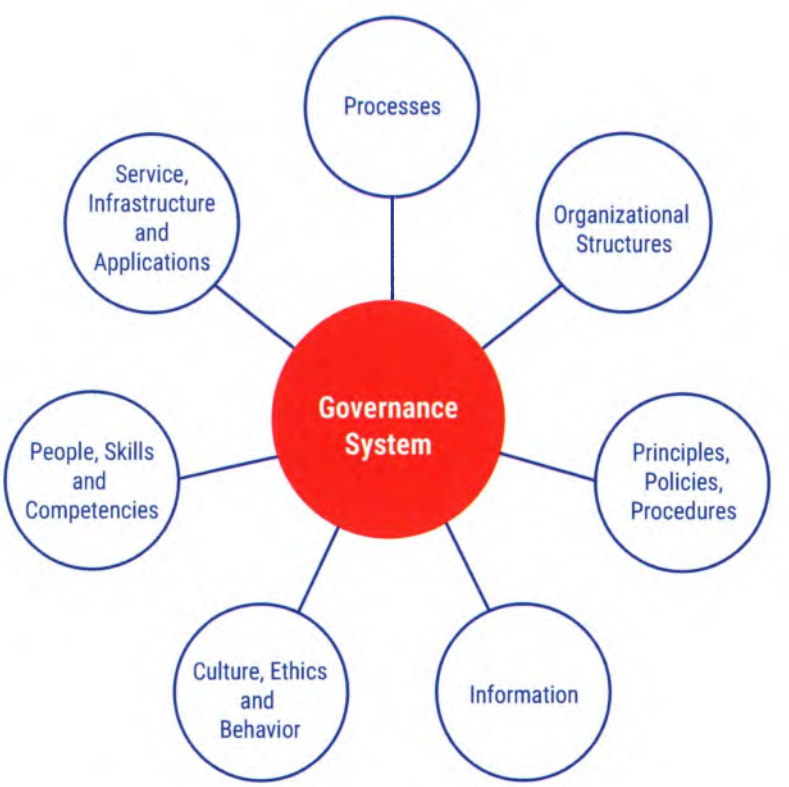
2.2 Organizational Structure, IT Governance and IT Strategy

Ethical issues, decision-making and overall practices within an enterprise must be fostered through corporate governance practices. These make up the system by which enterprises are directed and controlled. The board of directors is responsible for the governance of the enterprise. IT governance consists of the leadership and organizational structures and processes that ensure that the enterprise sustains and extends strategies and objectives.

Corporate governance involves a set of relationships among a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the company's objectives are set, and the means of attaining those objectives and monitoring performance are determined. Corporate governance aims to help build an environment of trust, transparency and accountability for fostering long-term investment, financial stability and business integrity, thereby supporting more robust growth and more inclusive societies.[19]

A corporate governance framework is being increasingly used by government bodies globally to reduce the frequency and impact of inaccurate financial reporting and provide greater transparency and accountability. Many government regulations require that senior management sign off on the adequacy of internal controls and include an assessment of organizational internal controls in the organization's financial reports. **Figure 2.1** illustrates the components of an enterprise governance framework.

Figure 2.1—COBIT Components of a Governance System



Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018

[19] Organisation for Economic Co-operation and Development, *G20/OECD Principles of Corporate Governance*, OECD, 11 September 2023, *https://www.oecd-ilibrary.org/sites/ed750b30-en/index.html?itemId=/content/publication/ed750b30-en*

©ISACA. All Rights Reserved.

2.2.1 Enterprise Governance of Information and Technology

EGIT implies a system in which all stakeholders, including the board, senior management, internal customers and departments, such as finance, provide input into the IT decision-making process. EGIT is the responsibility of the board of directors and executive management. In other words, EGIT is about the stewardship of IT resources on behalf of all stakeholders (internal and external) who expect their interests to be met. The board of directors, which is responsible for this stewardship, looks to management to implement the necessary systems and IT controls.

The purpose of EGIT is to direct IT endeavors to ensure that IT aligns with and supports the enterprise's objectives and realization of promised benefits. Additionally, IT should enable the enterprise by exploiting opportunities and maximizing benefits. IT resources should be used responsibly, and IT-related risk should be managed appropriately.

Implementing an EGIT framework addresses these issues by implementing practices that provide feedback on value delivery and risk management. The overall processes are:

- **IT resource management**—Focuses on maintaining an updated inventory of all IT resources and addresses the risk management process.
- **Performance measurement**—Focuses on ensuring that all IT resources perform as expected to deliver value to the business and identify risk early on. This process is based on performance indicators optimized for value delivery, from which any deviation might lead to risk.
- **Compliance management**—Focuses on implementing processes that address legal and regulatory policy and contractual compliance requirements.

ISACA's COBIT framework, developed to help enterprises optimize the value of information assets, makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes. COBIT's view on this key distinction between governance and management is:

- **Governance**—Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives; direction is set through prioritization and decision making, and performance and compliance are monitored against agreed-on direction and objectives.
- **Management**—Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

EGIT, one of the domains of enterprise governance, comprises the issues addressed in considering how IT is applied within the enterprise.

Effective enterprise governance focuses on individual and group expertise and experience in areas where it can be most effective. Initially, IT was considered only an enabler of the enterprise's strategy. Now, IT is seen as an integral part of the strategy. Senior management agrees that strategic alignment between IT and enterprise objectives has become a critical success factor (CSF) for enterprise and cannot be seen simply as IT management or IT specialist operations. Rather, IT must receive guidance and supervision from senior management and oversight by the board of directors. The key element of EGIT is the alignment of business and IT that leads to achieving business value.

Fundamentally, EGIT is concerned with two issues: (1) that IT delivers value to the business and (2) that IT risk is managed. The first is driven by the strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise.

2.2.2 Good Practices for EGIT

The purpose of an IT governance system is to satisfy stakeholder needs and generate value from the use of IT. This value is a balance among benefits, risk and resources.

EGIT has become significant due to many factors, including:

- Business managers and boards demanding a better return from IT investments (i.e., that IT delivers what the business needs to enhance stakeholder value)
- Concern over the generally increasing level of IT expenditure
- The need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting (e.g., SOX, Basel Accords and the EU GDPR) and in specific sectors, such as finance, pharmaceuticals and healthcare
- The selection of service providers and the management of service outsourcing and acquisition (e.g., cloud computing)
- IT governance initiatives that include the adoption of control frameworks and good practices to help monitor and improve critical IT activities to increase

 ©ISACA. All Rights Reserved.

business value and reduce business risk (e.g., emerging risk related to cybersecurity)
- The need to optimize costs by following, where possible, standardized rather than specially developed approaches
- The growing maturity and the consequent acceptance of well-regarded frameworks
- The need for enterprises to assess how they are performing against generally accepted standards and their peers (i.e., benchmarking)

The processes to evaluate, direct and monitor are integrated end-to-end into the governance process and focus on the evaluation, direction and monitoring of the following:
- Conformance and performance
- System of internal controls
- Compliance with external requirements

2.2.3 Audit's Role in EGIT

Enterprises are governed by generally accepted good practices, ensured by establishing controls. Good practices guide enterprises in determining how to use resources. Results are measured and reported, providing input to controls' cyclical revision and maintenance.

Similarly, IT is governed by good practices, which ensure that the enterprise's information and related technology support the enterprise business objectives (i.e., strategic alignment), deliver value, use resources responsibly, manage risk appropriately and measure performance.

Audit plays a significant role in successfully implementing EGIT within an enterprise. Audit is well-positioned to provide leading practice recommendations to senior management to help improve the quality and effectiveness of the IT governance initiatives implemented.

Audit is an entity that monitors compliance, and, therefore, helps ensure compliance with EGIT initiatives implemented within an enterprise. The continual monitoring, analysis and evaluation of metrics associated with EGIT initiatives require an independent and balanced view to ensure a qualitative assessment that facilitates the qualitative improvement of IT processes and associated EGIT initiatives.

Reporting on EGIT involves auditing at the highest level in the enterprise and may cross divisional, functional or departmental boundaries. An audit charter stating the authority that audit has to move freely within the enterprise should be in place and approved by the audit governing body (i.e., the Audit Committee). With the charter in place, audit can undertake an engagement related to EGIT with more detailed boundaries. The IS auditor should confirm that the terms of reference for the audit state the following:
- Scope of the work, including a clear definition of the functional areas and issues to be covered
- Reporting line to be used, where EGIT issues are identified to the highest level of the enterprise
- IS auditor's right of access to information both within the enterprise and from third-party service providers

The IS auditor's organizational status and skill sets should be considered for appropriateness regarding the nature of the planned audit. When this is deemed insufficient, an appropriate management level should consider hiring an independent third party to manage or perform the audit.

Under the defined role of the IS auditor, the following aspects related to EGIT need to be assessed:
- How enterprise governance and EGIT are aligned
- Alignment of the IT function with the enterprise mission, vision, values, objectives and strategies
- Achievement of performance objectives (e.g., effectiveness and efficiency) established by the business and the IT function
- Legal, environmental, information quality, fiduciary, security and privacy requirements
- The control environment of the enterprise
- The inherent risk within the IS environment
- IT investment/expenditure

Three Lines Model

Enterprise governance spans the entire enterprise, with different roles, each playing a part in the management of risk to the enterprise. As a best practice, the teams each have specific actions and responsibilities to the enterprise to ensure that control processes are designed appropriately and operating effectively. The practice is known as the Three Lines Model[20] (**figure 2.2**), developed by the IIA.

The first line of defense is the enterprise management function that is assumed to have a strong interest in the proper function of business processes. Controls, associated metrics and indicators, and regular reviews serve as means for identifying weaknesses or deficiencies. The implicit expectation is that the first line

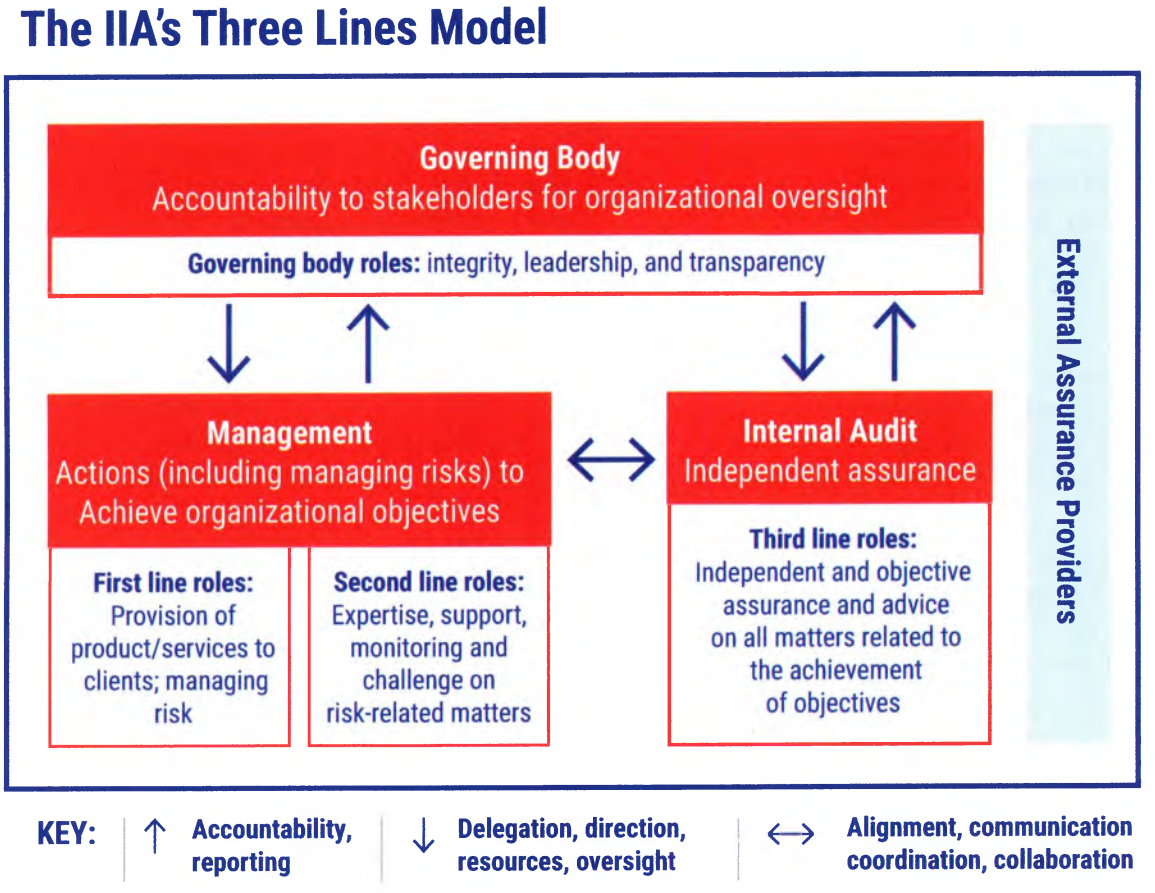
[20] The Institute of Internal Auditors, *The IIA's Three Lines Model*, USA, 2020, *https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf*

©ISACA. All Rights Reserved.

of defense will further identify necessary improvements to the enterprise's control environment.

Risk management, the second line of defense, is designed to evaluate independently any known or emerging risk. This is usually done using appropriate tools and methods for risk identification, analysis and treatment. The second line of defense partners with the first line to ensure that risk is identified, understood, documented and mitigated through the design and implementation of controls. More enterprises are establishing a second line of defense to mature their IT risk governance program.

Figure 2.2—Institute of Internal Auditors Three Lines Model



Source: The Institute of Internal Auditors, *The IIA's Three Lines Model*, 2020, *https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf*

Because of mandated independence, the risk management function may inform and assess management decisions and provide guidance, but it should not replace or overrule these decisions.

The third line of defense includes testing and assurance. The third line is the enterprise audit function and is independent, because auditors set their own audit programs and decide independently on the scope of their audits. This line of defense includes a separate reporting line to the audit committee within the enterprise.

IS audit's role in EGIT is to provide assurance that the enterprise is taking the necessary action to mitigate risk that would prevent the enterprise from achieving its objectives. They operate independently from the basic management structure, reporting their findings to the applicable oversight body (e.g., the audit committee).

 ©ISACA. All Rights Reserved.

2.2.4 Information Security Governance

The strategic direction of a business is defined by business goals and objectives. Information security must support business activities to be of value to the enterprise. Information security governance is a subset of corporate governance that provides strategic direction for security activities and ensures that objectives are achieved. It ensures that information security risk is appropriately managed and enterprise information resources are used responsibly. According to the US National Institute of Standards and Technology (NIST):

> *Information security governance can be defined as the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.* [21]

Management must establish and maintain a framework to guide the development and management of a comprehensive information security program that supports business objectives, to achieve effective information security governance.

An information security governance framework generally consists of the following elements:

- A comprehensive security strategy intrinsically linked with business objectives
- Governing security policies that address each aspect of strategy, controls and regulation
- A complete set of standards for each policy to ensure that procedures and guidelines comply with the policy
- An effective security organizational structure void of conflicts of interest
- Institutionalized monitoring processes to ensure compliance and provide feedback on effectiveness

This framework provides the basis for developing a cost-effective information security program that supports the enterprise's business goals. The objective of the information security program is a set of activities that provides assurance that information assets are given a level of protection commensurate with their value or the risk that their compromise poses to the enterprise.

Effective Information Security Governance

Because of its prominent role within IT governance processes, information security governance has risen to one of the highest levels of focused activity with specific value drivers: confidentiality, integrity, availability of information, continuity of services and protection of information assets. Security has become a significant governance issue due to global networking, rapid technological innovation and change, increased dependence on IT, increased sophistication of threat agents and exploits, and an extension of the enterprise beyond its traditional boundaries. Therefore, information security is an important and integral part of IT governance. Negligence in this regard will diminish an organization's capacity to mitigate risk and take advantage of IT opportunities for business process improvement.

Globally, boards of directors and CEOs are accountable and responsible for information security governance. The CEO is accountable to the board of directors for information security governance and responsible for its discharge through executive management, the organization and the resources under the CEO's charge.

The members of senior management who approve security policies should come from various operations and staff functions within the enterprise to ensure a fair representation of the enterprise. This minimizes potential bias toward a specific business priority, technology overhead or security concerns. Typically, the board-level committee approving security policies may include directors, the CEO, the chief operating officer (COO), the chief financial officer (CFO), the chief risk officer (CRO), the chief information officer (CIO), the chief technology officer (CTO), the head of HR, the chief of audit, the chief compliance officer (CCO) and legal. To the greatest extent possible, policy approval should be based on consensus.

Information is a key resource for all enterprises. From the time that information is created or received to the moment that it is disposed of (e.g., destroyed, erased, sanitized, etc.), technology plays a significant role. IT is increasingly advanced and pervasive in enterprise, social, public and business environments. As a result, enterprises and their executives strive to accomplish the following:

- Maintain high-quality information to support business decisions

[21] National Institute of Standards and Technology, *Special Publication 800-100: Information Security Handbook: A Guide for Managers*, USA, 7 March 2007, *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf*

©ISACA. All Rights Reserved.

- Generate business value from IT-enabled investments (i.e., achieve strategic goals and realize business benefits through effective and innovative use of IT)
- Achieve operational excellence through the reliable and efficient application of technology
- Maintain IT-related risk at an acceptable level
- Optimize the cost of IT services and technology
- Comply with ever-increasing relevant laws, regulations, contractual agreements and policies

Until recently, protection efforts have focused on the information systems that collect, process and store information rather than the information itself. This approach has become too narrow to accomplish the necessary overall security. Information security takes the broader view that data and the information and knowledge based on them must be adequately protected regardless of where they are created, received, processed, transported, or stored and disposed of. This applies particularly to situations where data are shared easily over the Internet through blogs, newsfeeds, peer-to-peer or social networks or websites. Thus, the reach of protection efforts should encompass the process that generates the information and the continued preservation of information generated due to the controlled processes.

Some significant trends that global business is experiencing include outsourcing in-house processes and increased use of cloud computing. Information security coverage extends beyond the geographic boundary of the enterprise's premises in onshoring and offshoring models.

The primary outcomes of effective information security governance include strategic alignment, risk management, compliance and value delivery. These outcomes are enabled through the development of the following:

- **Performance measurement**—Measurement, monitoring and reporting on information security processes to ensure that specific, measurable, attainable, realistic and timely (SMART) objectives are achieved. The following should be accomplished to achieve performance measurement:
  - A defined, agreed-on and meaningful set of metrics adequately aligned with strategic objectives
  - A measurement process that will help identify shortcomings and provide feedback on progress made in resolving issues
  - Independent assurance provided by external assessments and audits
- **Resource management**—Use of information security knowledge and infrastructure efficiently and effectively. The following should be considered related to resource management:
  - Ensure that knowledge is captured and available.
  - Document security processes and practices.
  - Develop security architecture(s) to define and use infrastructure resources efficiently.
- **Process integration**—A focus on integrating an enterprise's management assurance processes for security. Security activities are sometimes fragmented and segmented into silos with different reporting structures. This makes it difficult, if not impossible, to seamlessly integrate them. Process integration serves to improve overall security and operational efficiencies.

2.2.5 Information Systems Strategy

Information systems are crucial in enterprises' support, sustainability and growth. Previously, governing boards and senior management executives could minimize their involvement in the direction and development of IS strategy, leaving most decisions to functional management. However, this approach is no longer acceptable or possible with increased or total dependency on IS for day-to-day operations and successful growth. With the near-complete dependence on IS for functional and operational activities, enterprises face numerous internal and external threats, ranging from IS resource abuse to cybercrime, fraud, errors and omissions. IS strategic processes are integral components within the enterprise's governance structure to provide reasonable assurance that both existing and emerging business goals and objectives will be attained as critical facilitators for enhancing competitive advantage.

2.2.6 Strategic Planning

Strategic planning from an IS standpoint relates to the enterprise's long-term direction in leveraging IT to improve its business processes. Under the responsibility of top management, factors for consideration include identifying cost-effective IT solutions in addressing problems and opportunities that confront the enterprise and developing action plans for identifying and acquiring needed resources. In developing strategic plans, enterprises should ensure that the plans are fully aligned and consistent with the overall enterprise goals and objectives. IT department management, the IT steering committee and the strategy committee (which provides valuable strategic input related to stakeholder value) play key roles in developing and implementing plans.

 ©ISACA. All Rights Reserved.

The frequency of strategic planning depends on various factors, such as the nature of the enterprise, industry dynamics, market conditions and the pace of change in the external environment. Although the traditional approach has been to develop strategic plans every three to five years, there is growing recognition that this may not be sufficient in today's rapidly evolving business landscape.

In dynamic industries where disruptive technologies and market trends can quickly reshape the competitive landscape, enterprises often need to reassess and adjust their strategies more frequently. Some enterprises adopt an approach known as an agile strategy or strategic agility, where strategic planning is conducted continuously, with shorter time horizons, to enable faster responses to changing conditions.

Additionally, enterprises operating in highly uncertain or volatile environments may benefit from more frequent strategic reviews. This allows them to monitor shifts in customer preferences, technological advancements, regulatory changes or geopolitical developments and make timely adjustments to their plans.

Ultimately, the appropriate frequency of strategic planning will depend on each organization's specific circumstances and needs. Striking a balance between the need for agility and the need for stability and long-term vision is important. Regular monitoring and periodic strategic plan reviews can help to ensure its relevance and effectiveness.

Effective IS strategic planning involves consideration of the enterprise's requirements for new and revised information systems and the IT organization's capacity to deliver new functionality through well-governed projects. Determining requirements for new and revised information systems involves systematically considering the enterprise's strategic intentions, how these translate into specific objectives and business initiatives and what IT capabilities will be needed to support them.

In assessing IT capabilities, the existing system's portfolio should be reviewed regarding functional fit, cost and risk. Assessing IT's capacity to deliver involves reviewing the enterprise's technical IT infrastructure and key support processes (e.g., project management, software development, maintenance practices, security administration and help desk services) to determine whether expansion or improvement is necessary. The strategic planning process must encompass the delivery of new systems and technology and consider the return on investment (ROI) on existing IT and the decommissioning of legacy systems. The strategic IT plan should balance the cost of maintenance of existing systems against the cost of new initiatives or systems to support business strategies.

IS auditors should pay full attention to the importance of IS strategic planning, taking management control practices into consideration. IT strategic plans should be synchronized with the overall business strategy. IS auditors must focus on the importance of a strategic planning process or framework. Particular attention should be paid to assessing how operational, tactical or business development plans from the business are considered in IT strategy formulation, contents of strategic plans, requirements for updating and communicating plans, and monitoring and evaluation requirements. IS auditors should also consider how the CIO or senior IT management creates the overall business strategy. A lack of IT involvement in the creation of the business strategy indicates a risk that the IT strategy and plans will not be aligned with the business strategy.

2.2.7 Business Intelligence

Organizations need comprehensive, organized data to support the strategic planning process. Business intelligence (BI) is important to strategic planning because it provides management with the data and insights they need to make informed decisions about their future. BI tools can help businesses to:

- **Identify trends and patterns**—BI can help businesses to identify trends and patterns in their data that they may not be able to uncover otherwise. This information can be used to develop new strategies and opportunities.
- **Understand customer behavior**—BI can help businesses to understand customer behavior better, including their needs, wants and preferences. This information can be used to improve products and services, and to develop more effective marketing campaigns.
- **Assess performance**—BI can help businesses to assess their performance and identify areas where they can improve. This information can be used to set realistic goals and to track progress over time.
- **Make better decisions**—By providing businesses with the data and insights they need, BI can help them to make better decisions about their future. This can lead to improved financial performance, increased customer satisfaction and a more competitive advantage.

Investments in BI technology can be applied to enhance understanding of a wide range of business

©ISACA. All Rights Reserved.

questions. Some typical areas in which BI is applied for measurement and analysis purposes include the following:

- Process cost, efficiency and quality
- Customer satisfaction with product and service offerings
- Customer profitability, including the determination of which attributes are useful predictors of customer profitability
- Staff and business unit achievement of key performance indicators
- Risk management (e.g., by identifying unusual transaction patterns and accumulation of incident and loss statistics)

The interest in BI as a distinct field of IT activity is due to several factors:

- **The increasing size and complexity of modern enterprises**—The result is that even fundamental business questions cannot be properly answered without establishing serious BI capability.
- **Pursuit of competitive advantage**—Most enterprises have automated their basic, high-volume activities for many years. Significant enterprise-wide IT investment, such as enterprise resource planning (ERP) systems, is now commonplace. Many enterprises are increasing their investment in cloud-based technology to distribute products/services and for supply chain integration. Investment in IT to maintain and extend enterprise knowledge capital represents a new opportunity to use technology to gain an advantage over competitors.
- **Legal requirements**—Legislation exists to enforce the need for enterprises to understand the whole of the business. Financial institutions must now be able to report on all accounts/instruments belonging to their customers and all transactions against those accounts/instruments, including any suspicious transaction patterns.

Enterprises must design and implement (progressively, in most cases) a data architecture to deliver effective BI. A complete data architecture consists of two components:

- Enterprise data flow architecture (EDFA)
- Logical data architecture

An example of optimized EDFA is depicted in **figure 2.3**. Explanations of the various layers/components of this data flow architecture follow:

- **Presentation/desktop access layer**—This is where end users directly deal with information. This layer includes familiar desktop tools, such as spreadsheets, direct querying tools, reporting and analysis suites, and purpose-built applications, such as balanced scorecards (BSCs) and digital dashboards. Power users can build their own queries and reports, while others will interact with the data in predefined ways.
- **Data source layer**—Enterprise information derives from several sources: operational, external and nonoperational data.
- **Core data warehouse**—A core data warehouse is where all (or at least the majority of) the data of interest to an enterprise are captured and organized to assist reporting and analysis. data warehouses are normally instituted as large relational databases. While there is no unanimous agreement, many pundits suggest that the data warehouse should hold fully normalized data to support the flexibility to deal with complex and changing business structures.
- **Data mart layer**—Data marts represent subsets of information from the core data warehouse selected and organized to meet the needs of a particular business unit or business line. Data marts may be relational databases or online analytical processing (OLAP) data structures (a data cube). Data marts have a simplified structure compared to the normalized data warehouse.
- **Data staging and quality layer**—This layer is responsible for data copying, transformation into data warehouse format and quality control (QC). Only reliable data must get loaded to the core data warehouse. This layer needs to be able to deal with problems periodically thrown up by operational systems, such as changes to account number formats and the reuse of old account and customer numbers (when the data warehouse still holds information on the original entity).
- **Data access layer**—This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoids the need to know exactly how these data stores are organized.
- **Data preparation layer**—This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is precalculating the values loaded into OLAP data repositories to increase access speed. Specialist data mining also normally requires the preparation of data. Data mining explores large volumes of data to determine patterns and trends of information.
- **Metadata repository layer**—Metadata is data about data. The information held in the metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the

 ©ISACA. All Rights Reserved.

various layers, including documenting transformation and validation rules. Ideally, information in the metadata layer can be directly sourced by software operating in the other layers, as required.

- **Warehouse management layer**—The function of this layer is scheduling the tasks necessary to build and maintain the data warehouse and populate data marts. This layer is also involved in the administration of security.
- **Application messaging layer**—This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses the generation, storage and targeted communication of control messages.
- **Internet/intranet layer**—This layer is concerned with basic data communication, which includes browser-based user interfaces and Transmission Control Protocol/Internet Protocol (TCP/IP) networking.

The construction of the logical data architecture for an enterprise is a major undertaking that would normally be undertaken in stages. One reason for separating logical data model determination by business domain is that different parts of large business organizations often deal with different transaction sets, customers and products.

Ultimately, the data architecture must be structured to efficiently accommodate enterprise needs. Factors for consideration include the types of transactions in which the enterprise engages, the entities that participate in or form part of these transactions (e.g., customers, products, staff and communication channels) and the dimensions (hierarchies) that are important to the business (e.g., product and enterprise hierarchies).

With modern data warehouses, storage capacity is not really an issue. Therefore, the goal should be to obtain the most granular or atomic data possible. The lowest-level data are most likely to have attributes that can be used for analysis purposes that would be lost if summarized data are loaded.

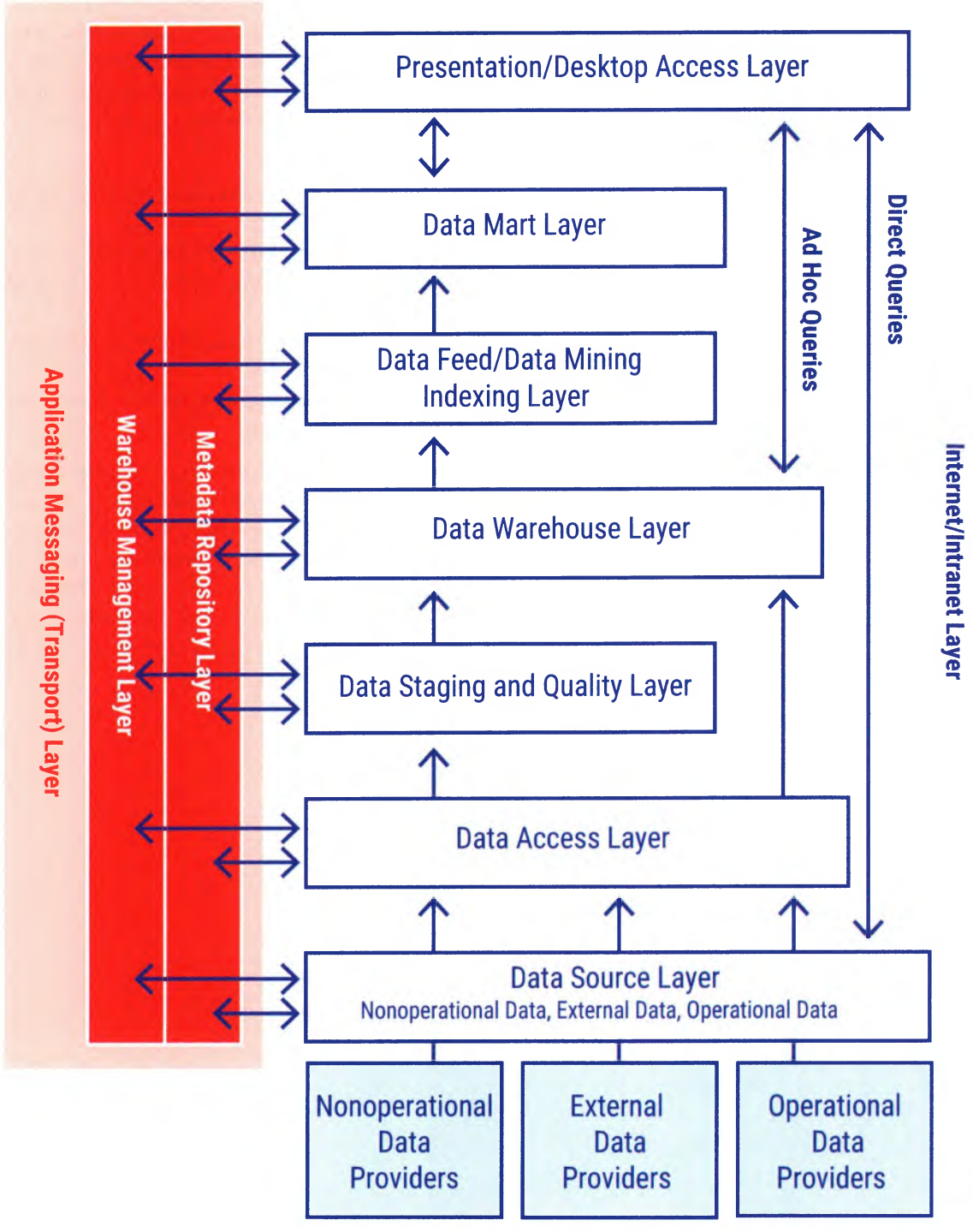
Various analysis models used by data architects/analysts include the following:

- **Context diagrams**—Outline the major processes of an enterprise and the external parties with which the business interacts.
- **Activity or swim-lane diagrams**—Deconstruct business processes.
- **Entity relationship diagrams**—Depict data entities and how they relate.

These data analysis methods are important in developing an enterprise data model. However, it is also crucial that knowledgeable business operatives be involved in the process. This way, a proper understanding of the business purpose and context of the data can be obtained. This also mitigates the risk of replicating suboptimal data configurations from existing systems and databases into the data warehouse.

©ISACA. All Rights Reserved.

Figure 2.3—Data Flow Architecture Sample



 ©ISACA. All Rights Reserved.

2.2.8 Organizational Structure

Organizational structure is a key component of governance. It identifies the key decision-making entities in an enterprise. The following section provides guidance for organizational structures, roles and responsibilities within EGIT. Actual structures may differ depending on an enterprise's size, industry and location.

IT Governing Committees

Traditionally, enterprises have had executive-level steering committees to handle IT issues that are relevant enterprisewide. There should be a clear understanding of the IT strategy and steering levels. ISACA has issued a document offering a clear analysis of the responsibilities of the IT steering committee as compared to the traditional IT strategy committee (**figure 2.4**). Enterprises may also have other committees guiding IT operations, such as an IT executive committee, IT governance committee, IT investment committee and/or IT management committee.

Note

The analysis of IT steering committee responsibilities is information that the CISA candidate should know.

Figure 2.4—Analysis of IT Steering Committee Responsibilities

Level	IT Strategy Committee	IT Steering Committee
Responsibility	• Provides insight and advice to the board on topics such as: • Relevance of developments in IT from a business perspective • Alignment of IT with business direction • Achievement of strategic IT objectives • Availability of suitable IT resources, skills and infrastructure to meet the strategic objectives • Optimization of IT costs, including the role and value delivery of external IT sourcing • Risk, return and competitive aspects of IT investments • Progress on major IT projects • Contribution of IT to the business (i.e., delivering the promised business value) • Exposure to IT risk, including compliance risk • Containment of IT risk • Direction to management relative to IT strategy • Drivers and catalysts for the board IT strategy	• Decides the overall level of IT spending and how costs will be allocated • Aligns and approves the enterprise IT architecture • Approves project plans and budgets, setting priorities and milestones • Acquires and assigns appropriate resources • Ensures that projects continuously meet business requirements, including a reevaluation of the business case • Monitors project plans to deliver expected value and desired outcomes on time and within budget • Monitors resource and priority conflict between enterprise divisions and the IT function and between projects • Makes recommendations and requests for changes to strategic plans (priorities, funding, technology approaches, resources, etc.) • Communicates strategic goals to project teams • Is a major contributor to management IT governance responsibilities and practices
Authority	• Advises the board and management on IT strategy • Is delegated by the board to provide input to the strategy and prepare its approval • Focuses on current and future strategic IT issues	• Assists the executive in the delivery of the IT strategy • Oversees day-to-day management of IT service delivery and IT projects • Focuses on implementation
Membership	• Board members and specialists who are not board members	• Sponsoring executive • Business executives (key users) • Chief information officer (CIO) • Key advisors as required (i.e., IT, audit, legal, finance)

©ISACA. All Rights Reserved.

Roles and Responsibilities of Senior Management and Boards of Directors

Information security governance requires strategic direction and impetus. It requires commitment, resources and assignment of responsibility for information security management and a means for the board to determine that its intent has been met.

Effective information security governance can be accomplished only by the involvement of the board of directors and/or senior management in approving policy; ensuring appropriate monitoring; and reviewing metrics, reports and trend analysis.

Board of Directors

Board members must know the enterprise's information assets and their criticality to ongoing business operations. This can be accomplished by periodically providing the board with the high-level results of comprehensive risk assessments and business impact analysis (BIA). It may also be accomplished by business dependency assessments of information resources. These activities should include approval by board members to assess key assets to be protected, which helps ensure that protection levels and priorities are appropriate to a standard of due care.

The tone at the top must be conducive to effective security governance. It is unreasonable to expect lower-level personnel to abide by security measures if they are not exercised by senior management. Senior management endorsement of intrinsic security requirements ensures that security expectations are met at all enterprise levels. Penalties for noncompliance must be defined, communicated and enforced from the board level down.

The board of directors is the accountable and liable body for the enterprise. Accountability means the board is responsible for ensuring that the enterprise follows the laws, behaves ethically and makes effective use of its resources.

Senior Management

Implementing effective security governance and defining the strategic security objectives of an enterprise is a complex task. As with any other major initiative, it must have leadership and ongoing support from executive management to succeed. Developing an effective information security strategy requires integrating with and cooperating with business process owners. A successful outcome aligns information security activities to support business objectives. The extent to which this is achieved will determine the cost-effectiveness of the information security program in achieving the desired objective of providing a predictable, defined level of assurance for business information and processes and an acceptable level of impact from adverse events.

Information Security Standards Committee

Security affects all aspects of an enterprise to some extent, and it must be pervasive throughout the enterprise to be effective. To ensure that all stakeholders impacted by security considerations are involved, many enterprises use a steering committee comprised of senior representatives of affected groups. This facilitates achieving consensus on priorities and trade-offs. It also serves as an effective communication channel. It provides an ongoing basis for ensuring the alignment of the security program with business objectives. It can also be instrumental in modifying behavior toward a culture more conducive to good security.

The chief information security officer (CISO) will primarily drive the information security program to have sensible policies, standards, procedures and processes that are implementable and auditable and to achieve a balance of performance about security. However, involving the affected groups in a deliberating committee, which may be called the information security standards committee (ISSC), is necessary. The ISSC includes members from C-level executive management and senior managers from IT, application owners, business process owners, operations, HR, audit and legal. The committee will deliberate on the suitability of recommended controls and good practices in the enterprise's context, including the secure configuration of operating systems (OSs) and databases. The auditor's presence is required to make the systems auditable by providing suitable audit trails and logs. Legal is required to advise on liability and conflicts with the law. This is not a prescriptive list of members to be included in the ISSC. Members of the committee may be modified to suit the context of the enterprises, and other members may be co-opted as necessary to suit the control objectives in question.

Chief Information Security Officer

All organizations have a CISO, whether anyone holds the exact title. The responsibilities may be performed by the CIO, CTO, CFO or, in some cases, the CEO, even when an information security office or director is in place. The scope and breadth of information security are such that the authority required and the responsibility taken will inevitably make it a senior officer or top management responsibility. This could include a position such as a

 ©ISACA. All Rights Reserved.

CRO or a CCO. Legal responsibility will, by default, extend up the command structure and ultimately reside with senior management and the board of directors.

Failure to recognize this and implement appropriate governance structures can make senior management unaware of this responsibility and the related liability. It also usually results in a lack of effective alignment of business objectives and security activities. Increasingly, prudent management is elevating the position of information security officer to senior management as enterprises increasingly recognize their dependence on information and its growing threats.

IT Steering Committee

Enterprise senior management should appoint a planning or steering committee to oversee the IT function and its activities.

A high-level steering committee for information systems is an important factor in ensuring that the IT department is in harmony with the enterprise's mission and objectives. Although not a common practice, it is highly desirable that a member of the board of directors who understands the risk and issues is responsible for IT and is chair of this committee. The committee should include representatives from senior management, each line of business, enterprise departments, such as HR and finance, and the IT department.

The committee's duties and responsibilities should be defined in a formal charter. Committee members should know IT departmental policies, procedures and practices. They should have the authority to make decisions within the group for their respective areas.

This committee typically serves as a general review board for major IS projects. It should not become involved in routine operations. Primary functions performed by this committee include:

- Reviewing the IT department long- and short-range plans to ensure that they align with the enterprise objectives
- Reviewing and approving major acquisitions of hardware and software within the limits approved by the board of directors
- Approving and monitoring major projects and the status of IS plans and budgets, establishing priorities, approving standards and procedures, and monitoring overall IS performance
- Reviewing and approving sourcing strategies for select or all IS activities, including insourcing or outsourcing, and the globalization or offshoring of functions
- Reviewing the adequacy of resources and allocation of resources in terms of time, personnel and equipment
- Making decisions regarding centralization versus decentralization, and assignment of responsibility
- Supporting development and implementation of an enterprise-wide information security management program
- Reporting to the board of directors on IS activities

Note

Responsibilities will vary from enterprise to enterprise; the responsibilities listed are the most common responsibilities of the IT steering committee. Each enterprise should have formally documented and approved terms of reference for its steering committee. IS auditors should familiarize themselves with the IT steering committee documentation and understand the major responsibilities assigned to its members. Many enterprises may refer to this committee by a different name. The IS auditor needs to identify the group that performs the previously mentioned functions.

Matrix of Outcomes and Responsibilities

The relationships between the outcomes of effective security governance and management responsibilities are shown in **figure 2.5**. This matrix is not meant to be comprehensive. It is intended merely to indicate some primary tasks and the management level responsible for them. Depending on the nature of the enterprise, the titles may vary. The roles and responsibilities should exist even if different labels are used.

Note

Although **figure 2.5** is not specifically tested in the CISA exam, the CISA candidate should be aware of this information.

©ISACA. All Rights Reserved.

Figure 2.5—Relationships of Security Governance Outcomes to Management Responsibilities

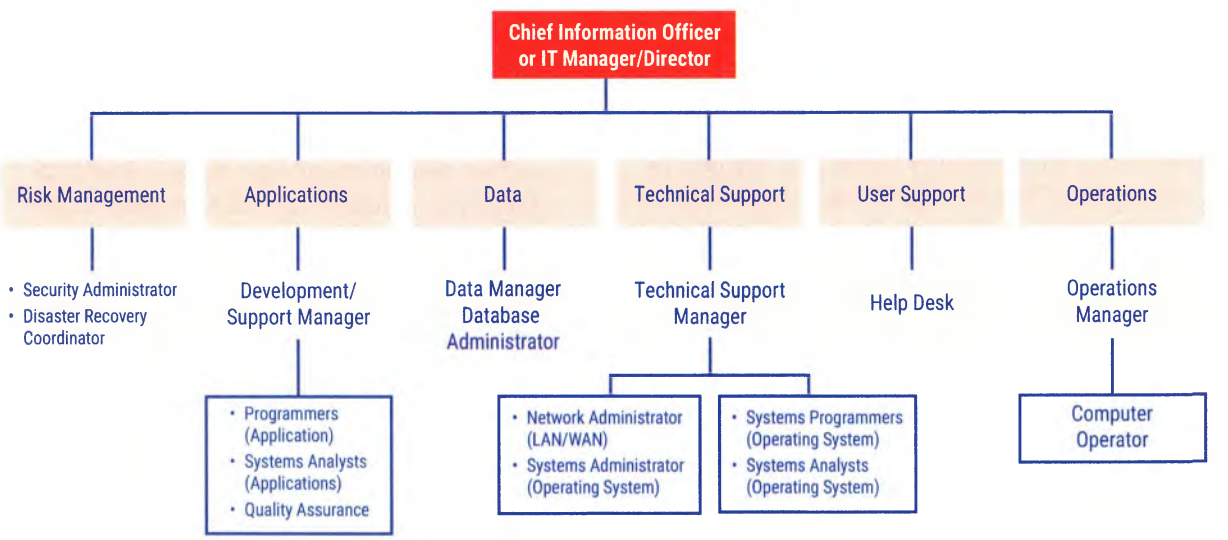
Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	Process Assurance
Board of directors	Require demonstrable alignment	• Establish risk tolerance • Oversee a policy of risk management • Ensure regulatory compliance	Require reporting of security activity costs	Require reporting of security effectiveness.	Oversee a policy of knowledge management and resource utilization	Oversee a policy of assurance process integration
Executive management	Institute processes to integrate security with business objectives	• Ensure that roles and responsibilities include risk management in all activities • Monitor regulatory compliance	Require business case studies of security activities	Require monitoring and metrics for security initiatives	Ensure processes for knowledge capture and efficiency metrics	Provide oversight of all assurance functions and plans for integration
Steering committee	• Review and assist security strategy and integration efforts • Ensure that business owners support integration	Identify emerging risk, promote business unit security practices and identify compliance issues	Review and advise on the adequacy of security initiatives to serve business functions	Review and advise whether security initiatives meet business objectives	Review processes for knowledge capture and dissemination	• Identify critical business processes and assurance providers • Direct assurance integration efforts
CISO/ information security management	Develop the security strategy, oversee the security program and initiatives, and liaise with business process owners for ongoing alignment	• Ensure that risk and business impact assessments are conducted • Develop risk mitigation strategies • Enforce policy and regulatory compliance	Monitor utilization and effectiveness of security resources	Develop and implement monitoring and metrics approaches, and direct and monitor security activities	Develop methods for knowledge capture and dissemination and metrics for effectiveness and efficiency	• Liaise with other assurance providers • Ensure that gaps and overlaps are identified and addressed
Audit executives	Evaluate and report on the degree of alignment	Evaluate and report on enterprise risk management (ERM) practices and results	Evaluate and report on efficiency	Evaluate and report on the effectiveness of measures in place and metrics in use	Evaluate and report on efficiency or resource management	Evaluate and report on the effectiveness of assurance processes performed by different management areas

 ©ISACA. All Rights Reserved.

IT Organizational Structure and Responsibilities

An IT department can be structured in different ways. One such format is shown in **figure 2.6**. The organizational chart depicted includes security, applications development and maintenance functions; technical support for network and systems administration; and operations. The organizational structure shows the IT department typically headed by an IT manager/director or, in large enterprises, by a CIO.

Figure 2.6—IT Department Organization



Note

The CISA exam does not test specific job responsibilities, because they may vary among enterprises. However, universally known responsibilities such as business owners, information security functions and executive management might be tested, especially when access controls and data ownership are tested. A CISA should be familiar with separation of duties (SoD).

Data Ownership

Data ownership refers to the classification of data elements and the allocation of responsibility for ensuring that they are kept confidential, complete and accurate. A key point of ownership is that accountability is established by assigning responsibility for protecting data to particular employees. The IS auditor can use this information to determine if proper ownership has been assigned and whether the data owner is aware of the assignment. The IS auditor should also review a sample of job descriptions to ensure that responsibilities and duties are consistent with the information security policy. The auditor should review the classification of data and evaluate their appropriateness, as they relate to the area under review.

Responsibilities include identifying and classifying data based on associated risk, authorizing access to data, review access controls, determine protection mechanism for data owned by them. In short, data owners are responsible for the security of data throughout the life cycle of that data—from origination to disposal.

Data Owners

Data owners are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur and regularly reviewing access rules for the data for which they are responsible.

Data Custodians

Data custodians are responsible for storing and safeguarding the data and include IS personnel, such as systems analysts and computer operators.

©ISACA. All Rights Reserved.

Security Administrator

Security administrators are responsible for providing adequate physical and logical security for IS programs, data and equipment. Physical security may be handled by someone other than the security administrator. Normally, the information security policy will provide the basic guidelines under which the security administrator will operate.

New IT Users

In general, all new users who are assigned PCs or other IT resources should sign a document stating the main IT security obligations that they are thereby engaged to know and observe. These obligations are:

- Read and agree to follow security policies.
- Keep logon IDs and passwords secret.
- Create quality passwords according to policy.
- Lock terminal screens when not in use.
- Report suspected violations of security.
- Maintain good physical security—keep doors locked, safeguard access keys, do not disclose access door lock combinations and question unfamiliar people.
- Conform to applicable laws and regulations.
- Use IT resources only for authorized business purposes.

Data Users

Data users include internal and external user communities. Their access levels should be authorized by the data owners and restricted and monitored by the security administrator. Their responsibilities regarding security are to be vigilant regarding the monitoring of unauthorized people in the work areas and comply with general security guidelines and policies.

Documented Authorizations

Data access should be identified and authorized in writing. The IS auditor can review a sample of these authorizations to determine if the proper level of written authority was provided. If the facility practices data ownership, only the data owners provide written authority.

IT Roles and Responsibilities

An organizational chart is important for all employees because it clearly defines the department's hierarchy and authority. Additionally, job descriptions; responsible, accountable, consulted, informed (RACI) charts; and swimlane workflow diagrams provide IT department employees a more complete and clear direction regarding their (and others') roles and responsibilities. The IS auditor should spend time in an auditee's area to observe and determine whether the formal job description and structures coincide with actual ones and are adequate. Generally, the following IT functions should be reviewed:

- **Systems development manager**—Systems development managers are responsible for programmers and analysts who implement and maintain new systems.
- **Project management**—Project managers are responsible for planning and executing IS projects. They may report to a project management office or to the development organization. Project management staff use budgets assigned to them to deliver IS initiatives and report on project progress to the IT steering committee. Project managers play a central role in executing the vision of the IT strategy and IT steering committees by planning, coordinating and delivering IT projects to the enterprise.
- **Help desk (service desk)**—More and more enterprises find a help desk function critical for their IT departments. A help desk is a unit within an enterprise that responds to technical questions and problems users face. Most software companies have help desks. Questions and answers can be delivered by telephone, fax, email or instant messaging. Help desk personnel may use third-party help desk software to quickly find answers to common questions. A procedure to record the problems reported, solved and escalated should be in place to analyze the problems/questions. It helps monitor the user groups and improves the software/information processing facility (IPF) services. Help desk/support administration includes the following activities:
  - Acquire hardware/software (HW/SW) for end users.
  - Assist end users with HW/SW difficulties.
  - Train end users to use HW/SW and databases; answer end-user queries.
  - Monitor technical developments and inform end users of pertinent developments.
  - Determine the source of problems with production systems and initiate corrective actions. Inform end users of problems with HW/SW or databases that could affect their control of installing HW/SW upgrades.
  - Initiate changes to improve efficiency.
- **End user**—End users are responsible for operations related to business application services. There is a small distinction between the terms end user and user. An end user is slightly more specific and refers to someone who accesses a business application. User is

 ©ISACA. All Rights Reserved.

broader and can refer to administrative accounts and accounts to access platforms.
- **End-user support manager**—The end-user support manager is a liaison between the IT department and the end users.
- **Data management**—Data management personnel are responsible for the data architecture in larger IT environments and manage data as corporate assets.
- **Quality assurance (QA) manager**—The QA manager is responsible for negotiating and facilitating quality activities in all areas of IT.
- **Information security management**—This function generally needs to be separate from the IT department and headed by a CISO. The CISO may report to the CIO or have a dotted-line (indirect reporting) relationship with the CIO. Even when the security officer reports to the CIO, there is a possibility of conflict because the goals of the CIO are to efficiently provide continuous IT services. In contrast, the CISO may be less interested in cost reduction if this impacts the quality of protection.

Vendor and Outsourcer Management

With the increase in outsourcing, including using multiple vendors, dedicated staff may be required to manage the vendors and outsourcers. This may necessitate staff performing the following functions:
- Acting as the prime contact for the vendor and outsourcer within the IT function
- Providing direction to the outsourcer on issues and escalating internally within the enterprise and IT function
- Monitoring and reporting on the service levels to management
- Reviewing changes to the contract due to new requirements and obtaining IT approvals

Infrastructure Operations and Maintenance

An operations manager is responsible for computer operations personnel, including all the staff required to run the data center efficiently and effectively (e.g., computer operators, librarians, schedulers and data control personnel). The data center includes the servers and mainframe; peripherals, such as high-speed printers; networking equipment; magnetic media; and storage area networks. The data center constitutes a major asset investment and impacts the enterprise's functioning ability.

The control group is responsible for the collection, conversion and control of input and the balancing and distribution of output to the user community. The supervisor of the control group usually reports to the IPF operations manager. The input/output control group should be in a separate area where only authorized personnel are permitted because they handle sensitive data.

Media Management

Media management must record, issue, receive and safeguard all program and data files maintained on removable media. Depending on the enterprise's size, this function may be assigned to a full-time individual or a member of operations who also performs other duties.

This is a crucial function. Therefore, many enterprises provide additional support through software that assists in maintaining inventory, movement, version control and configuration management.

Data Entry

Data entry is critical to information processing and includes batch or online entry. In most enterprises, user department personnel do their own online data entry. In many online environments, data are captured from the original source (e.g., electronic data interchange [EDI] input documents, data from bar codes for time management and departmental store inventory). The user department and the system application must have controls to ensure that data are validated, accurate, complete and authorized.

Supervisory Control and Data Acquisition

With the advancement of technology within industrial plants, enterprises are implementing operational technology for data acquisition. Industrial control system (ICS) is a general term that encompasses several types of control systems (for more information, see chapter 5 Protection of Information Assets). These systems include barcode readers or supervisory control and data acquisition (SCADA) systems. SCADA usually refers to centralized systems that monitor and control entire sites or complexes of systems spread out over large areas (e.g., across kilometers or miles). These systems are typical of industrial plants, steel mills, power plants, electrical facilities, etc. Most site control is performed automatically by remote terminal units (RTUs) or programmable logic controllers (PLCs). Host control functions are restricted to basic site overriding or supervisory-level intervention. An example of automated systems for data acquisition are those used on oil rigs to measure and control oil extraction and the temperature and flow of water. Data acquisition begins at the RTU or PLC level. It includes meter readings and equipment

©ISACA. All Rights Reserved.

status reports communicated to SCADA as required. Data are then compiled and formatted so that a control room operator using human-machine interfacing (HMI) networks can make supervisory decisions to adjust or override normal RTU or PLC controls. Data may also be fed to a history log, often built on a commodity database management system, to allow trending and another analytical auditing.

SCADA applications traditionally use dedicated communication lines, but there has been a significant migration to the Internet. This has obvious advantages, including easier integration into the enterprise business applications. However, a disadvantage is that many such enterprises are nation-critical infrastructures and become easy prey to cyberattacks.

Systems Administration

The systems administrator is responsible for maintaining major multiuser computer systems, including local area networks (LANs), wireless local area networks (WLANs), wide area networks (WANs), virtual machine/server/network environments, personal area networks (PANs), storage area networks (SANs), intranets and extranets and mid-range and mainframe systems. Typical duties include the following activities:

- Adding and configuring new workstations and peripherals
- Setting up user accounts
- Installing systemwide software
- Performing procedures to prevent/detect/correct the spread of viruses
- Allocating mass storage space

Small enterprises may have one systems administrator, whereas larger enterprises may have a team of them. Some mainframe-centric enterprises may refer to a systems administrator as a systems programmer.

Security Administration

Security administration begins with management commitment. Management must understand and evaluate security risk and develop and enforce a written policy that clearly states the standards and procedures to be followed. The duties of the security administrator should be defined in the policy. To provide adequate SoD, this individual should be a full-time employee who may report directly to the infrastructure director. However, in a small enterprise, it may not be practical to hire a full-time individual for this position. The individual performing the function should ensure that the various users comply with the enterprise's security policy and that controls are adequate to prevent unauthorized access to the company assets (including data, programs and equipment). The security administrator's functions usually include the following:

- Maintaining access rules to data and other IT resources
- Maintaining security and confidentiality over issuing and maintaining authorized user IDs and passwords
- Monitoring security violations and taking corrective action to ensure adequate security
- Periodically reviewing and evaluating the security policy and suggesting necessary management changes
- Preparing and monitoring the security awareness program for all employees
- Testing the security architecture to evaluate the security strengths and detect possible threats
- Work with compliance, risk management and audit functions to ensure that security is appropriately designed and updated based on audit feedback or testing

Database Administration

The database administrator (DBA), as custodian of the enterprise's data, defines and maintains the data structures in the enterprise database system. The DBA must understand the requirements of the enterprise and user data and data relationship (structure). This position is responsible for the security of the shared data stored on database systems. The DBA is responsible for the corporate databases' design, definition and proper maintenance. The DBA usually reports directly to the director of the IPF. The DBA's role includes:

- Specifying the physical (computer-oriented) data definition
- Changing the physical data definition to improve performance
- Selecting and implementing database optimization tools
- Testing and evaluating programming and optimization tools
- Answering programmer queries and educating programmers in database structures
- Implementing database definition controls, access controls, update controls and concurrency controls
- Monitoring database usage, collecting performance statistics and tuning the database
- Defining and initiating backup and recovery procedures

The DBA has the tools to establish controls over the database and the ability to override these controls. The DBA also can gain access to all data, including production data. It is usually not practical to prohibit

 ©ISACA. All Rights Reserved.

or completely prevent access to production data by the DBA. Therefore, the IT department must exercise close control over database administration through the following approaches:

- SoD
- Management approval of DBA activities
- Supervisor review of access logs and activities
- Detective controls over the use of database tools

Systems Analyst

Systems analysts are specialists who design systems based on the user's needs and are usually involved during the initial system development life cycle (SDLC) phase. These individuals interpret the user's needs and develop requirements, functional specifications and high-level design documents. These documents enable programmers to create a specific application.

Security Architect

Security architects evaluate security technologies; design security aspects of the network topology, access control, identity management and other security systems and establish security policies and requirements. One may argue that systems analysts perform the same role; however, the required skills are quite different. The deliverables (e.g., program specifications versus policies, requirements, architecture diagrams) differ. Security architects should also work with compliance, risk management and audit functions to incorporate their requirements and recommendations for security into the security policies and architecture.

System Security Engineer

The system security engineer, as defined under *ISO/IEC 21827:2008: Information technology—Security techniques—Systems Security Engineering—Capability Maturity Model*, provides technical information system security engineering support to the enterprise that encompasses the following:

- Project life cycles, including development, operation, maintenance and decommissioning activities
- Entire enterprises, including management, organizational and engineering activities
- Concurrent interactions with other disciplines, such as system software and hardware, human factors, test engineering, system management, operation and maintenance
- Interactions with other enterprises, including acquisition, system management, certification, accreditation and evaluation

Applications Development and Maintenance

Applications staff are responsible for developing and maintaining applications. Development can include developing new code or changing the existing setup or configuration of the application. Staff develop the programs or change the application setup to run in a production environment. Therefore, management must ensure that staff cannot modify production programs or application data. Staff should work in a test-only environment and deliver their work to another group to move programs and application changes into the production environment.

Infrastructure Development and Maintenance

Infrastructure staff are responsible for maintaining the systems software, including the OS. This function may require staff to have broad access to the entire system. IT management must closely monitor activities by requiring that electronic logs capture this activity and are not susceptible to alteration. Infrastructure staff should have access to only the system libraries of the specific software they maintain. Domain administration and superuser account usage should be tightly controlled and monitored.

Network Management

Many enterprises have widely dispersed IPFs. They may have a central IPF, but they also make extensive use of the following:

- LANs at branches and remote locations
- WANs, where LANs may be interconnected for ease of access by authorized personnel from other locations
- Wireless networks established through mobile devices

Network administrators are responsible for key components of this infrastructure (e.g., routers, switches, firewalls, network segmentation, performance management and remote access). Because of geographical dispersion, each LAN may need an administrator. Depending on the enterprise's policy, these administrators can report to the director of the IPF or, in a decentralized operation, may report to the end-user manager. However, at least a dotted line to the director of the IPF is advisable. This position is responsible for technical and administrative control over the LAN. This includes ensuring that transmission links function correctly, system backups occur and software/hardware purchases are authorized and installed properly. This person may be responsible for security administration over the LAN in smaller installations. The LAN administrator should have no application programming

©ISACA. All Rights Reserved.

responsibilities but may have systems programming and end-user responsibilities.

Separation of Duties Within IT

Actual job titles and organizational structures vary greatly from one enterprise to another, depending on the size and nature of the business. However, an IS auditor should obtain enough information to understand and document the relationships among the various job functions, responsibilities and authorities, and assess the adequacy of the SoD.

SoD avoids the possibility that a single person can be responsible for diverse and critical functions, so errors or misappropriations can occur and not be detected promptly and in the normal course of business processes.

SoD is an important means by which fraudulent and/or malicious acts can be discouraged and prevented. Duties that should be segregated include:

- Custody of the assets
- Authorization
- Recording transactions

If adequate SoD does not exist, the following can occur:

- Misappropriation of assets
- Misstated financial statements
- Inaccurate financial documentation (i.e., errors or irregularities)
- Undetected improper use of funds or modification of data
- Undetected, unauthorized or erroneous changes or modifications of data and programs

When duties are separated, access to the computer, production data library, production programs, programming documentation, and OS and associated utilities can be limited. The potential damage from the actions of any one person is, therefore, reduced. The IS and end-user departments should be organized to achieve adequate SoD. See **figure 2.7** for a guideline of the job responsibilities that should not be combined.

Figure 2.7—Segregation of Duties Control Matrix

	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database	Network	Systems	Security Administrator	Systems Programmer	Quality Assurance
Control Group		X	X	X		X	X	X	X	X		X	
Systems Analyst	X			X	X		X				X		X
Application Programmer	X			X	X	X	X	X	X	X	X	X	X
Help Desk and Support Manager	X	X	X		X	X		X	X	X		X	
End User		X	X	X			X	X	X			X	X
Data Entry	X		X	X			X	X	X	X	X	X	
Computer Operator	X	X	X		X	X		X	X	X	X	X	
Database Administrator	X		X	X	X	X	X		X	X		X	

 ©ISACA. All Rights Reserved.

Figure 2.7—Segregation of Duties Control Matrix (cont.)

	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database	Network	Systems	Security Administrator	Systems Programmer	Quality Assurance
Network Administrator	X		X	X	X	X	X	X					
System Administrator	X		X	X		X	X	X				X	
Security Administrator		X	X			X	X					X	
Systems Programmer	X		X	X	X	X	X	X		X	X		X
Quality Assurance		X	X		X							X	
X-Combination of these functions may create a potential control weakness.													

Note

The SoD control matrix (**figure 2.7**) is not an industry standard but a guideline indicating which positions should be separated and which require compensating controls when combined. The matrix illustrates potential SoD issues and should not be viewed or used as an absolute; rather, it should be used to help identify potential conflicts so that proper questions may be asked to identify compensating controls.

In actual practice, functions and designations may vary in different enterprises. Further, the risk may vary depending on the nature of the business processes and technology deployed. However, an IS auditor needs to understand the functions of each designation specified in this manual. IS auditors need to understand the risk of combining functions, as indicated in **figure 2.7**. In addition, depending on the complexity of the applications and systems deployed, an automated tool may be required to evaluate a user's access against an SoD matrix. Most tools come with a predefined SoD matrix that must be tailored to an enterprise's IT and business processes, including any additional functions or risk areas not included in the delivered SoD matrix.

Regarding privileged users of the system, remote logging (sending system logs to a separate log server) should be enabled so that the privileged users do not have access to their own logs. For example, the activities of the DBA may be remotely logged to another server where an official in the IT department can review/audit the DBA's actions. The activities of system administrators may be similarly monitored via the separation of log review duties on an independent log server.

Compensating controls are internal controls intended to reduce the risk of an existing or potential control weakness when duties cannot be appropriately segregated. The enterprise structure and roles should be considered when determining the appropriate controls for the relevant environment. For example, an enterprise may not have all the positions described in the matrix or one person may be responsible for many roles. The size of the IT department may also be an important factor that should be considered (i.e., certain combinations of roles in an IT department of a certain size should never be used). However, if combined roles are required for some reason, then compensating controls should be developed and put in place.

©ISACA. All Rights Reserved.

Separation of Duties Controls

Several control mechanisms can be used to strengthen SoD. The controls are described in the following sections.

Transaction Authorization

Transaction authorization is the responsibility of the user department. Authorization is delegated to the degree that it relates to the particular level of responsibility of the authorized individual in the department. Periodic checks must be performed by management and audit to detect the unauthorized entry of transactions.

Ownership of Assets

Ownership of enterprise assets must be determined and assigned appropriately. The data owner usually is assigned to a particular user department. That individual's duties should be specific and in writing. The data owner is responsible for determining authorization levels required to provide adequate security. At the same time, the administration group is often responsible for implementing and enforcing the security system.

Access to Data

Controls over access to data are provided by a combination of physical, system and application security in the user area and the IPF. The physical environment must be secured to prevent unauthorized personnel from accessing the various tangible devices connected to the central processing unit, thereby permitting access to data. System and application security are additional layers that may prevent unauthorized individuals from accessing enterprise data. Access to data from external connections continues to be a growing concern because of the Internet. Therefore, IT management has added responsibilities to protect information assets from unauthorized access.

Access control decisions are based on enterprise policy and two generally accepted standards of practice—SoD and least privilege. Controls for effective use must not disrupt the usual workflow more than necessary or place too much burden on auditors or authorized users. Further access must be conditional, and access controls must adequately protect the enterprise's resources.

Policies establish sensitivity levels—such as top secret, secret, confidential and unclassified—for data and other resources. These levels should be used for guidance on the proper procedures for handling information resources. The levels also may be used as a basis for access control decisions. Individuals are granted access to only those resources at or below a specific level of sensitivity. Labels are used to indicate the sensitivity level of electronically stored documents. Policy-based controls may be characterized as either mandatory or discretionary.

Authorization Forms

System owners must provide IT with formal authorization forms (either hard copy or electronic) that define each individual's access rights. In other words, managers must define who should have access to what. Authorization forms must be evidenced properly with management-level approval. Generally, all users should be authorized with specific system access via a formal request from management. In large enterprises or in those with remote sites, signature authorization logs should be maintained, and formal requests should be compared to the signature log. Access privileges should be reviewed periodically to ensure that they are current and appropriate to the user's job functions.

User Authorization Tables

The IT department should use the data from the authorization forms to build and maintain user authorization tables. These define who can update, modify, delete and/or view data. These privileges are provided at the system, transaction or field level. In effect, these are user access control lists. These authorization tables must be secured against unauthorized access by additional password protection or data encryption. A control log should record all user activity, and appropriate management should review this log. All exception items should be investigated.

Compensating Controls for Lack of Separation of Duties

In a small enterprise where the IT department may consist of only four or five people, compensating control measures must exist to mitigate the risk resulting from a lack of SoD. Before relying on system-generated reports or functions as compensating controls, the IS auditor should carefully evaluate the reports, applications and related processes for appropriate controls, including testing and access controls to make changes to the reports or functions. Compensating controls include the following:

- Audit trails are an essential component of all well-designed systems. Audit trails help the IT and user departments and the IS auditor by providing a map to retrace the transaction flow. Audit trails enable the user and IS auditor to recreate the actual transaction

 ©ISACA. All Rights Reserved.

flow from the point of origination to its existence on an updated file. Without adequate SoD, good audit trails may be an adequate compensating control. The IS auditor should be able to determine who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained and what files it updated.
- Reconciliation is ultimately the responsibility of the user department. In some enterprises, limited reconciliation of applications may be performed by the data control group using control totals and balance sheets. This independent verification type increases confidence that the application is processed successfully, and the data are balanced properly.
- Exception reporting should be handled at the supervisory level and require evidence, such as initials on a report, noting that the exception has been handled properly. Management should also ensure that exceptions are resolved promptly.
- Transaction logs may be manual or automated. An example of a manual log is a record of transactions (grouped or batched) before they are submitted for processing. An automated transaction log records all transactions processed and is maintained by the computer system.
- Supervisory reviews may be performed through observation and inquiry or remotely.
- Independent reviews are carried out to compensate for mistakes or intentional failures in following prescribed procedures. These reviews are particularly important when duties in a small organization cannot be appropriately segregated. Such reviews will help detect errors or irregularities.

2.2.9 Auditing IT Governance Structure and Implementation

Although many conditions concern the IS auditor when auditing the IT function, some of the more significant indicators of potential problems include the following:
- Excessive costs
- Budget overruns
- Late projects
- High staff turnover
- Inexperienced staff
- Frequent HW/SW errors
- An excessive backlog of user requests
- Slow computer response time
- Numerous aborted or suspended development projects
- Unsupported or unauthorized HW/SW purchases
- Frequent HW/SW upgrades
- Extensive exception reports
- Exception reports that were not followed up
- Lack of succession plans
- Reliance on one or two key personnel
- Lack of adequate training

Reviewing Documentation

IS auditors should review the following governance documents:
- IT strategies, plans and budgets
- Security policy documentation
- Organization/functional charts
- Job descriptions
- IT steering committee reports
- System development and program change procedures
- Operations procedures
- HR manuals
- QA procedures

The documents should be assessed to determine whether:
- They were created as management authorized and intended.
- They are current and up to date.

2.3 IT Policies, Standards, Procedures and Guidelines

Application of the terms policies, standards, procedures and guidelines vary widely. The definitions and interpretations used in this document agree with the major standard-setting bodies. These should be adopted to ensure clear communication. Policies and standards are considered tools of governance and management, respectively. Procedures and guidelines are the responsibility of operations.

2.3.1 Policies

Policies are high-level statements of management intent, expectations and direction. Well-developed high-level policies in a mature enterprise can remain static for extended periods. Policies can be considered the constitution of governance and must be clearly aligned with and support the strategic objectives of the enterprise.

Although high-level enterprise policies set the tone for the enterprise, individual divisions and departments should define lower-level policies. Lower-level policies apply to the employees and operations of these units and focus on the activity at the operational level. The lower-level policies should be consistent with and support the high-level policies.

Management should review all policies periodically. Ideally, these documents should specify who approved the policy and a review date, which the IS auditor

©ISACA. All Rights Reserved.

should check for currency. Policies must be updated regularly to reflect new technology, changes in the risk and control environment (e.g., regulatory compliance requirements) and significant changes in business processes. IS auditors should pay close attention to processes that take advantage of emerging technology for efficiency and effectiveness in productivity or for competitive gains. Policies must support the achievement of business objectives and should be reinforced through the implementation of IS controls. The broad policies at a higher level and the detailed policies at a lower level must align with the business objectives.

Because policies exist to support strategic objectives, IS auditors should consider policies within the audit scope and test the policies for compliance. Alternatively, suppose another assurance function tests policies for compliance. In that case, there may be an opportunity for IS auditors to rely on that work if it meets the standards of the audit department. IS controls should flow from the enterprise policies, and IS auditors should use policies as a benchmark for evaluating compliance. However, if a policy hinders the achievement of business objectives, this policy must be identified and reported for improvement. The IS auditor should also consider the extent to which policies apply to third parties or outsourced service providers (OSPs), the extent to which third parties or OSPs comply with the policies and whether the policies of the third parties or OSPs conflict with the enterprise's policies.

Information Security Policy

An information security policy (ISP) is a set of rules and/or statements that an enterprise develops to protect its information and related technology. A security policy for information and related technology helps guide behaviors. It is the foundation for building the security infrastructure for technology-driven enterprises. Policies will often set the stage regarding what tools and procedures are needed for the enterprise. ISPs must balance the level of control with the level of productivity. Also, the control cost should never exceed the expected benefit to be derived. The enterprise culture will play an important role in designing and implementing these policies. The ISP must be approved by senior management. It should be documented and communicated, as appropriate, to all employees, service providers and business partners (e.g., suppliers). IS auditors should use the ISP as a reference framework for performing various IS audit assignments. The adequacy and appropriateness of the security policy could also be an area of review for the IS auditor.

The ISP should state management commitment and outline the enterprise's approach to managing information security. The ISO/IEC 27001 standard (or equivalent standards) and the 27002 guidelines may be considered benchmarks for the content covered by the ISP document. Many enterprises model their ISP on the domains and major ISO/IEC 27001 subsections.

The policy document should generally contain the following elements:

- A definition of information security of the enterprise
- The scope and objectives of the policy document
- A statement of management's intent and expectations regarding information security
- Acknowledgment of the framework(s) used for setting control objectives and controls, including the expected structure for risk assessments and risk management
- A brief explanation of the information security policies, principles, standards and compliance requirements of particular importance to the enterprise, including:
  - Compliance with legislative, regulatory and contractual requirements
  - Information security education, training and awareness requirements
  - Business continuity management and disaster recovery plans
  - Consequences of information security policy violations
- A definition of general and specific responsibilities for information security management, including guidelines for reporting information security incidents
- References to supplemental documentation that may support the policy (e.g., more detailed security policies, standards and procedures for specific information systems or security rules with which users should comply)

The ISP should be communicated throughout the enterprise to users in a form that is accessible and understandable to the intended reader. The ISP might be a part of a general policy document. It may be suitable for distribution to third parties and outsourced service providers of the enterprise if care is taken not to disclose sensitive enterprise information. Some enterprises maintain a detailed ISP for internal use and a summary version for external distribution. All employees or third parties with access to information assets should be required to sign off on their understanding and willingness to comply with the ISP when hired and regularly after that (e.g., annually) to account for policy changes over time.

 ©ISACA. All Rights Reserved.

Depending upon the need and appropriateness, enterprises may document information security policies as a set of policies. Generally, the following policy concerns are addressed:

- A high-level information security policy should include confidentiality, integrity and availability statements.
- A data classification policy should describe the classifications, levels of control at each classification and responsibilities of all potential users, including ownership.
- An acceptable use policy that is comprehensive, and includes information for all information resources (e.g., hardware, software, networks, internet), and describes the enterprise permissions for using IT and information-related resources.
- An end-user computing policy describes users' parameters and usage of desktop, mobile computing and other tools, including using personal devices for enterprise business.
- Access control policies describe the method for defining and granting access to users to various IT resources, such as network access, application access and remote network access.
- An incident response policy that describes the steps to take in the event of a breach or attack, steps to take to minimize exposure and who to notify when the breach occurs.
- A remote access policy, or work-from-home (WFH) policy, sets expectations for remote security measures, public networks, home networks, VPN protocols and enterprise and customer data handling.

Review of the Information Security Policy

The ISP should have an owner who has approved management responsibility for developing, reviewing and evaluating the policy. The ISP should be reviewed at planned intervals (at least annually) or when significant changes to the enterprise, business operations or inherent security-related risk occur to ensure its suitability, adequacy and effectiveness. The review should include assessing opportunities for improvement to the enterprise's ISP and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

Maintaining and updating the ISP should consider the results of these reviews. The policy should be subjected to a defined management review procedure, including a schedule or period for the review, responsibility for updating the policy, final approval and distribution to internal and external stakeholders.

The input to the management review should include the following:

- Feedback from interested parties
- Results of independent reviews
- Status of preventive, detective and corrective actions
- Results of previous management reviews
- Process performance and ISP compliance
- Changes that can affect the enterprise's approach to managing information security, including changes to the organizational environment; business circumstances; resource availability; contractual, regulatory and legal conditions or technical environment
- Use of certain third-party relationships, outsourced service providers or offshoring of IT or business functions
- Trends related to threats and vulnerabilities
- Reported information security incidents
- Recommendations provided by relevant authorities, governing bodies or regulators

The output from the management review should include any decisions and actions related to the following:

- Improvement in the alignment of information security with business objectives
- Improvement of the enterprise's approach to managing information security and its processes
- Improvement to the risk assessment and risk management process
- Improvement of control objectives and controls
- Improvement in the allocation of resources and/or responsibilities

A record of management reviews should be maintained with version control numbers, revision dates and distribution dates. Management approval for the revised policy should be obtained.

Note

This review is performed by management to address the changes in environmental factors.

While reviewing the policies, the IS auditor needs to assess the following:

- Basis or framework on which the policy has been defined
- Appropriateness and completeness of the policies
- Contents of policies
- Exceptions to the policies, clearly noting in which area the policies do not apply and why (e.g., password policies may not be compatible with legacy applications)
- Policy approval process

©ISACA. All Rights Reserved.

- Policy implementation process
- Effectiveness of implementation of policies
- Awareness and training
- Periodic review and update process

2.3.2 Standards

A standard is a mandatory requirement, code of practice or specification approved by a recognized external standards organization. Within an enterprise, standards are the criteria used to determine whether procedures, processes or systems meet policy requirements. Where policies are the enterprise's constitution, standards are the laws used to measure policy compliance. Standards govern the creation of procedures and guidelines by setting the boundaries within which the procedures will operate, the security baselines and acceptable risk appetite as directed by management. Boundaries are generally set regarding allowable limits on processes, people and technologies.

Strong standards are necessary in current fast-moving environments. Standards help ensure the effectiveness and reliability of products and services. These are necessary for the trust and effectiveness needed to ensure continued growth. Standards are updated as needed to address the latest thinking and technology.

Note

Professional standards refer to standards issued by professional organizations, such as ISACA and the IIA, with related guidelines and techniques that assist the professional in implementing and complying with other standards.

2.3.3 Procedures

Procedures are documented, defined steps for achieving specific policy objectives. The procedures must be derived from the parent policy and reflect the spirit or intent of the policy statement while operating within the boundaries of the standards. Procedures must be written clearly and concisely to be easily and properly understood by those executing their steps. Procedures document business and aligned IT processes and embedded controls. Procedures typically are formulated by process owners as an effective translation of policies.

Generally, procedures are more dynamic than their respective parent policies. Procedures must reflect the regular changes in business, supporting IT systems and the compliance environment. As a result, frequent review and procedure updates are essential to remain relevant. IS auditors review procedures to identify controls, evaluate control design, test controls over the business and support IT processes. The controls embedded in procedures are evaluated to ensure that they fulfill necessary control objectives while making the process as efficient and practical as possible. Where operational practices do not match documented procedures or where documented procedures do not exist, the execution of the procedure may be inconsistent, especially as new employees are onboarded. A lack of documentation makes it difficult for management and auditors to identify and assess controls.

One of the most critical aspects of procedures is awareness by the individuals who rely on them. A procedure that is not thoroughly known by the personnel who use it is ineffective. Managers and process owners should use reliable deployment methods and automation to retain, distribute and manage IT procedures to ensure awareness. Although not as formal as policies, procedures should also go through change management steps for updates, approval and distribution.

When possible, procedures should be embedded in information systems to further integrate these procedures within the enterprise and to reduce deviation from expected procedural steps.

2.3.4 Guidelines

Guidelines for executing procedures are typically created by process owners to give more details to the individual following the procedure steps. Guidelines should contain information that will help execute the procedures, such as clarification of policies and standards, dependencies, suggestions and examples, narrative clarifying the procedures, background information that may be useful and tools that can be used. Guidelines can be useful in many other circumstances. They are considered here in the context of information security governance.

To combine these concepts and illustrate how this could look in practice, **figure 2.8** uses the common example system access to show how a policy, standard, procedure and guideline are connected, with each element building on the previous element.

 ©ISACA. All Rights Reserved.

Figure 2.8—Policy, Standard, Procedure and Guideline Examples

Policy	Information resources must be controlled to effectively prevent unauthorized access.
Standard	The enterprise has adopted the principle of least privilege, so only minimum system resources and authorizations should be granted, allowing the individual to perform their job function.
Procedure	Accounting department individuals are provided access to the accounts payable (AP) system based on their specific job title and role.
Guideline	Each accounting team member is assigned a specific job title and role that corresponds to the function they serve within the department. Access to the AP system has been configured to restrict access to only the functionality the individual needs to perform their job. Job changes and termination in the HR system will trigger a mandatory review by the person's manager. Failure to respond within five days results in the automatic revoking of access.

2.4 Enterprise Architecture and Considerations

With increasing complexity in the IT landscape within modern enterprises, there is a need for transparency related to enterprise architecture (EA). EA involves documenting the enterprise's IT assets in a structured manner to facilitate understanding, management and planning for IT investments. From an investment point of view, enterprises need to understand how their IT environment will be impacted by additional investment, and management needs to determine returns or losses on those investments.

The Framework for Enterprise Architecture: Background, Description and Utility[22], a groundbreaking work in the field of EA, was first published by John Zachman in the late 1980s. The Zachman framework continues to be a starting point for many contemporary EA projects. Zachman reasoned that constructing IT systems had considerable similarities to constructing a building. In building construction, one moves from the abstract to the physical using models and representations (e.g., blueprints, floor plans and wiring diagrams). Similarly, with IT, different artifacts (e.g., diagrams, flowcharts, data/class models and code) are used to convey different aspects of the enterprise's systems at progressively greater levels of detail. In both cases, various participants become involved at different project stages.

The basic Zachman framework is shown in **figure 2.9**.

Figure 2.9—Zachman Framework for Enterprise Architecture

	Data	Functional (Application)	Network (Technology)	People (Organization)	Process (Workflow)	Strategy
Scope						
Enterprise model						
Systems model						
Technology model						
Detailed representation						

The goal is to complete all cells of the matrix. At the outset of an EA project, most enterprises are expected to have difficulty providing details for every cell, particularly at the highest level. In attempting to complete an EA diagram, enterprises can address the challenge from either a technology or a business process perspective.

Completing an EA from a technology perspective attempts to clarify the complex technology choices faced by modern enterprises. The idea is to provide guidance on issues, such as when to use advanced technical environments (e.g., JavaEE or .NET) for application development, how to better connect intra- and inter-organizational systems, how to enable legacy and ERP

[22] Zachman, J.A.; The Framework for Enterprise Architecture: Background, Description and Utility, 2016, *https://zachman-feac.com/resources/ea-articles-reference/150-the-framework-for-enterprise-architecture-background-description-and-utility*

©ISACA. All Rights Reserved.

applications for web deployment without an extensive rewrite, whether to insource or outsource IT functions and when to use solutions such as virtualization and cloud computing.

An EA focused on business processes attempts to understand the enterprise's core value-adding and supporting processes. By understanding processes, the constituent parts and the technology that supports them, business improvement can be obtained as aspects are progressively redesigned and replaced. The enterprise's business process model can be mapped to the upper rows of the Zachman framework. After the mapping is completed, an enterprise can consider the optimal mix of technologies needed to support its business processes.

Other EA frameworks include The Open Group Architecture Framework (TOGAF), which provides a high-level approach for designing, planning, implementing and governing an enterprise information technology architecture, and Sherwood Applied Business Security Architecture (SABSA), which focuses on information security architecture.

When auditing infrastructure and operations, the IS auditor should follow the overall EA selected by the enterprise as a main source of information. Further, the IS auditor should ensure the systems align with the EA and meet the enterprise's objectives.

2.5 Enterprise Risk Management

From an IT perspective, ERM is the process of identifying vulnerabilities and threats to the information resources used by an enterprise in achieving business objectives and deciding what countermeasures (safeguards or controls), if any, to take in reducing risk to an acceptable level (i.e., residual risk), based on the value of the information resource to the enterprise.

ERM operates as a management function, not as an independent audit function like an internal audit. As such, ERM's role is to advise senior leaders on which strategy to use to reach the enterprise's acceptable risk level or risk appetite. A clear understanding of the enterprise's appetite for risk drives all risk management efforts and, in an IT context, impacts future investments in technology, the extent to which IT assets are protected and the level of assurance required. Risk management encompasses identifying, analyzing, evaluating, treating, monitoring and communicating the impact of risk on IT processes. After defining the risk appetite and identifying risk exposures, strategies for managing risk can be set and responsibilities clarified.

Risk appetite is the amount of risk that an enterprise is willing to take to achieve its strategic objectives. It is a deliberate decision that is made by the enterprise senior leadership. Risk tolerance is the acceptable deviation from the enterprise risk appetite. It is the amount of risk that the enterprise can withstand without jeopardizing its ability to achieve its strategic objectives (i.e., generally, the amount of money the enterprise is willing to risk). Risk appetite and risk tolerance are closely related. Risk appetite is a more strategic concept, while risk tolerance is a more tactical concept. Risk appetite is set at the enterprise level, while risk tolerance can be set at different levels, such as the departmental or project level.

For example, a technology enterprise may have a high-risk appetite because it is operating in a rapidly changing industry. The enterprise may be willing to take on more risk to develop new products and services and enter new markets. However, the enterprise may have a lower risk tolerance for financial losses, because it is important for the enterprise to maintain a healthy balance sheet. The enterprise risk appetite and risk tolerance inform its decision-making process. When the enterprise is considering launching a new product, it assesses the risk of the product launch and compares that to its overall risk appetite and risk tolerance. The new product will incur costs for research, development and marketing, and an opportunity cost because existing products receive less attention. If the risk of the product launch is too high, then the enterprise may decide not to launch the product.

Depending on the type of risk and its significance to the business, management and the board may choose one of the following responses:

- **Avoid**—Avoidance seeks to eliminate the risk exposure by not pursuing certain activities, processes, business relationships or ventures that would incur risk.
- **Mitigate**—Risk mitigation lessens the probability of a risk event or impact of risk on the enterprise by defining, implementing and monitoring appropriate controls.
- **Share or Transfer**—Sharing risk spreads the impact of the risk across multiple enterprises through partnership. Like sharing, transferring the risk places the impact on a third party through insurance coverage, contractual agreement or other means.
- **Accept**—With acceptance, management acknowledges the existence of the risk and agrees to move forward with its plan despite the possible impact. Acceptance sometimes occurs when the risk is deemed unavoidable. Within a tolerance level, management believes the business can absorb risk

 ©ISACA. All Rights Reserved.

independently. In this case, formal monitoring is implemented to ensure that the enterprise reacts appropriately if the risk increases.

Therefore, risk can be avoided, reduced, transferred or accepted. An enterprise can also reject risk by ignoring it, which can be dangerous and should be considered a red flag by the IS auditor.

It is important to realize that IT risk management needs to operate at multiple levels, including:

- **Operational level**—At the operational level, one is concerned with the risk that can compromise the effectiveness and efficiency of IT systems and supporting infrastructure, the ability to bypass system controls, the possibility of loss or unavailability of key resources (e.g., systems, data, communications, personnel, premises) and failure to comply with laws and regulations.
- **Project level**—Risk management needs to focus on the ability to understand and manage project complexity and, if this is not done effectively, to handle the consequent risk that the project objectives will not be met.
- **Strategic level**—The risk focus shifts to considerations such as how well the IT capability is aligned with the business strategy, how it compares with that of competitors and the threats (and the opportunities) posed by technological change.

Identifying, evaluating and managing IT risk at various levels are the responsibility of different individuals and groups within the enterprise. However, these individuals and groups should not operate separately, because risk at one level or in one area may also impact risk in another. A major system malfunction can impair the enterprise's ability to deliver customer service or deal with suppliers, and it can have strategic implications that require top management attention. Similarly, problems with a major project can have strategic implications. Also, as projects deliver new IT systems and infrastructure, the new operational risk environment must be considered.

2.5.1 Developing a Risk Management Program

Steps to developing a risk management program include:

- **Establish the purpose of the risk management program**—The first step is determining the enterprise's purpose for creating a program. The program's purpose should align with the enterprise's overall strategy. Risk management programs usually exist to advise management on risk related to achieving their objectives. By determining its intention before initiating risk management planning, the enterprise can define key performance indicators (KPIs), key risk indicators (KRIs) and metrics to evaluate the results to determine the program effectiveness. Typically, senior management sets the tone and goals for the risk management program with the board of directors. For more information, see section 2.10 IT Performance Monitoring and Reporting.
- **Assign responsibility for the risk management plan**—The second step is to designate an individual or team responsible for developing and implementing the ERM program. Although the team is primarily responsible for the risk management plan, a successful program requires integrating risk management within all levels of the enterprise. Operational staff and board members should assist the risk management committee in identifying risk and developing reasonable loss control and intervention strategies.

2.5.2 Risk Management Life Cycle

To ensure that an enterprise manages its risk consistently and appropriately, it should identify and establish a repeatable process to manage its IT risk. **Figure 2.10** illustrates the risk management life cycle.

Figure 2.10—The IT Risk Management Life Cycle



Source: ISACA, *CRISC Official Review Manual 7th Edition, Revised*, USA, 2023

Basic steps in the risk management process are described in the following sections.

©ISACA. All Rights Reserved.

Step 1: IT Risk Identification

The first step in the process is identifying and collecting relevant data to enable effective IT-related risk identification, analysis and reporting. This will help to identify information resources or assets that need protection because they are vulnerable to threats. In this context, a threat is any circumstance or event that can cause harm to an information resource (such as destruction, disclosure, modification of data and/or denial of service). The purpose of this classification may be either to prioritize further investigation and identify appropriate protection (simple classification based on asset value) or to enable a standard model of protection to be applied (classification in terms of criticality and sensitivity). The most critical data enable the business to continue operations. Examples of typical assets associated with information and IT include:

- Information and data
- Hardware
- Software
- Documents
- Personnel
- Clients and customers

Other, more traditional business assets for consideration are buildings, stock of goods (inventory), cash and intangible assets, such as goodwill or image/reputation.

Step 2: IT Risk Assessment

The second step in the process is to assess threats and vulnerabilities associated with the information resource and the likelihood of their occurrence. Common classes of threats are:

- Errors and omissions
- Malicious damage/attack
- Fraud
- Theft
- Equipment/software failure

IT risk occurs because of threats (or predisposing conditions) that can potentially exploit vulnerabilities associated with using information resources. Vulnerabilities are characteristics of information resources that can be exploited by a threat to cause harm. Examples of vulnerabilities are:

- Lack of user knowledge
- Lack of security functionality
- Inadequate user awareness/education (e.g., poor choice of passwords)
- Untested technology
- Transmission of unprotected communications

For a vulnerability to be realized, there must be either a human or environmental threat to exploit the vulnerability. Typical human threat actors (or threats caused by humans) are:

- Novices (script kiddies)
- Hacktivists
- Criminals
- Terrorists
- Nation-states
- Riots and civil unrest
- Political instability and transitions

Typical environmental threats include the following:

- Floods
- Lightning
- Tornados
- Hurricanes
- Earthquakes
- Fires

The result of a threat agent exploiting a vulnerability is called an impact. The impact can vary in magnitude, affected by severity, duration and other factors like velocity. In commercial enterprises, threats usually result in a direct financial loss in the short term or an indirect financial loss in the long term. Examples of such losses include:

- Direct loss of money (cash or credit)
- Breach of legislation (e.g., unauthorized disclosure)
- Loss of reputation/goodwill
- Endangerment of staff or customers
- Breach of confidence
- Loss of business opportunity
- Reduction in operational efficiency/performance
- Interruption of business activity

The impact can vary widely based on the nature of the enterprise. Loss of customer data from a small retailer can damage its reputation to the point of bankruptcy, while a larger enterprise can survive. Likewise, loss of customer data (i.e., patient records) at a hospital can result in the loss of life.

After the risk elements have been established, they are combined to form an overall view of risk. This exercise aims to establish a relative prioritization of risk for the enterprise. A common method of combining the elements is calculating, for each threat, probability of occurrence × magnitude of impact. This gives a measure of overall risk.

The risk is proportional to the estimated likelihood of the threat and the value of the loss/damage. In recent years, factors like velocity have been used to measure the speed at which the risk may pervasively impact the

 ©ISACA. All Rights Reserved.

enterprise. When other factors are considered, these will also modify the score. For example, the calculation can be the probability of occurrence × magnitude of impact × velocity of impact.

Step 3: Risk Response and Mitigation

After identifying the risk, existing controls can be evaluated (or new controls designed) to reduce the vulnerabilities to an acceptable level. These controls are referred to as countermeasures or safeguards and include actions, devices, procedures or techniques (i.e., people, processes or products) implemented to offset either the impact or probability of the risk occurring. The strength of a control can be measured in terms of its inherent or design strength and the likelihood of its effectiveness.

The strongest controls are preventive, automated and formal, because these stop the occurrence without human interaction, and the effectiveness has been tested. The weakest controls are informal and manual because these are deployed inconsistently. When developing controls, if full automation is not achievable, the enterprise may opt for IT dependent, or hybrid, controls that include a mix of manual and automated processes. The strength of the control can be judged along a matrix (**figure 2.11**).

Residual risk is the remaining level of risk after controls have been applied. An acceptable level of risk can be established by management (risk appetite). Risk above this level should be reduced by implementing more stringent controls or secondary controls. Risk below this level should be evaluated to determine whether an excessive level of control is being applied and whether cost savings can be made by removing these excessive controls. Final acceptance of residual risk considers:

- Organizational policy
- Risk appetite
- Risk identification and measurement
- Uncertainty incorporated in the risk assessment approach
- Cost and effectiveness of implementation
- Cost of control versus benefit

Figure 2.11—Control Matrix



An IS auditor is often focused on high-risk issues associated with the confidentiality, integrity or availability of sensitive and critical information and the underlying information systems and processes that generate, store and manipulate such information. In reviewing these types of IT-related business risk, an IS auditor often assesses the effectiveness of the risk management process that an enterprise uses.

In analyzing the business risk arising from the use of IT, it is important for an IS auditor to have a clear understanding of the following aspects:

- Industry and/or internationally accepted risk management processes
- The purpose and nature of business, the environment in which the business operates and related business risk
- Dependence on technology in the achievement of business goals and objectives
- The business risk of using IT and how it impacts the achievement of the business goals and objectives
- A good overview of the business processes and the impact of IT and related risk on the business process objectives

The risk assessment process is an iterative life cycle that begins with identifying business objectives; information assets and the underlying systems or information resources that generate, store, use or manipulate the assets (e.g., hardware, software, databases, networks, facilities, people) critical to achieving these objectives. Because IT risk is dynamic, management should recognize the need for and establish an adaptive IT risk management process that supports the business risk

©ISACA. All Rights Reserved.

management process. As a result, the most effort can be directed toward the most sensitive or critical assets to the enterprise. Next, a risk assessment is performed to identify vulnerabilities and threats and determine the probability of occurrence and the resulting impact and additional safeguards that would mitigate this impact to a level acceptable to management.

During the risk mitigation phase, controls are identified for treating the identified risk. These controls should prevent or reduce the likelihood of a risk event occurring, detect the occurrence of a risk event, minimize the impact or transfer the risk to another enterprise.

The assessment of countermeasures should be performed through a cost-benefit analysis where controls are selected to reduce risk to a level acceptable to management. This process may be based on the following:

- The cost of the control compared to the benefit of minimizing the risk
- Management's risk appetite (i.e., the level of residual risk that management is prepared to accept)
- Preferred risk-reduction methods (e.g., terminate the risk, minimize probability of occurrence, minimize impact, transfer the risk via insurance)

Step 4: Risk and Control Monitoring and Reporting

The final phase relates to monitoring performance levels of the risk being managed and identifying any significant changes in the environment that would trigger a risk reassessment, warranting changes to its control environment. The last phase encompasses three processes —risk assessment, risk mitigation and risk reevaluation —in determining whether risk is being mitigated to a level acceptable to management. It should be noted that, to be effective, risk assessment should be an ongoing process in an enterprise that endeavors to continually identify and evaluate risk as it arises and evolves.

In summary, the risk management process should achieve a cost-effective balance between applying security controls as countermeasures and adapting to significant threats. Some threats are related to security issues that can be extremely sensitive for some industries.

2.5.3 Risk Analysis Methods

The most common risk analysis methods include qualitative, semiquantitative and quantitative. Each has advantages and limitations.

Qualitative Analysis Methods

Qualitative risk analysis methods use words or descriptive rankings to describe the impacts or likelihood. These are normally based on checklists, interviews and subjective risk ratings, such as high, medium or low. These are the simplest and most frequently used methods, mostly where the risk level is low.

Although often less complicated than the other methods, qualitative analysis lacks the rigor customary for accounting and management. Also, gathering, deconstructing and analyzing text-based information to form an analysis can be time-consuming beyond the data's usefulness.

Semiquantitative Analysis Methods

In semiquantitative analysis, the descriptive rankings are associated with a numeric scale. Such methods are frequently used when using a quantitative method or reducing subjectivity in qualitative methods is impossible. For example, the qualitative measure of high may be given a quantitative weight of 5, medium may be given 3 and low may be given 1. The total weight for the evaluated subject area may be the aggregate of the weights derived for the various factors being considered. This method is often used in surveys with questions like: On a scale of 1 to 5, with 1 being the lowest and 5 being the highest, how would you rank the risk of loss of data due to a phishing attack?

Quantitative Analysis Methods

Quantitative analysis methods use numeric (e.g., monetary) values to describe the likelihood and impacts of risk, using data from several sources such as historical records, past experiences, industry practices and records, statistical theories, testing, and experiments. These methods provide measurable results.

Many quantitative risk analysis methods are currently used by military, nuclear, chemical and financial entities and other areas. A quantitative risk analysis is generally performed during a BIA. The main problem within this process is the valuation of information assets. Depending on the relevance of the information to the individuals, individuals may assign different values to the same asset. In the case of technology assets, it is not only the cost of the asset that is considered but also the cost of replacement and the value of information processed by that asset.

In some enterprises that are required to comply with financial reporting regulations (e.g., SOX), applications

are brought into scope based on the volume or the value of transactions processed by that system. If an enterprise has two point of sale (POS) systems, one that processes 98 percent of the enterprise revenue and the other only two percent, it could be that only the system processing 98 percent would be considered in scope for the regulation and subjected to the formality of control documentation and testing required.

2.6 Data Privacy Program and Principles

A data privacy governance program ensures that all personal information within the enterprise are identified and managed per legal requirements for personal information use and protection, governing policies, procedures and guidelines and data subject rights. Although the definition varies among regulations, personal data is generally any piece of information that relates to an identifiable person.

Privacy management practice areas include establishing privacy roles and responsibilities related to data, fostering privacy training and awareness communications and activities, monitoring vendor and third-party management practices, developing a privacy audit process and implementing a privacy incident management capability.

Enterprises must design, implement and operate appropriate controls to protect and manage an individual's privacy throughout the full life cycle of personal and associated sensitive information. To accomplish this, enterprises must determine the internal and external requirements for the enterprise's privacy programs and practices. Key requirements vary by specific regulation or statute concerning detailed implementation. These can be divided into internal and external requirements, as described in **figure 2.12**.

Figure 2.12—Privacy Program Requirements

Type of Requirement	Consideration
Internal Requirements	• Assigning privacy roles and responsibilities • Defining and inventorying personal information • Implementing enterprise employee privacy policies, procedures and training • Establishing vendor management programs • Managing privacy incidents • Performing privacy audits and assessments • Harmonizing with organizational culture (or changing it with management support) • Accounting for the capabilities and limitations of information systems
External Requirements	• Identifying and documenting applicable laws, regulations, standards and contractual obligations • Choosing privacy principles and frameworks • Posting a privacy notice that reflects actual enterprise practices and meets legal requirements • Maintaining third-party oversight • Addressing data subject rights • Addressing requirements from customers, investors and industry sources • Accommodating existing contractual relationships

Source: ISACA, *CDPSE Official Review Manual, 2nd Edition*, USA, 2023

Privacy principles within an established privacy framework enable an enterprise to apply privacy controls comprehensively and consistently to all business activities. A few examples of popular privacy principles include:

- ISO/TS 17975:2022 Health Informatics - Principles and Data Requirements for Consent in the Collection, Use or Disclosure of Personal Health Information
- OECD Privacy Principles
- AICPA Generally Accepted Privacy Principles
- ISACA Privacy Principles

Data privacy is an area that is becoming more heavily regulated, with various laws passed in the European Union and the United States, often based on the principles above. For example, EU regulators have passed laws like the GDPR and Trans-Atlantic Data Privacy Framework (DPF) to protect EU individuals' personal data when the personal data is stored in

©ISACA. All Rights Reserved.

the United States. These data privacy laws impact all enterprises and countries that trade within the EU.

2.6.1 Privacy Documentation

An effective privacy governance program is not possible without documentation. Maintaining various types of documentation is critical to clearly demonstrate enterprise data management practices and objectives, to meet obligations under applicable privacy laws, to build trust among key stakeholders and to demonstrate a standard of due care in the management of the privacy program.

- Internal policies and procedures, external privacy notices and other related documents are aligned with the applicable privacy laws, regulations, contractual obligations and other legal requirements.
- Any required or enterprise-adopted industry standards are reflected in the enterprise's privacy documentation and practices.
- Both inward-facing policies, procedures and related documentation and outward-facing privacy notices, websites, social media pages and related documentation are regularly reviewed and evaluated to ensure alignment with privacy requirements.
- The breadth and depth of the privacy program meets or exceeds any requirements imposed by applicable laws, regulations or standards.

Types of Documentation

A wide variety of documentation is necessary to support and demonstrate a comprehensive privacy management program and meet a wide variety of privacy legal requirements. The common types of documentation that privacy practitioners must understand—and typically create, maintain, evaluate and communicate to others—are discussed in this section.

This is not an exhaustive list of all types of documentation necessary for supporting all forms of privacy management programs. Also, the types of documentation are not listed in any implied order of importance or use. Each enterprise should use this list as a starting point for determining the documentation necessary to meet its own legal requirements and privacy risk.

Privacy Notice

A privacy notice is an outward-facing statement that is written for data subjects and data protection authorities. It describes how the enterprise collects, uses, retains, safeguards and securely discloses personal information. Privacy policies are discussed later in this manual; however, the same provisions published outwardly as a privacy notice are often referred to as a privacy policy or a privacy statement when considered from within the enterprise.

Because privacy relies on informed consent, an enterprise's privacy notice establishes its legal accountability. Regulators, auditors and lawyers judge the enterprise privacy management program and managers against the enterprise practices as they relate what the enterprise attested it would do in terms of use and protection of data. The data controller and the data processor are responsible for complying with the parameters established by a privacy notice.

In addition to accountability, privacy notices also serve other purposes, including:

- Providing data subjects, using easily understood language, with explanations of:
  - What personal data are collected and why
  - Why the personal data are collected
  - How the personal data are used, processed and handled
  - With whom the personal data are shared without the data subject's knowledge
  - How long the personal data are retained
  - How the data collection may impact the data subjects
  - Where and how the personal data are destroyed (where applicable)
- Informing data subjects about procedures to exercise their rights over their associated personal information
- Supporting data subjects' consent or other legal authorization permitting the data controller to use the personal information as intended or planned
- Building and maintaining data subjects' trust

Privacy notices vary and may be presented to data subjects in many ways, such as:

- A page on the enterprise website that is dedicated to describing privacy-related activities.
- Forms that ask for personal information and indicate how the personal information will be used and safeguarded.
- Brochures, such as those sent out each year in the United States by payment card enterprises, to describe privacy protections and rights.
- Documents that are provided at enterprise facilities, such as a healthcare clinic or hospital, that explain how personal information is collected, used and shared, and set forth individuals' rights to access their associated personal information.
- Contracts, such as those for loans or other financial services, that describe how the enterprise

collects, uses, stores, shares and safeguards personal information.
- Signs on buildings or interior walls, such as those warning that closed-circuit television (CCTV) cameras are in use, can serve as privacy notices.

Terms-of-use statements commonly include descriptions of the rules governing how the enterprise will use personal information, and the associated enterprises point to those statements as their privacy notices. Although this is a common practice, it is best to maintain separate privacy notices and terms-of-use statements to avoid the perception of duplicity or obfuscation. The timing of privacy notices relative to when data are collected should also be considered, with sufficient time between notice and collection for data subjects to evaluate whether acceptance is in their best interest. Where too little time is afforded to data subjects prior to collection, even comprehensive notice may be deemed insufficient, potentially creating unacceptable risk to the enterprise.

Consent Form

The agreement by a data subject with the terms of a privacy notice is documented by a consent form. The intended uses of a consent form are to provide information for the potential data subject's current and future reference and to document the interaction between the subject and the entity obtaining the consent.

Consent forms should include provisions for:
- Obtaining consent for existing personal data
- Renewing consent if noncompliant

A consent form could take the form of an opt-in/opt-out button, a tick box on a web page at the bottom of the privacy notice or statement or a signature box at the bottom of paper forms containing similar privacy notices. The more explicitly it is that consent must be provided to a privacy notice, the greater the protection the enterprise gains against subsequent claims of insufficient understanding.

A signed consent form on its own may not establish an adequate consent process. The informed consent process is an ongoing exchange of information between the enterprise and the data subject. It could include the use of question-and-answer sessions, emails, community meetings and videotape presentations.[23]

Obtaining documented consent is a separate activity from data controllers informing data subjects about how to make inquiries or notifying the enterprise of various types of decisions (e.g., withdrawal of consent, request to delete personal data or request the deletion of data). In most cases, data subjects have the right to withdraw their consent at any time, and mechanisms used to capture consent should take into account the potential for a data subject to do so. As with the level of clarity associated with a privacy notice, the ease with which consent may be withdrawn is one factor that helps data collecting enterprises maintain an acceptable level of risk.

Personal Information Inventory

A personal information inventory is a documented repository of the personal data assets collected, derived, processed, stored or otherwise handled by an enterprise. Unlike other documentation that arises from legal or regulatory requirements, personal information inventories are internally focused documents intended to support a variety of privacy and data protection measures through increased awareness of what might be at risk. Inclusion of data flow mappings with data inventories provides valuable insight to an enterprise and is recommended whenever possible.

Because the inventory is not a regulatory requirement unto itself and there is no universal definition of personal information, each enterprise must first determine the specific information items to document in its enterprise's personal information inventory. The specific information items should reflect the established definition of personal information related to the enterprise's services, products, locations, customers, patients, employees and vendors and other determining factors. Privacy practitioners should take care to ensure that procedures exist to keep inventories and any existing dataflow diagrams updated and current.

Often used with IT, security or governance manuals or automated tools, personal information inventories include details about the enterprise's network, applications, systems, storage areas and physical forms of information.

Inventories support the efforts of privacy management program initiatives to record detailed information about the enterprise's personal information (e.g., human resources data, customer data or marketing data). Because every enterprise is unique, the personal information inventory items will vary from one enterprise to the next. Personal information inventories can be documented within hard copy media, spreadsheets, word processing documents, databases or other types of tools used for asset inventories.

[23] U.S. Department of Health and Human Services, "Informed Consent FAQs," *www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/informed-consent/index.html*

©ISACA. All Rights Reserved.

Other Types of Documentation

There are many other types of documentation that support enterprises in managing their privacy programs and meeting a wide range of specific legal requirements. The format and content of such documentation often varies greatly between, and often within, enterprises. Some important but not rigidly defined types of documentation include:

- **Activity logs**—Activity logs documenting privacy management activities can be manually created, generated by applications and systems, or automatically created through a wide range of vendor- or in-house created tools. Logs can detail information, such as the names of individuals who have attended privacy training, the number of unsuccessful identity-verification attempts, the locations of people using employee-issued vehicles and the identities of those who have access to personal information records.
- **Data protection legal requirements**—Enterprises should identify and document all privacy legal requirements applicable to their operations. This documentation should be provided to key stakeholders throughout the enterprise—notably to privacy engineers, to help them ensure that systems, applications, networks and other services and products they design appropriately support the legal requirements.
- **Privacy risk assessment reports**—A privacy risk assessment report reflects the findings from a systematic evaluation of how personal information is collected, used, shared, maintained and destroyed by an enterprise and its third-party service providers. A privacy risk assessment report is important documentation that provides an overview of the enterprise's privacy risk status. It is useful not only to meet legal requirements, including those from privacy regulations, such as GDPR and CCPA, but also to manage risk that may accompany new and emerging technologies and to address privacy risk not covered by legal requirements.
- **Privacy impact assessment (PIA) reports**—A PIA is a process used to determine if personal information is appropriately safeguarded, used, shared, made available to the individuals associated with it and destroyed. A PIA report details the findings of a PIA and includes associated documentation detailing how the discovered privacy risk will be appropriately mitigated. For more information, see section 2.11.1 Data Inventory and Classification.
- **Privacy governance reports**—Privacy governance reports communicate to key stakeholders the current levels of privacy compliance throughout the enterprise; improvements made since the last privacy governance report was published; risk, incidents and problems encountered since the last privacy governance report was published; and the status and outcomes of privacy programs and practice changes. Such a report is necessary for multiple reasons, the primary reasons being:
  - To demonstrate the value of the privacy department and governance program
  - To make key stakeholders aware of privacy problems and risk throughout the enterprise
  - To communicate successes and improvements within the privacy program
  - To engage key stakeholders with the privacy practitioners and learn the areas of concern to the key stakeholders
- **Training activities**—It is important to document when training occurs, the topic of the training, those who attended the training and the date and time of the training. In addition, it is important to document how the training was delivered and the results of any quizzes or tests provided to the training attendees. Such documentation provides important evidence to prove a standard of due care for training activities to any auditor or regulator. Documentation also provides a historical record of the training activities that have occurred, supports better understanding of the training's effectiveness and can provide insights for how to improve the training program.
- **Data incident register**—Stores records of all personal data incidents in an inventory or log. It must contain the facts about the incident, effects of the breach, remedial measures and preventive measures to avoid the breach in the future.
- **Individual rights register**—Record of all the requests from individuals about their records and how/when it was received and sourced. These can include individuals requesting a copy of their records, asking for rectification, etc.

2.6.2 Audit Process

Data privacy audits, assessments, testing and compliance reviews are used to ensure that the enterprise's privacy policies, procedures, practices, personal information rules and standards comply with internal and external laws, regulations, directives and other legal requirements and privacy standards. Annual data protection audits are an essential element to aid in compliance. Privacy audits, assessments or similar activities can also be used to identify failures of enterprise architecture and information architecture to support privacy based on

design principles and considerations, creating business risk as a result.

Performing data privacy audits demonstrates a standard of due care and supports ISACA Privacy Principle 9: Monitoring, Measuring and Reporting,[24] which recommends the enterprise establish appropriate and consistent monitoring, measuring and reporting of the effectiveness of the privacy management program and tools. To support this, the enterprise should:

- Establish a framework for auditing, measuring/evaluating and monitoring the following:
  - Effectiveness of the data privacy management program
  - Level of compliance with applicable policies, standards and legal requirements
  - Use and implementation of privacy tools
  - Advancements in privacy-enhancing technologies
  - Changes in privacy regulations and laws
  - Types and numbers of privacy breaches that occur
  - Privacy risk areas within the data controller's digital ecosystem
  - Third parties that have access to personal information, sensitive information and the associated risk levels
- Report compliance with privacy policies, applicable standards and laws to key stakeholders
- Integrate internationally accepted privacy practices into business practices and then check during privacy audits to ensure that those practices have been implemented appropriately and are followed consistently
- Establish procedures that cover the use of personal data in investigating, monitoring, continuous auditing, analytics, etc., completed by internal or external auditors
- Anonymize data if the local/national law is not allowed to monitor pure personal data for fraud/crime prevention, etc.; perform audits to ensure the anonymization processes are effective and consistently applied throughout the enterprise

To support the enterprise, IS auditors play a vital role in the evaluation of the data privacy program. This involves evaluating the effectiveness of data privacy policies, including:

- Data privacy requirements are included in third-party contracts.
- Data retention and destruction policies are implemented.
- Cross border regulations for data privacy are addressed in data processes.
- Employees received training about data privacy regulations.
- Data inventory is created and maintained.
- Data subject requests are handled appropriately.

2.7 Data Governance and Classification

The enterprise must compile a detailed inventory of information assets to effectively control data, information assets and resources. Creating this list is the first step in classifying assets and determining the level of protection needed for each asset. After the initial listing and classification are created, the inventory must be reviewed and updated regularly. The classification must be reviewed for appropriateness.

Information assets have varying degrees of sensitivity and criticality in meeting business objectives. By assigning classifications, or levels of sensitivity and criticality, to information resources and establishing specific security rules for each classification, it is possible to define the level of access controls that should be applied to each information asset. Classification of information assets helps to build and maintain a consistent perspective of the security requirements for data resources throughout the enterprise. As a secondary benefit, this enables a cost-benefit analysis to implement the proper amount of control to reduce the risk of overspending on unnecessary protection by linking data security to business objectives.

The information owner is responsible for the information and should decide on the appropriate classification based on the enterprise's data classification and handling policy. Classifications should be simple, such as designations by differing degrees for sensitivity and criticality. End-user managers and security administrators can then use these classifications in their risk assessment process to determine who can access what and the most appropriate level of such access. Most enterprises use a classification scheme with three to five levels of sensitivity. The number of classification categories should consider the size and nature of the enterprise and the fact that complex schemes may become too impractical to use.

Data classification is a major part of managing data as an asset. Data classification as a control measure should define the following:

- Importance of the information asset
- Information asset owner
- Process for granting access

[24] ISACA, *ISACA Privacy Principles and Program Management Guide*, USA, 2016

©ISACA. All Rights Reserved.

- The person responsible for approving the access rights and access levels
- Extent and depth of security controls

Data classification must consider legal, regulatory, contractual and internal requirements for maintaining privacy, confidentiality, integrity and availability of information. Data classification is also useful to identify who should have access to the production data used to run the business versus those permitted to access test data and programs under development. For example, application or system development programmers should not have access to production data or programs.

Adopting a classification scheme and assigning the information to one sensitivity level enables uniform data treatment by applying level-specific policies and procedures rather than addressing each type of information. It is difficult to follow information security policies if documents and media are not assigned to a sensitivity level and users are not instructed on the procedures for dealing with each piece of information. Suppose documents or media are not labeled according to a classification scheme. In that case, this indicates a potential misuse of information. Users might reveal confidential information because they did not know the requirements prohibited disclosure. Social engineering capitalizes on this kind of misunderstanding at the end-user level. Examples of classification of information include:

- **Public**—Public data are open and freely accessible to the public. Public data can be used, reused and redistributed by anyone. Examples of public data include marketing material and press releases.
- **Internal**—Internal data are strictly limited to employees expressly granted access to the information. Internal data examples include business plans, organization charts and reports.
- **Confidential**—Confidential data need to be kept private. Confidential files include unpublished financial information, customer lists, payment card information or contracts that can have negative ramifications if exposed. Confidential data may also fall under data privacy and security laws like HIPAA and PCI DSS.
- **Restricted**—Restricted data are highly sensitive and can lead to criminal charges or legal fines if exposed. Examples of restricted data might include proprietary information or research and data protected by state and federal regulations.

Inventorying and classifying sensitive data provides guidance on handling the enterprise's critical data assets. IT governance teams must prioritize data protection efforts for the organization's benefit to further business objectives through data security and comply with regulations.

2.7.1 Data Inventory and Classification

A fully specified and populated data inventory and classification is the most important resource for conducting a privacy impact assessment (PIA), because the master inventory covers all sensitive data. The data inventory includes the types of personal information collected and the information necessary to ensure privacy compliance.[25] The scope of the data inventory and classification must be enterprisewide and up to date to ensure that a PIA confirms adequate controls and identifies vulnerabilities.

The content and scope of the data inventory for sensitive information is largely consistent with a metadata repository, which is implemented and managed by data governance. As part of enterprise metadata management, the privacy data inventory should be collaboratively managed between privacy and data governance, and the inventory should consider the unintentional capture, use and storage of personal data.

2.7.2 Legal Purpose, Consent and Legitimate Interest

Legal purpose, consent and legitimate interest relate to all the ways personal information is processed, including how it is obtained, used, shared, processed, made available to the associated individuals (the data subjects), retained and accessed for other types of activities.

Although these terms and concepts have been used and understood for decades in a subjective sense, their explicit use within the EU GDPR has increased interest and heightened the need to understand their associated meanings and requirements. GDPR includes several processing bases beyond the three listed in this section; however, these are the most commonly used and are also commonly included under other privacy and protection standards around the world, including self-regulatory models. Understanding the terms and concepts is particularly necessary for privacy engineers, because a large portion of the systems, applications, networks, services and procedures engineered must conform with legal requirements defined by these terms.

[25] *Ibid.*

 ©ISACA. All Rights Reserved.

Legal Purpose

It is a long-held privacy principle[26] that when an enterprise collects and uses personal information, the data controller should:

- Describe and specify in the privacy notice, or other means of communication, the purpose for which personal information and any associated sensitive information is collected, ensuring that the purpose complies with applicable law and relies on a permissible legal basis.
- Align subsequent use of the personal information and sensitive information with the purpose provided and the consents obtained and comply with associated legal requirements for use limitation.
- When necessary, communicate with applicable data protection legal authorities about legitimate purpose and use limitations.

The purposes for which personal information are collected, used and shared must be consistent with associated legal requirements, such as the GDPR.[27] While EU member states must meet minimum requirements, each may establish additional, more specific requirements. Therefore, it is important for each enterprise to know the requirements of all the countries from which personal information is collected and processed. Additionally, the specific requirements of a legal-purpose basis may not be consistent between different regulations, particularly as it relates to the methods and sufficiency of consent.

Consent

When collecting personal information from individuals, enterprises should:[28]

- Obtain appropriate consent, implicit or explicit, according to what any corresponding regulation mandates with respect to the collection, use and disclosure of personal information.
- Ensure that appropriate and necessary consents have been obtained:
  - Prior to commencing collection activities
  - Prior to using the personal information for purposes beyond those for which it was originally collected
  - Prior to the transfer of personal information to third parties or other jurisdictions

If obtaining consents through an electronic transmission method, it is a good security practice to include a cover sheet notifying recipients that enclosed documents may contain privileged information that must be safeguarded against unauthorized disclosure.

Privacy engineers are needed to ensure that consent options are provided to individuals appropriately and consistently. The privacy engineers should also ensure that associated consents and withdrawals of consent are appropriately recorded. For denials of consent, because the individual may not provide any documentation for a denial, the privacy engineer needs to establish a method to document, either digitally or manually, that the denial occurred.

Going forward, services and products must be engineered to support:

- Decisions regarding the use or nonuse of personal information
- Compliance with associated legal requirements for use limitation

Multiple regulations throughout the world have specific requirements for how and when consents should be collected and used (e.g., GDPR and HIPAA).

Legitimate Interest

The legitimate interests of an enterprise that collects personal information from consumers or employees, derives personal information from IoT device data or AI activities, or is given personal information from another enterprise to perform an activity on its behalf may establish the legal basis for performing various processing activities without the associated individuals' consent. Such a situation may occur if the interests or legal rights of the associated individuals do not override the enterprise's legal rights for processing, when considering the reasonable expectations of individuals based on their relationship with the enterprise. In short, legitimate interest is the basis for the lawful processing of data.

In general, there is a relevant and appropriate relationship between the individual (data subject) and the enterprise (data controller) when the individual is a client, customer

---

[26] *Ibid.*

[27] The European Parliament and the Council of the European Union, *General Data Protection Regulation*, 27 April 2016, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation [or GDPR]) (OJ L 119, 4.5.2016, p. 1)

[28] *Op cit* ISACA 2016

©ISACA. All Rights Reserved.

or patient, or is employed by or in some type of relationship with the enterprise. For example:

- When an enterprise needs to use employee personal information to create stakeholder annual statements or to file country tax return reports
- When in the interest of national security, such as obtaining summary patient infection statistical data when determining the total number of individuals infected with COVID-19 in each geographic area of a country to support controlling the spread
- When conducting forensic analysis to determine the source of a network hacking incident

Determining if legitimate interest applies depends upon the assessment of the situation, including whether the involved individuals could have reasonably expected, when their personal information was collected, that analysis of their personal data could reasonably take place. The interests and legal rights of the individuals could supersede the interest of the enterprise if the individuals did not reasonably expect further processing. It is important for privacy engineers to be aware of such legitimate interest rights when they are establishing services and products involving the use of personal information. Because of the need for assessment to determine legal interest, privacy engineers should involve their legal counsel, information security officer and privacy officer in making such decisions.

Data privacy engineers can conduct a legitimate interest assessment by identifying the purpose, necessity and balance elements and determining if a decision can be made on whether legitimate interest is appropriate and lawful or if more scrutiny is required.

GDPR is commonly referenced as the predominant regulation that requires legitimate interest assessment. However, other local, state and national laws and regulations may also allow consideration of legitimate interest prior to using personal information for purposes that were not explicit when the personal information was collected.

2.7.3 Data Subject Rights

The issue of data subject rights (i.e., the rights of the individuals associated with personal information) is a topic of ongoing debate. Laws and regulations have established a wide range of diverse data subject rights over the past several decades. Privacy engineers and other privacy practitioners need to identify, document and understand the rights that apply to the data subjects whose personal information they collect, derive, store, transmit, share, access or otherwise process.

The NIST Privacy Framework,[29] which is a tool that enterprises can use to build a privacy management program, includes two specific functions supporting data subject rights for access, control and communications about their personal information:

- **Control-P**—Develop and implement appropriate activities to enable enterprises or individuals to process data with sufficient granularity to manage privacy risk. The Control-P function considers data processing management from the standpoints of enterprises and individuals.
- **Communicate-P**—Develop and implement appropriate activities to enable enterprises and individuals to have a reliable understanding and engage in a dialog about data processing methods and associated privacy risk. The Communicate-P function recognizes that enterprises and individuals may need to know how data are processed to be able to manage privacy risk effectively.

Privacy engineers can use the controls described within the categories and subcategories of the Control-P and Communicate-P functions to guide the engineering of services and products that allow individuals to access their own associated personal information. These include the following categories:

- **Control-P categories:**
  - Data processing policies, processes and procedures (CT.PO-P): Policies, processes and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the enterprise's risk strategy to protect individuals' privacy. Legal and regulatory requirements must be considered in addition to the organization's policies.
  - Data processing management (CT.DM-P): Data are managed consistent with the enterprise risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).
  - Disassociated processing (CT.DP-P): Data processing solutions increase disassociability consistent with the enterprise's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).

[29] National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, Version 1.0, 16 January 2020, *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf*.

- **Communicate-P categories:**
  - Communication policies, processes and procedures (CM.PO-P): Policies, processes and procedures are maintained and used to increase transparency of the enterprise's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem; management commitment) and associated privacy risk.
  - Data processing awareness (CM.AW-P): Individuals and enterprises have reliable knowledge about data processing practices and associated privacy risk, and effective mechanisms are used and maintained to increase predictability consistent with the enterprise's risk strategy to protect individuals' privacy.

Subcategories, and their associated details, for each category previously listed are found in the NIST Privacy Framework.[30] The subcategories give privacy engineers specific types of guidance, capabilities and controls to consider when supporting data subject rights.

Transborder Data Flow

Transborder data flow refers to data transmission between two countries. Information, such as email, invoices, payment advice, etc., can be transmitted via suboceanic cables, telephone, television links and satellites. The selection of transmission alternatives should consider cost and possible transmission delays. The country of origin or the country of destination could have several laws applicable to transborder data flow that should be addressed. Legal compliance and protection, and data security and integrity are a concern with transborder transmissions. Privacy also is an issue because laws regarding protection and access to personal information may be different or conflicting between the source and destination countries.

Some countries also have laws concerning the encryption of data/information sent via transborder communications, thereby affecting the security and protection of data that may be exchanged between countries.

This is a particularly important issue in Internet communications, because the itinerary of the information is determined by the routers, is not fixed and, therefore, may cross a country border even while connecting two computers located in the same country.

[30] *Ibid.*

Page intentionally left blank

Part B: IT Management

IT management consists of overseeing the activities related to IT operations and resources. IT management plans, builds, implements, operates and monitors activities in alignment with the direction set by the governance body to achieve enterprise objectives. IT management ensures that IT continues to support enterprise objectives.

2.8 IT Resource Management

Each enterprise is challenged to use limited resources, including people and money, to achieve its goals and objectives. When an enterprise invests its resources in a given effort, it incurs opportunity costs because it cannot pursue other efforts that can bring value to the enterprise. An IS auditor should understand the enterprise's investment and allocation practices to determine whether the enterprise is positioned to achieve the greatest value from the investment of its resources.

Traditionally, when IT professionals and senior managers discussed an IT project ROI, they considered financial benefits, including impacts on the enterprise's budget and finances (e.g., cost reductions or revenue increases). Today, business leaders also consider the nonfinancial benefits of IT investments, which include impacts on operations, achieving strategic objectives and other results, like improved customer satisfaction, better information and shorter cycle times. Where feasible, nonfinancial benefits should be made visible and tangible by using algorithms that transform them into monetary units to make their impact more understandable and improve analysis.

2.8.1 Value of IT

IT projects are selected based on the perceived value of the investment. The value of the IT project is determined based on the relationship between what the enterprise will pay (costs) and what it will receive (benefits). The larger the benefit compared to the cost, the greater the value of the IT project.

IT portfolio management is distinct from IT financial management in that it has an explicitly directive, strategic goal in determining how much the enterprise will invest or continue to invest versus what the enterprise will divest.

2.8.2 Implementing IT Portfolio Management

IT portfolio management determines if the enterprise is pursuing the best IT-related projects to achieve enterprise goals. Whether financial, strategic or tactical, portfolio criteria can be classified and evaluated. Although the criteria should be comprehensive, they also need to be able to change as the enterprise's strategy changes.

The first practical and necessary step for implementation is to standardize the enterprise's terminology to reduce misunderstandings. Initial tasks include the following:

- Ensure management commitment and agreed-on targets.
- Plan the portfolio management model in line with the enterprise's management process.
- Specify portfolio inclusion criteria.
- Describe the roles, tasks and decisions of those involved.
- Organize the required tools, support and instructions.

Implementation methods include the following:

- Analysis and assessment of risk profile
- Diversification of projects, infrastructure and technologies
- Alignment and continuous realignment with business objectives
- Continuous improvement

Although many projects are discretionary, others are mandatory for regulatory compliance or to mitigate technical debt. In either situation, a documented business case should be required. After completed, programs should not be deleted from the portfolio. Instead, their status should be changed, and results evaluated against the original plans.

2.8.3 IT Management Practices

In most enterprises, the IT department has a service or support function. The traditional role of a service department is to help production departments conduct their operations more effectively and efficiently. In a modern enterprise, IT is a critical function that is integrated throughout the operations of an enterprise. IT management practices reflect implementing policies and procedures developed for various IT-related activities. IS auditors must understand and appreciate the extent to which a well-managed IT department is crucial to achieving the enterprise objectives.

IT management activities include reviewing policies and procedures that impact the IT function. The review should include the effectiveness of human resource

©ISACA. All Rights Reserved.

(HR) management, enterprise change management, financial management practices and information security management.

2.8.4 Human Resource Management

HR management relates to enterprise policies and procedures for recruiting, hiring, training and promoting staff. HR is also involved in measuring staff performance, disciplining, planning for succession and retaining and terminating staff. The effectiveness of these activities, as they relate to the IT function, impacts the quality of staff and the performance of IT duties.

Note

The IS auditor should be aware of HR management issues. However, this information is not tested in the CISA exam due to its subjectivity and organization-specific subject matter.

Recruiting and Hiring

An enterprise's hiring practices are important to ensure that the most qualified candidates are chosen, and that the enterprise complies with legal recruitment requirements. Common hiring controls include the following:

- Background checks (e.g., criminal, educational, financial, professional)
- Confidentiality agreements or nondisclosure agreements. Specific provisions may be made in these agreements to abide by the security policies of the previous employer and not to exploit the knowledge of internal controls in that enterprise.
- Employee bonding to protect against losses due to theft, mistakes and neglect. Employee bonding is not accepted worldwide; in some countries, the practice is illegal.
- Conflict of interest disclosures
- Codes of professional conduct/ethics
- Noncompete agreements

Residual risk includes the following possibilities:

- Employees may not be suitable for the position they are hired to fill.
- Reference checks may not be carried out or may be fraudulent.
- Temporary staff and third-party contractors may introduce uncontrolled risk.
- Lack of awareness of confidentiality requirements may lead to the compromise of the overall security environment.

Employee Handbook

Employee handbooks, distributed to all employees at the time of hire, should explain items such as:

- Security policies and procedures
- Acceptable and unacceptable conduct
- Organizational values and ethics code
- Company expectations
- Employee benefits
- Vacation (holiday) policies
- Overtime rules
- Outside employment
- Performance evaluations
- Emergency procedures
- Disciplinary actions for:
  - Excessive absence
  - Breach of confidentiality and/or security
  - Noncompliance with policies

In general, there should be a published code of conduct for the enterprise that specifies the responsibilities of all employees. An employee handbook is not a control, only a source of information.

Training

Training involves new hiring orientation training and ongoing training. New-hire training establishes a baseline for all employees to ensure that all individuals have received the information required for employment. New-hire training generally includes IT training on topics like cybersecurity, confidentiality, data management, compliance and conflict of interest. Specialized training for IT professionals on information security, access controls and end-user training for applications may be included. Ongoing training covers refresher training for important topics and updated training for job functions and tools.

Training should be provided regularly to all employees and should focus on areas where knowledge or employee expertise may be lacking. Training is particularly important for IT professionals, given the rapid rate of change in technology and products. It assures more effective and efficient use of IT resources and strengthens employee morale. Training must be provided when new hardware and/or software is implemented. Training should also include relevant management, project management and technical training.

Cross-training means having more than one individual properly trained to perform a specific job or procedure. This practice has the advantage of decreasing dependence on one employee and can be part of succession planning. Cross-training also provides a backup for personnel in

the event of absence for any reason, providing continuity of operations. However, in using this approach, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposure this may cause.

Scheduling and Time Reporting

Proper scheduling provides for more efficient operation and use of computing resources. The information being entered or recorded into a system must be accurate. Time reporting allows management to monitor the scheduling process. Management can then determine whether staffing is adequate and the operation runs efficiently.

One of the scarcest resources in IT is time, and its proper reporting will help better manage this finite resource. Time reporting can be an excellent source of information for IT governance purposes. This input can be useful for cost allocation, invoicing, chargebacks, KPI measurement and activities analysis (e.g., how many hours the enterprise dedicates to application changes versus new developments).

Terms and Conditions of Employment

As part of their contractual obligation, employees, contractors and third-party users should agree to and sign the terms and conditions of their employment, which should state their and the enterprise's responsibilities for information security. Terms and conditions of employment ensure that the employee, contractor or other third party is aware of expectations for continued employment and repercussions if these are violated. The terms and conditions of employment should reflect the enterprise's security policy in addition to clarifying and stating the following:

- All employees, contractors and third-party users who are given access to sensitive information must sign a confidentiality or nondisclosure agreement before being given access to internal information.
- The employees', contractor's and any other user's legal responsibilities and rights (e.g., regarding copyright laws or data protection legislation)
- Responsibilities for classifying information and managing enterprise assets associated with information systems and services handled by the employee, contractor or third-party user
- Responsibilities of the employee, contractor or third-party user for handling information received from other enterprises or external parties
- Responsibilities of the enterprise for handling employee, customer and vendor personal information, including personal information created as a result of, or in the course of, employment with the enterprise
- Responsibilities that extend outside the enterprise's premises and outside normal working hours (e.g., remote or hybrid working arrangements)
- Actions to be taken if the employee, contractor or third-party user disregards the enterprise's security requirements

The enterprise should ensure that employees, contractors and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of their access to the enterprise's assets associated with information systems and services. Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of employment.

Expectations During Employment

Management should require employees, contractors and third-party users to apply security measures in accordance with the enterprise's established policies and procedures. Specific responsibilities should be documented in approved job descriptions. This guidance will help ensure that employees, contractors and third-party users are aware of their responsibilities and information security threats and concerns. Clear guidance ensures that they are equipped to support the enterprise's security functions during normal work and reduce the risk of human error.

Management responsibilities should be defined to ensure security is applied throughout an individual's employment. All employees, contractors and third-party users should be provided adequate awareness, education and training in security procedures, and the correct ways to access internal resources to minimize possible security risk. A formal disciplinary process for handling security breaches should be established.

Employee Performance Management

Performance management includes goal setting and performance reviews.[31] Goal setting establishes clear objectives for the individual over a specific period. Goals may be based on fulfilling job descriptions, completing projects or displaying behaviors. Often, managers and

[31] Ravishankar, R.A.; K. Alpaio; "5 Ways to Set More Achievable Goals," Harvard Business School Publishing, 30 August 2022, *https://hbr.org/2022/08/5-ways-to-set-more-achievable-goals*

©ISACA. All Rights Reserved.

employees work together to create goals using the SMART goal framework. SMART goals are:

- Specific, clear and understandable
- Measurable, verifiable and results-oriented
- Attainable yet sufficiently challenging
- Relevant to the mission of the department or enterprise
- Time-bound with a schedule and specific milestones

Performance reviews measure progress toward the goal(s). The same process allows the enterprise to gauge employee aspirations and satisfaction and identify problems. Salary increases, performance bonuses and promotions should be based on performance.

Disciplinary Actions

When problems related to an employee's conduct or performance arise, HR may be brought in to provide disciplinary action. One of the most common forms of discipline is a performance improvement plan (PIP). The goal of a PIP is to help employees correct conduct problems and resolve performance issues in a structured, measurable approach.

Promotion Policies

Promotion policies should be fair and equitable and understood by employees. Policies should be based on objective criteria and consider the business need in addition to an individual's performance, education, experience and level of responsibility.

The IS auditor should ensure that the IT organization has well-defined policies and procedures for promotion and is adhering to them. For example, historical promotion data can be audited to look for indicators of bias toward specific demographics.

Required Vacations

A required vacation (holiday) ensures that once a year, at minimum, someone other than the regular employee will perform a job function. This reduces the opportunity to commit improper or illegal acts. During this time, it may be possible to discover fraudulent activity if there has been no collusion between employees to cover possible discrepancies.

Job rotation provides additional control to reduce the risk of fraudulent or malicious acts because the same individual does not always perform the same tasks. This allows someone other than the regularly assigned person to perform the job and notice possible irregularities. In addition, job rotation also guards against the risk of over-dependence on key staff by spreading experience in procedures and controls and specific technologies. Without this, an enterprise can be vulnerable if a key employee is unavailable.

Note

A CISA should be familiar with ways to mitigate internal fraud. Mandatory leave is such a control measure.

Retention and Succession Plans

HR is also responsible for employee retention and succession planning. Retention plans may involve compensation, increased pay, benefits (e.g., paid time off), mentorship programs and professional development.

Succession plans acknowledge that employees will eventually leave the employer or retire. The succession plan ensures there is someone else to perform critical job functions either through redundancies or by having another individual trained to replace a specific individual.

Termination Policies

Written termination policies should be established to provide clearly defined steps for employee separation. Policies must be structured to adequately protect the enterprise's computer assets and data. Termination practices should address voluntary and involuntary (e.g., immediate) terminations. For certain situations, such as involuntary terminations under adverse conditions, an enterprise should have clearly defined and documented procedures for escorting the terminated employee from the premises. In all cases, however, the following control procedures should be applied:

- **Return all devices, access keys, ID cards and badges**—To prevent physical and logical access to enterprise resources. If employees are allowed to use personal devices, these should have company information blocked or removed.
- **Deletion/revocation of assigned login IDs and passwords**—To prohibit system access. Access revocation should include application-specific credentials, not just network IDs and passwords.
- **Notification**: To alert appropriate staff and security personnel regarding the employee's status change to terminated.
- **Arrangement of the final pay routines**—To remove the employee from active payroll files.
- **Performance of a termination interview**—To gather insight into the employee's perception of management and identify opportunities to improve employee retention.

 ©ISACA. All Rights Reserved.

Note

Changes in job role and responsibilities, such as a transfer to a different department, may necessitate revocation and issuance of different system and work area access rights, similar to termination procedures.

2.8.5 Enterprise Change Management

Enterprise change management involves using a defined and documented process to identify and apply technology improvements at the infrastructure and application levels that benefit the enterprise and involve all levels impacted by the changes. This level of involvement and communication will ensure that the IT department fully understands the users' expectations and that users do not resist or ignore changes after implementation.

The IT department is the focal point for such changes by leading or facilitating enterprise change. This includes staying abreast of technological changes that can lead to significant business process improvements and obtaining senior management commitment for the changes or projects required at the user level.

After senior management support is obtained to move forward with changes or projects, the IT department can begin working with each functional area and its management to obtain support for the changes. In addition, the IT department will need to develop a communication process targeting the end users to provide an update on the changes, how they impact their jobs, and the expected benefit they will bring. The communication should include a method for obtaining user feedback and involvement.

User feedback should be obtained throughout the project, including validation of the business requirements, end-user acceptance testing and training on the new or changed functionality.

For more information, see chapter 3 Information Systems Acquisition, Development and Implementation.

2.8.6 Financial Management Practices

Financial management is a critical element of all business functions. From a financial perspective, technology costs are a major element of an enterprise's budget. Technology resources are expensive to acquire, develop and maintain. Plus, the useful life of those resources is relatively short, requiring the enterprise to incur regular replacement costs.

Cost Allocation

Some enterprises employ a process where the receiving department incurs the cost directly to allocate IT costs back to the supported business function. In this scheme, the costs of IS services—including staff time, computer time and other relevant costs—are charged back to the end users based on a standard (uniform) formula or calculation. This user-pays method can improve the application and monitoring of IS expenses and available resources.

Using chargebacks provides all involved parties with a cost similar to a market rate for the service provided by the IPF. Where implemented, the chargeback policy should be established by the board and jointly implemented by the CFO, user management and IS management.

IS Budgets

IS management, like all other departments, must develop a budget. A budget facilitates forecasting, monitoring and analyzing financial information. The budget includes the expected allocation of funds, especially in an IS environment with high expenses. The IS budget should be linked to short-term projects and long-term IT objectives.

Software Expenses versus Capitalization

Properly classifying software costs as operating or capital expenses is a major financial element in IT. In the United States and countries using International Accounting Standards Board (IASB) guidance, accounting standards require companies to understand their development efforts, including time spent on specific projects and activities. An IS auditor should understand these requirements and companies' practices to track software development costs.

International Accounting Standard 38 (IAS 38) outlines six criteria to be met if development costs are capitalized. Of these, an enterprise should demonstrate "[h]ow the intangible asset will generate probable future economic benefits."[32] Intangible assets include websites and software if they satisfy this criterion. Interpretations vary on the meaning of demonstrating the usefulness of the intangible asset. Therefore, the IS auditor who is working with enterprises following International

[32] International Financial Reporting Standards Foundation, "IAS 38 Intangible Assets," *https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/*

©ISACA. All Rights Reserved.

Financial Reporting Standards (IFRS) must obtain guidance from the chartered accountants responsible for financial reporting.

Similarly, when software is purchased, certain costs may be considered capital versus operating expenses, but these must follow accounting guidelines. For example, software purchased outright and installed on-premises is generally a capital expense, compared to cloud-based software purchased as a subscription, which is usually an operating expense. Fraudulently manipulating these classifications can lead to material financial reporting misstatements. Although IS auditors may not be expected to know all the accounting rules in this area, they can help the enterprise by ensuring that teams are tracking the expenses properly against an approved budget.

2.8.7 Information Security Management

Information security management provides the lead role to ensure that the enterprise's information and information processing resources are properly protected. An information security management team is responsible for safeguarding the enterprise's information assets and protecting them from unauthorized access, use, disclosure, disruption, modification or destruction. Their primary goal is maintaining the enterprise's information confidentiality, integrity and availability. They play a crucial role in protecting the enterprise's sensitive information, maintaining the trust of customers and partners and ensuring business continuity in the face of evolving cybersecurity threats. Some key responsibilities within information security management include the following:

- **Risk assessment and management**—They identify and assess the potential risk to the enterprise's information systems and assets. This involves conducting regular risk assessments, evaluating vulnerabilities and implementing risk management strategies.
- **Security policy development**—They develop and enforce information security policies, standards, guidelines and procedures for the enterprise. These policies outline the rules and best practices to be followed by employees, contractors and other stakeholders to ensure information security.
- **Incident response and management**—The team establishes procedures to handle security incidents and coordinates the response efforts. They investigate security breaches, mitigate the impact and take necessary actions to prevent future incidents.
- **Security awareness and training**—They conduct security awareness programs and training sessions for employees to educate them about information security best practices, threats and their responsibilities. This helps in creating a security-conscious culture within the organization.
- **Security architecture and design**—They collaborate with other teams to design secure information systems, networks and infrastructure. They ensure that security controls, such as firewalls, intrusion detection systems, encryption and access controls, are implemented effectively.
- **Vulnerability management**—They regularly scan systems and networks for vulnerabilities, apply patches and updates and conduct penetration testing to identify weaknesses that attackers can exploit. They also ensure that the enterprise has a process for addressing vulnerabilities promptly.
- **Business continuity planning (BCP) and disaster recovery planning (DRP)**—They conduct BIAs and desktop scenarios to determine key metrics such as recovery time objective (RTO) and recovery point objective (RPO). RTO is the maximum acceptable downtime or time to recover a system, application or service after a disruption. RTO defines the time a business must resume operations to avoid significant consequences. RPO specifies the maximum amount of data loss (usually expressed in time units) that an enterprise is willing to tolerate in the event of a data loss. See chapter 4 Information Systems Operations and Business Resilience for more information.
- **Identity and access management**—They manage user accounts, access rights and privileges within the enterprise's systems and applications. This includes implementing strong authentication mechanisms, enforcing least privilege principles and monitoring user activity for suspicious behavior. See section 5.3 Identity and Access Management for more information.
- **Compliance and regulatory requirements**—The team ensures that the enterprise complies with relevant laws, regulations and industry standards about information security. They conduct audits, implement controls and provide documentation to demonstrate compliance.
- **Security incident monitoring and analysis**—They monitor security logs and alerts from various systems and employ security information and event management (SIEM) tools to detect and analyze potential security incidents. They investigate anomalies, identify patterns and take appropriate action to mitigate threats.

 ©ISACA. All Rights Reserved.

2.9 IT Vendor Management

IT vendor and third-party risk management have become major concerns for enterprises. There is an increased reliance on products and services offered by third-party vendors, which increases the probability of security incidents, data breaches and other risk exposure. Many of the most significant data breaches in recent years originated through vendor access to enterprise networks. Increased risk exposure from IT vendors requires enterprises to take an active role in managing and mitigating third-party risk before negative impacts are faced by their customers or operations.

Best practices in managing risk from IT vendors includes:

- Performing risk assessments on all potential IT vendors before awarding contracts
- Including right-to-audit clauses in all vendor contracts
- Providing the minimum access required to vendors (i.e., the principle of least privilege)
- Maintaining an accurate inventory of all IT vendors and the level of access provided
- Removing vendor access when the relationship ends
- Monitoring and certifying all IT vendors regularly

2.9.1 Sourcing Practices

Sourcing practices relate to how the enterprise obtains the IT functions required to support the business. Enterprises can perform all the IT functions in-house (known as insourcing) in a centralized fashion or outsource all functions across the globe. The sourcing strategy should consider each IT function and determine which approach allows the IT function to meet the enterprise goals.

Delivery of IT functions can be characterized as:

- **Insourced**—Fully performed by enterprise staff
- **Outsourced**—Fully performed by the vendor staff
- **Hybrid**—Performed by a mix of enterprise and vendor staff; can include joint ventures/supplemental staff

IT functions can be performed across the globe, taking advantage of time zones and arbitraging labor rates, and can be classified as:

- **Onsite**—Staff work onsite in the IT department.
- **Offsite**—Also known as nearshore, staff works remotely in the same area.
- **Offshore**—Staff work at a remote location in a different geographic region.

The enterprise should evaluate its IT objectives and current staffing model to determine the most appropriate method of delivering the IT functions, considering the following questions:

- Is this a core function of the enterprise?
- Does this function have specific knowledge, processes and staff critical to meeting its goals and objectives, which cannot be replicated externally or in another location?
- Can this function be performed by another party or in another location for the same or lower price, with the same or higher quality, and without increasing risk?
- Does the enterprise have experience managing third parties or using remote/offshore locations to execute IS or business functions?
- Are there any contractual or regulatory restrictions preventing offshore locations or the use of foreign nationals?

On completion of the sourcing strategy, the IT steering committee should review and approve the decision if an agreement is reached. At this point, if the enterprise has chosen to use outsourcing, a rigorous process should be followed, including the following steps:

- Define the IT function to be outsourced.
- Describe the service levels required and minimum metrics to be met.
- Know the desired level of knowledge, skills and quality of the expected service provider desired.
- Know the current in-house cost information to compare with third-party bids.
- Conduct due diligence reviews of potential service providers.
- Confirm any architectural considerations to meet contractual or regulatory requirements.
- Communicate the decision and any monitoring requirements to impacted internal stakeholders.

Using this information, the enterprise can perform a detailed analysis of the service provider bids and determine whether outsourcing will allow the enterprise to meet its goals cost-effectively, with limited risk. The same process should be considered when an enterprise chooses to outsource its IT functions offshore.

An IS auditor must understand the scope of vendor-provided services (e.g., commercial off-the-shelf hardware/software products, outsourced services to include cloud offerings, managed services, etc.) and the functional requirements these services address. Furthermore, an IS auditor needs to understand the vendor's SLAs that are in place to address system/software operational and technical support requirements. Additional considerations include the suppliers' financial viability, licensing scalability and provisions for software escrow.

©ISACA. All Rights Reserved.

Although IS auditors are not legal or contract auditors, they must understand the importance of requirements specifications that form the request for proposal (RFP). They must understand the need for required security and other controls to be specified, the essential elements of vendor selection to ensure that a reliable and professional vendor is chosen and the essential contents of the contract—most notably, the need, as appropriate, for an escrow agreement to be in place. The right to audit must also be addressed in the contract.

The contract should also set expectations for any assurance testing and reporting by a trusted third party (e.g., through certification in an international standard). For example, many cloud-based service providers must deliver an SOC report each year detailing their internal controls and testing results completed by an external auditor.

2.9.2 Outsourcing Practices and Strategies

Outsourcing is the mechanism that allows enterprises to transfer the delivery of services to third parties. Fundamental to outsourcing is accepting that, while service delivery is transferred, accountability remains firmly with the management of the client enterprise, which must ensure that the risk is managed correctly with the continued delivery of value from the service provider. Transparency and ownership of the decision-making process must reside within the client's purview.

The decision to outsource is a strategic, not merely a procurement, decision. The enterprise that outsources is effectively reconfiguring its value chain by identifying core activities to its business to retain and noncore activities for outsourcing. Understanding this in light of governance is key, not only because well-governed enterprises have been shown to increase shareholder value but also because organizations compete in an increasingly aggressive, global and dynamic market.

Establishing and retaining competitive and market advantage require the enterprise to respond effectively to competition and changing market conditions. Outsourcing can support this only if the enterprise understands which parts of its business create a competitive advantage.

Outsourcing practices relate to contractual agreements under which an enterprise hands over control of part or all of the functions of the IT department to an external party. Most IT departments use information resources from a wide array of vendors and, therefore, need a defined outsourcing process to manage contractual agreements with these vendors.

The contractor provides the resources and expertise required to perform the agreed-on service. Outsourcing is becoming increasingly important in many enterprises. The IS auditor must know the various forms outsourcing can take and the associated risk.

The specific objectives for IT outsourcing vary from enterprise to enterprise. Typically, the goal is to achieve lasting, meaningful improvement in business processes and services through enterprise restructuring to take advantage of a vendor's core competencies. Like with the decision to downsize or rightsize, outsourcing services and products requires management to revisit the control framework on which it can rely.

Reasons for embarking on outsourcing include:

- A desire to focus on core activities
- Pressure on profit margins
- The increasing competition that demands cost savings and faster time-to-market
- Flexibility concerning organization, structure and market size

An IS auditor should determine whether an enterprise considered the advantages, disadvantages, business risk and risk reduction options depicted in **figure 2.13** as it developed its outsourcing practices and strategies.

 ©ISACA. All Rights Reserved.

Figure 2.13—Advantages, Disadvantages and Business Risk, and Risk Reduction Options Related to Outsourcing

Possible Advantages	Possible Disadvantages and Business Risk	Risk Reduction Options
• Commercial outsourcing enterprises can achieve economies of scale by deploying reusable component software. • Outsourcing vendors are likely to be able to devote more time and focus more effectively and efficiently on a given project than in-house staff. • Outsourcing vendors will likely have more experience with various problems, issues and techniques than in-house staff. • Developing specifications and contractual agreements using outsourcing services will likely result in better specifications than if created only by in-house staff. • Because vendors are highly sensitive to time-consuming diversions and changes, feature or scope creep is substantially less likely with outsourcing vendors.	• Costs exceeding customer expectations • Loss of internal IT experience • Loss of control over IT • Vendor failure (ongoing concern) • Limited product access • Difficulty in reversing or changing outsourced arrangements • Deficient compliance with legal and regulatory requirements • Contract terms not being met • Lack of loyalty of contractor personnel toward the customer • Disgruntled customers/employees as a result of the outsourcing arrangement • Service costs not being competitive throughout the entire contract • Obsolescence of vendor IT systems • Failure of either enterprise to receive the anticipated benefits of the outsourcing arrangement • Reputational damage to either or both enterprises due to project failures • Lengthy, expensive litigation • Loss or leakage of information or processes	• Establishing measurable, partnership-enacted shared goals and rewards • Software escrow to ensure maintenance of the software • Using multiple suppliers or withholding a piece of business as an incentive • Performing periodic competitive reviews and benchmarking/bench trending • Implementing short-term contracts • Forming a cross-functional contract management team • Including contractual provisions to consider as many contingencies as can reasonably be foreseen

In addition, an enterprise should consider the following provisions in its outsourcing contracts:

- Incorporate service quality expectations, including using *ISO/IEC TR 33015:2019 Information technology—Process assessment—Guidance for process risk determination*, CMMI, ITIL or ISO methodologies.
- Ensure adequate contractual consideration of access control/security administration for the enterprise and the vendor.
- Ensure that the contract requires violation reporting and follow-up, ideally with associated SLAs.
- Ensure any requirements for owner notification and cooperation with any investigations.
- Ensure that change/version control and testing requirements are contractually required for the implementation and production phases.
- Ensure that the parties responsible and the requirements for network controls are adequately defined and any necessary delineation of these responsibilities established.
- State specific performance parameters that must be met, such as minimum processing times for transactions or minimum hold times for contractors.
- Incorporate capacity management criteria.
- Provide contractual provisions for making changes to the contract.
- Provide a clearly defined dispute escalation and resolution process.
- Ensure the contract indemnifies the enterprise from damages caused by the organization responsible for the outsourced services.
- Require confidentiality agreements such as nondisclosure agreements (NDAs) protecting both parties.
- Incorporate straightforward, unambiguous right-to-audit provisions, providing the right to audit vendor operations (e.g., access to facilities, access to records, right to make copies, access to personnel, provision

©ISACA. All Rights Reserved.

of computerized files) as they relate to the contracted services.
- Ensure the contract adequately addresses business continuity, disaster recovery provisions and appropriate testing.
- Establish that the confidentiality, integrity and availability (sometimes called the CIA triad) of enterprise-owned data must be maintained and clearly establish the ownership of the data.
- Require the vendor to comply with all relevant legal and regulatory requirements, including those enacted after contract initiation.
- Establish ownership of intellectual property developed by the vendor on behalf of the customer.
- Establish explicit warranty and maintenance periods.
- Provide software escrow provisions.
- Protect intellectual property rights.
- Comply with legislation.
- Establish clear roles and responsibilities between the parties.
- Require that the vendor follow the enterprise's policies, including its information security policy, unless the vendor policies have been agreed to in advance by the enterprise.
- The vendor must identify all subcontract relationships and require the enterprise's approval to change subcontractors.

Outsourcing requires management to actively manage the relationship and the outsourced services. Because the outsourcing agreement is governed by the contract terms, the contract with the outsourced service provider should include a description of the means, methods, processes and structure accompanying the offer of IT services and products and QC. The formal or legal character of these agreements depends on the relationship between the parties and the demands placed by principals on those performing the engagement.

After the outsourcer has been selected, the IS auditor should regularly review the contract and service levels to ensure that they are appropriate. In addition, the IS auditor could review the documented procedures of the outsourcer and results of its quality programs—including ISO/IEC TS 33061:2021, CMMI, ITIL and ISO methodologies. These quality programs require regular audits to certify that the process and procedures meet the quality standard.

Outsourcing is not only a cost decision; it is a strategic decision with significant control implications for management. Quality of service, guarantees of continuity of service, control procedures, competitive advantage and technical knowledge are issues that need to be part of the decision to outsource IT services. Choosing the right supplier is extremely important, mainly when outsourcing is a long-term strategy. The compatibility of suppliers in terms of culture and personnel is an essential issue that management should not overlook.

The decision to outsource a particular service currently within the enterprise demands proper attention to contract negotiations. A well-balanced contract and SLA are important for quality purposes and future cooperation between the concerned parties. SLAs stipulate and commit a vendor to a required level of service and support options. This includes providing a guaranteed level of system performance regarding downtime or uptime and a specified level of customer support. Software or hardware requirements are also stipulated. SLAs also provide penalty provisions and enforcement options for services not provided. They may also include incentives, such as bonuses or gain-sharing, for exceeding service levels.

SLAs are a contractual means of helping the IT department manage information resources under vendor control. Above all, an SLA should serve as an instrument of control. The enterprise should be aware of cross-border legislation if the outsourcing vendor is from another country. All outsourcing must be reviewed and approved by the enterprise's legal team.

Industry Standards/Benchmarking

Most outsourcing organizations must adhere to a well-defined set of standards that their clients can rely on. These industry standards provide a means of determining the level of the service supplied by similar outsourcing arrangements. These standards can be obtained from vendor user groups, industry publications and professional associations. Examples include *ISO 9001:2015: Quality management systems—Requirements* and CMMI.

Globalization Practices and Strategies

Many enterprises globalize their IT functions in addition to outsourcing functions. The globalization of IT functions is performed for many of the same reasons cited for outsourcing; however, the enterprise may choose not to outsource the IT function entirely. Globalizing IT functions requires management to actively oversee remote or offshore locations.

Where the enterprise performs functions in-house, it may move the IT functions offsite or offshore. The IS auditor can assist in this process by ensuring that IT management

 ©ISACA. All Rights Reserved.

considers the following risk and audit concerns when defining the globalization strategy and completing the subsequent transition to remote offshore locations:

- **Legal, regulatory and tax issues**—Operating in a different country or region may introduce new risk about which the enterprise may have limited knowledge.
- **Continuity of operations**—Business continuity and disaster recovery may not be adequately designed and tested.
- **Personnel**—Needed modifications to personnel policies may not be considered.
- **Telecommunication issues**—Network controls and access from remote or offshore locations may be subject to more frequent outages or a significant number of security exposures.
- **Cross-border and cross-cultural issues**—Managing people and processes across multiple time zones, languages and cultures may present unplanned challenges and problems. Cross-border data flow may also be subject to legislative requirements (e.g., that data must be encrypted during transmission).
- **Planned globalization and/or important expansion**—Understanding future business expansion plans may impact the location chosen for offshoring personnel.

Outsourcing and Third-Party Audit Reports

One method for the IS auditor to have an assurance of the controls implemented by a service provider requires the provider to periodically submit a third-party audit report. These reports cover a range of issues related to confidentiality, integrity and availability of data. In some industries, third-party audits may fall under regulatory oversight and control, such as Statement on Standards for Attestation Engagements (SSAE) 18 and an audit guide by the American Institute of Certified Public Accountants (AICPA), which provides a framework for three Service Organization Control (SOC) reporting options (SOC 1, SOC 2 and SOC 3 reports). These reporting standards represent significant changes from the previously used Statement on Auditing Standards (SAS) 70 report, because enterprises increasingly became interested in risk beyond financial statement reporting (e.g., privacy). The International Auditing and Assurance Standards Board (IAASB) also issued new guidance in the International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization.

An IS auditor should be familiar with the following:

- Management assertions and how well these address the services being provided by the service provider
- SSAE 18 reports as follows:
  - **SOC 1**—Report on the service organization's system controls that are likely to be relevant to the user entities' internal control over financial reporting
  - **SOC 2**—Report on the service organization's system controls that are relevant to security, availability, processing integrity, confidentiality, or privacy, including the service organization's compliance with its privacy practices
  - **SOC 3**—Similar to a SOC 2 report, but does not include a detailed understanding of the design of controls and the tests performed by the service auditor
- Additional third-party audit reports, such as penetration tests and security assessments.
- How to validate third-party assessments that were performed by independent, objective and competent third parties
- Internal processes for handling qualified opinions from the assessor
- The use of bridge letters when the new annual report is not available when expected
- How to obtain, review and present report results to management for further action

2.9.3 Cloud Governance

The strategic direction of the business and IT, in general, is the primary focus when considering cloud computing. As enterprises look to the cloud to provide IT services that traditionally have been managed internally, they will need to make some changes to help ensure that they continue to meet performance objectives, their technology provisioning and business are strategically aligned, and risk is managed. Ensuring that IT is aligned with the business, systems are secure and risk is managed can be challenging in any environment and even more complex in a third-party relationship. Typical governance activities, such as goal setting, policy and standard development, defining roles and responsibilities, and managing risk, must include special considerations when dealing with cloud technology and its providers.

As with all enterprise changes, it is expected that some adjustments will need to be made to how business processes are handled. Business/IT processes, such as data processing, development and information retrieval, are examples of potential change areas. Additionally,

©ISACA. All Rights Reserved.

processes detailing how information is stored, archived and backed up need to be revisited.

The cloud presents many unique situations for businesses to address. One significant governance issue is that business unit personnel, previously forced to go through IT for service, can now bypass IT and receive service directly from the cloud. Policies must be modified or developed to address the process of sourcing, managing and discontinuing cloud services.

Managing the relationship with a third party should be assigned to a designated individual or service management team. In addition, the enterprise should ensure that the third party assigns responsibilities for checking for compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor whether the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in service delivery are observed, such as enforcing SLAs or determining if the vendor is still a viable partner.

The enterprise should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or IPFs accessed, processed or managed by a third party.

The enterprise also should ensure that it retains visibility into security activities, such as change management, identification of vulnerabilities and information security incident reporting/response, through a clearly defined reporting process, format and structure.

Some considerations for addressing these areas include:

- Developing a cloud risk management strategy
- Implementing strong cybersecurity controls
- Managing cloud resilience, outsourcing, vendor lock-in and concentration risk
- Ensuring staff have adequate skillset to manage cloud risk

When outsourcing, the enterprise must know that the ultimate responsibility for information processed by an outsourcing party remains with the enterprise.

Note

Technical aspects of cloud computing and cloud computing delivery models are discussed in 5 Protection of Information Assets.

2.9.4 Governance in Outsourcing

Governance of outsourcing is the set of responsibilities, roles, objectives, interfaces and controls required to anticipate change and manage the introduction, maintenance, performance, costs and management of third-party-provided services. The client and service provider must work together to provide a common, consistent and effective approach that identifies the necessary information, relationships, controls and exchanges among stakeholders across both parties.

The decision to outsource and subsequently successfully manage that relationship demands effective governance. Most people who conduct outsourcing contracts include basic control and service execution provisions; however, one of the main objectives of the outsourcing governance process, as defined in the outsourcing contract, is to ensure continuity of service at the appropriate levels, profitability and added value to sustain the commercial viability of both parties. Experience has shown that many enterprises make assumptions about what is included in the outsourcing proposition. Although contractually defining every detail and action is not feasible, the governance process provides the mechanism to balance risk, service demand, service provision and cost.

The governance of outsourcing extends the responsibilities of both parties' (i.e., client and supplier) into the following:

- Ensure contractual viability through continuous review, improvement and benefits gained for both parties.
- Include an explicit governance schedule in the contract.
- Manage the relationship to meet contractual obligations through SLAs and operating level agreements (OLAs).
- Identify and manage all stakeholders, their relationships and expectations.
- Establish clear roles and responsibilities for decision making, issue escalation, dispute management, demand management and service delivery.
- Allocate resources, expenditures and service consumption in response to prioritized needs.
- Continuously evaluate performance, cost, user satisfaction and effectiveness.
- Communicate with all stakeholders on an ongoing basis.

The increasing size of the technology solution space is driven by the pace of technological evolution. Acquiring, training and retaining qualified staff are becoming more expensive. Investing in costly technology implementation

and training is seen as less of an enterprise core activity than the ability to work effectively across the value chain by integrating outsourcing services where appropriate.

Although the term business alignment is often used, what it encompasses is not always clear. In the broadest sense, alignment involves making the services provided by the enterprise IT function more closely reflect the requirements and desires of the business users. When enterprises recognize what is core to their business and which services provide them a differential advantage, then outsource the activities supporting these services, business alignment can be achieved. The implication is that SLAs and OLAs must be established, monitored and measured in terms of performance and user satisfaction. Business alignment should be driven by those who receive the service.

Governance should be preplanned and built into the contract as part of the service cost optimization. The defined governance processes should evolve as the needs and conditions of the outsourcing relationship adapt to changes in service demand and delivery and technological innovation.

The IS auditor must understand right-to-audit clauses and controls in outsourcing activities involving confidential information and sensitive processes. This understanding includes these issues:

- How auditing of the outsourced service provider is allowed to be conducted under the terms of the contract
- What visibility the IS auditor has into the internal controls being implemented by the outsourced service provider to provide reasonable assurance that confidentiality, integrity and availability and preventive, detective and corrective controls are in place and effective
- A requirement that SLAs regarding problem management, including incident response, are documented and communicated to all parties affected by these outsourcing agreements

2.9.5 Capacity and Growth Planning

Given the strategic importance of IT in enterprises and constant technological change, capacity and growth planning are essential. This activity must be reflective of long- and short-range business plans. It must be considered within the budgeting process. Changes in capacity should reflect changes in the underlying infrastructure and the number of staff available to support the enterprise. A lack of appropriately qualified staff may delay projects critical to the enterprise or result in not meeting agreed-on service levels. This can lead some enterprises to choose outsourcing as a solution for growth.

2.9.6 Third-Party Service Delivery Management

Every enterprise using the services of third parties should have a service delivery management system in place to implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.

The enterprise should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed to with the third party.

Monitoring and Review of Third-Party Services

The services, reports and records that the third party provides should be monitored and reviewed, and audits should be carried out regularly. Monitoring and reviewing third-party services should ensure that the agreement information security terms and conditions are being adhered to and information security incidents and problems are managed appropriately. This should involve a service management relationship and process between the enterprise and the third party to accomplish the following:

- Monitor service performance levels to check adherence to the agreements.
- Review service reports that the third party produces and arrange regular progress meetings as the agreements require.
- Provide information about information security incidents and review this information by the third party and the enterprise, as required by the agreements and any supporting guidelines and procedures.
- Review third-party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered.
- Resolve and manage any identified problems.

Managing Changes to Third-Party Services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed considering the criticality of business systems and processes involved and reassessing risk.

©ISACA. All Rights Reserved.

The process of managing changes to a third-party service needs to consider the following:

- Changes made by the enterprise to implement:
  - Enhancements to the current services offered
  - Development of any new applications and systems
  - Modifications or updates of the enterprise's policies and procedures
  - New controls to resolve information security incidents and improve security
  - Updates to policies, including the IT security policy
- Changes in third-party services to implement:
  - Changes and enhancements to networks
  - Use of new technologies
  - Adoption of new products or newer versions/ releases
  - New development tools and environments
- Changes to the physical location of service facilities
- Change of vendors or subcontractors

Service Improvement and User Satisfaction

SLAs set the baseline by which outsourcers perform the IT function. In addition, enterprises can set service improvement expectations in the contracts with associated penalties and rewards. Examples of service improvements include:

- Reductions in the number of help desk calls
- Reductions in the number of system errors
- Improvements to system availability

Service improvements should be agreed on by users and IT with the goals of improving user satisfaction and attaining business objectives. User satisfaction should be monitored by interviewing and surveying users at intervals aligned with SLA periods.

2.10 IT Performance Monitoring and Reporting

Enterprises recognize the need to increasingly invest in IT and related technology. With this investment, management's expectations have increased because it wants to see progress and a return on its investment. Stakeholders must be assured that these investments are strategically aligned, managed appropriately and focused on achieving business goals. IT performance measurement and reporting may be statutory or contractual requirements. Appropriate performance measurement practices for the enterprise include outcome measures for business value, competitive advantage and defined performance metrics that show how well IT performs. Incentives, such as rewards, compensation and recognition, should be linked to performance measures. Sharing results and progress with employees, customers and stakeholders is also important.

Effective IT performance management requires a monitoring process. Monitoring is needed to ensure that appropriate actions are taken to keep projects following the set directions and policies. The monitoring process includes defining key performance indicators (KPIs), key risk indicators (KRIs), key control indicators (KCIs), systematic and timely performance reporting and prompt action when discovering deviations. These metrics describe a quality critical to the enterprise, requiring a measurable baseline and usually a threshold for failure or success. These measurement metrics help monitor achievements compared to goals and evaluate the effectiveness and efficiency of business processes.

2.10.1 Key Performance Indicators

Many enterprises invest significant time and effort in one of the most common indicators used to monitor processes, KPIs, to ensure that teams are meeting their targets and the enterprise is meeting its objectives. One example of a KPI is employee satisfaction. This KPI measures the level of satisfaction that employees have with the IT services that they receive. A high employee satisfaction rating indicates that the IT department is meeting the needs of the business.

A KPI is a measure that determines how well the process is performing in enabling the goal to be reached. It is a lead indicator of whether a goal will likely be reached and a good indicator of capabilities, practices and skills. For example, a service delivered by IT is a goal for IT but a performance indicator and a capability for the business. This is why performance indicators are sometimes referred to as performance drivers, particularly in BSCs.

As controls are selected for implementation, criteria should also be established to determine the operational level and effectiveness of the controls. These criteria will often be based on KPIs that indicate whether a control is functioning correctly. For example, a KPI for the implementation process measures the relative success of the changeover compared to desired performance objectives. The success of a changeover is often measured as a percentage of errors, number of trouble reports, duration of a system outage or degree of customer satisfaction. The use of the KPI indicates to management whether the change control process was managed correctly, with sufficient levels of quality and testing.

 ©ISACA. All Rights Reserved.

2.10.2 Key Risk Indicators

KRIs provide an early warning, which can help an enterprise identify exposure to risk events that may harm business performance. One example of a KRI could be the percentage increase in phishing attempts. The KRI indicates an increased threat level. Generally, KRIs include a threshold above which alerts are sent to individuals assigned to monitor the risk.

2.10.3 Key Control Indicators

KCIs measure how well a control performs in reducing causes, consequences or the likelihood of risk. An example of a KCI is the percentage of IT assets compliant with security policies. This KCI measures the effectiveness of the enterprise's IT security policies in ensuring that IT assets are appropriately protected.

Developing metrics usually involves four steps:
1. Identify critical data points needed to achieve business objectives.
2. Identify specific, quantifiable outputs of work from the identified processes.
3. Establish targets against which results can be scored.
4. Monitor performance against the metrics and report results to those who can adjust.

For a metric to be considered effective, it should be consistently measured. In addition, it should be based on acceptable best practices, be useful for internal and external comparison and be meaningful to IT's customers and sponsors. The data should be gathered accurately; it should be expressed as a number, percentage or unit of measure, and it should be contextually specific.

An IS auditor should ensure that performance metrics cover the following:
- Impact on long-term organizational objectives (e.g., technical, financial and operational goals)
- Performance against the short-term business and IT plans
- Risk and compliance with regulations
- Internal and external user satisfaction with service levels
- Key IT processes, including solution and service delivery
- Future-oriented activities (e.g., emerging technology, reusable infrastructure, business and IT personnel skill sets)

Most enterprises must continuously monitor the performance and capacity of IT resources to ensure the performance measurement approach is regularly reviewed, revised and updated according to management feedback and changing business needs.

2.10.4 Performance Optimization

Performance measures how well a system works, including user and stakeholder satisfaction with the service. Performance optimization is the process of improving the efficiency of an information system while maintaining or increasing the perceived service performance to the highest level possible with minimal additional investment in the IT infrastructure. Effective performance management approaches create and facilitate actions to improve performance and enterprise governance. Performance measures are not used for assigning accountability or complying with reporting requirements.

A well-defined performance measurement process also ensures performance is monitored consistently and reliably. Effective governance significantly enables overall performance optimization and is achieved when:
- Goals are set by senior leadership and aligned with high-level, approved business objectives.
- Metrics are established by process owners and aligned with goals designed to achieve business objectives.
- Performance is monitored by each layer of management.

Critical Success Factors

The success or failure of a performance optimization effort often hinges on a series of CSFs. Each of the CSFs is a vital element, and the failure of any of the factors can undermine the success of the performance optimization.

Critical governance success factors include:
- **Leadership support**–Process optimization is a complex and time-consuming effort, so it is important to have the support of senior leadership. Leadership should be involved in setting the goals for process optimization, providing resources, communicating the benefits of process optimization to the enterprise and assuming ultimate accountability for the optimization program.
- **Clear goals and objectives**–Before the enterprise can optimize its processes, it must define the specific goals and objectives of the process optimization initiative. After the enterprise identifies what it wants to achieve, it can identify areas where processes can be improved.
- **Data-driven decision making**–Process optimization should be based on data, not gut instinct. The enterprise must collect data about its current

©ISACA. All Rights Reserved.

processes to identify areas where they can be improved. This data can be collected through surveys, interviews and process mapping.

- **Employee involvement**–The people who work in the enterprise are the experts on its processes. They know where the problems are and have the best ideas for improving them, making it important to involve employees in the process optimization process by forming a process improvement team or holding brainstorming sessions.
- **Continuous improvement**–Process optimization is not a one-time event. It is an ongoing process of identifying and improving enterprise processes. By creating a culture of continuous improvement in the enterprise, everyone in the enterprise constantly looks for ways to improve their processes.

IT is a complex and technical topic; therefore, it is important to maintain transparency by expressing goals, metrics and performance reports in common, understandable terms that are meaningful to the stakeholders so that appropriate actions can be taken.

Methodologies and Tools

Various improvement and optimization methodologies complement simple, internally developed approaches. These include:

- Continuous improvement methodologies, such as the plan, do, check, act (PDCA) cycle
- Comprehensive best practices, such as ITIL
- Frameworks, such as COBIT

The PDCA cycle is an iterative four-step management method used in business to control and continuously improve processes and products. The steps in each successive PDCA cycle are:

1. **Plan**—Establish the objectives and processes necessary to deliver results according to the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the specification are also a part of the targeted improvement. When possible, start on a small scale to test possible effects.
2. **Do**—Implement the plan, execute the process and make the product. Collect data for charting and analysis in the following check and act steps.
3. **Check**—Study the actual results (measured and collected in the do step) and compare them against the expected results (targets or goals from the plan step) to ascertain differences. Look for deviation in implementation from the plan and for the appropriateness/completeness of the plan to enable the execution (i.e., the do step). Charting data can make it much easier to see trends over several PDCA cycles and convert the collected data into information needed for the next step.
4. **Act**—Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improving the process or product. When passing through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve, with more detail in the next cycle iteration or attention placed in a different stage of the process.

Using PDCA following agile development allows for reassessment of the project's direction at points throughout the development life cycle. This is done through sprints or iterations, which require working groups to produce a functional product. This focus on abbreviated work cycles led to the description of agile methodology as iterative and incremental. Compared to a single opportunity to achieve each aspect of a project, like in the waterfall method, agile development allows each aspect to be continually revisited. Other examples of EGIT frameworks include:

- COBIT was developed by ISACA to support EGIT by providing a framework to ensure that IT is aligned with the business, IT enables the business and maximizes benefits, IT resources are used responsibly and IT risk is managed appropriately. COBIT provides tools to assess and measure the performance of IT processes within an enterprise.
- The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series is a set of best practices that guide enterprises in implementing and maintaining information security programs. ISO/IEC 27001 has become a well-known standard in the industry.
- The Information Technology Infrastructure Library (ITIL®) was developed by the UK Office of Government Commerce (OGC), in partnership with the IT Service Management Forum, and is a detailed framework with hands-on information regarding how to achieve successful operational service management of IT. It also includes business value delivery.
- The Open Information Security Management Maturity Model (O-ISM3) is a process-based ISM maturity model for security.
- *ISO/IEC 38500:2015 Information technology—Governance of IT for the organization* provides guiding principles for members of governing bodies of enterprises on the effective, efficient and acceptable use of IT within an enterprise.

- ISO/IEC 20000 is a specification for service management that is aligned with the ITIL service management framework. *ISO/IEC 20000-1:2018 Information technology—Service management—Part 1: Service management system requirements* consists of specific requirements for service management improvement and *ISO/IEC 20000-2:2019 Information technology—Service management—Part 2: Guidance on the application of service management systems* provides guidance and examples for the application of *ISO/IEC 20000-1:2018*.
- *ISO 31000:2018 Risk management—Guidelines* provides guidelines on, and a common approach to, risk management for enterprises.

2.10.5 Approaches and Techniques

Tools and techniques that facilitate measurements, good communication and organizational change are discussed in the following sections.

Six Sigma

Six Sigma and Lean Six Sigma are proven quantitative (data-driven) process analysis and improvement approaches that easily apply to IT. Six Sigma aims to implement a measurement-oriented strategy focused on process improvement and defect reduction. A Six Sigma defect is defined as anything outside customer specifications. Lean Six Sigma is similar but seeks to eliminate unnecessary steps that do not add value.

Business Agility/Agile Methodology

Business agility, or agile, is often described as a mindset or a way of working that emphasizes flexibility when delivering value to the enterprise. Agile aims to deliver products and services earlier, in smaller increments, instead of all at once and much later. In this way, IT can adjust the delivery based on changing needs and business requirements. Agile prioritizes customer satisfaction by responding to change and incorporating customer feedback. Although agile was first developed for software development teams, it has since been adapted into a project management methodology.

Key principles of the agile methodology include:

- **Customer collaboration**—Active involvement of customers or stakeholders throughout the project to gather requirements, provide feedback and ensure that the final product meets their needs.
- **Iterative development**—Breaking down the project into smaller iterations, often called sprints, with each iteration delivering a working and potentially shippable product increment.
- **Self-organizing teams**—Cross-functional teams collaborate closely, make decisions collectively and have the autonomy to organize their work and choose the best approaches to achieve project goals.
- **Continuous feedback**—Regularly gathering feedback from customers and stakeholders to inform the development process, adapt plans and make improvements.
- **Adaptability and flexibility**—Embracing change rather than strictly following a rigid plan. Agile teams are responsive to new requirements, market dynamics and emerging risk, allowing for adjustments during development.
- **Emphasis on simplicity**—Prioritizing simplicity in design and functionality to maximize value and minimize waste. Delivering the most essential features first and incorporating additional features incrementally.

Popular agile frameworks include Scrum, Kanban and Extreme Programming (XP). Scrum, one of the most common, uses time-boxed iterations (sprints), a product backlog and defined roles, such as product owner and scrum master, to manage and guide the development process.

IT Balanced Scorecard

The IT balanced scorecard (BSC)[33] is a management evaluation technique for assessing IT functions and processes (**figure 2.14**). The technique goes beyond the traditional financial evaluation, supplementing it with measures concerning customer (user) satisfaction, internal (operational) processes and the ability to innovate in the future. These additional measures drive the enterprise toward optimal use of IT, aligned with its strategic goals while keeping all evaluation-related perspectives in balance.

[33] Van Grembergen, W.; "The Balanced Scorecard and IT Governance," Conference Paper, January 2000, *https://www.researchgate.net/profile/Wim-Van-Grembergen/publication/221411772_The_balanced_scorecard_and_IT_governance/links/00b49529ef2cd93b96000000/The-balanced-scorecard-and-IT-governance.pdf*

©ISACA. All Rights Reserved.

Figure 2.14—IT Balanced Scorecard



IT Portfolio Management Versus Balanced Scorecard

The greatest advantage of IT portfolio management is its agility in adjusting investments. IT portfolio management allows enterprises to adjust investments based on the built-in feedback mechanism.

By comparison, BSCs emphasize using vision and strategy in any investment decision. With BSC, IT value and control of an operations budget are not the goal. BSCs focus on operationalizing the strategic plan. While BSC and portfolio management include a feedback loop, the BSC loop relates to strategic planning. In contrast, the portfolio loop considers entire program investments.

To apply the BSC to IT, the enterprise starts by understanding and defining each of the four perspectives:

- User orientation reflects the end user's perspective or evaluation of IT.
- Business contribution captures the business value of IT investments.
- Operational excellence describes the IT processes used to develop and deliver IT resources.
- Future orientation represents the human and technology resources that IT needs to deliver future resources.

Next, a multilayered structure (determined by each enterprise) is used in addressing the four perspectives:

- **Mission**
  - Become the preferred supplier of information systems.
  - Deliver economic, effective and efficient IT applications and services.
  - Obtain a reasonable business contribution from IT investments.
  - Develop opportunities to answer future challenges.
- **Strategies**
  - Develop special applications and operations.
  - Develop user partnerships and greater customer services.
  - Provide enhanced service levels and pricing structures.
  - Control IT expenses.
  - Provide business value to IT projects.
  - Provide new business capabilities.
  - Train and educate IT staff and promote excellence.

 ©ISACA. All Rights Reserved.

  - Provide support for research and development.
- **Measures**
  - Provide a balanced set of key performance metrics (KPIs) to guide business-oriented IT decisions.
  - Establish KRIs to serve as an early warning system in case the strategies and objectives are not being met.
  - Document KCIs to monitor the effectiveness of the control environment.
- **Sources**
  - End-user personnel (specific by function)
  - COO
  - Process owners

Using an IT BSC is one of the most effective means to aid the IT strategy committee and management in achieving IT governance through proper IT and business alignment. The objectives are establishing a vehicle for management reporting to the board; fostering consensus among key stakeholders about IT strategic aims; demonstrating the effectiveness and added value; and communicating information related to IT performance, risk and capabilities.

Additional Approaches for Performance Measurement

Benchmarking systematically compares enterprise performance against peers and competitors to learn the best business practices, including quality, logistic efficiency and other metrics.

Business process reengineering (BPR) is the thorough analysis and significant redesign of business processes and management systems to establish a more efficient and effective structure that is responsive to customer expectations and market conditions while yielding material cost savings. BPR typically seeks to radically redesign business processes to achieve dramatic performance improvements, such as cost, quality, service and speed. BPR often involves using IT to automate and streamline processes. An example is a fully automated supply chain using technology to improve visibility, optimize inventory levels and reduce transportation costs.

Root cause analysis is the diagnosis process to establish the origins of events (root causes). When the root causes have been identified, needed controls can be developed to accurately address what led to system failures and deficiencies. Furthermore, root cause analysis enables an enterprise to learn from consequences, typically errors and problems, to avoid repeating undesired actions or results.

Life cycle cost-benefit analysis assesses costs compared to outcomes to determine a strategic direction for IT enterprise systems and overall IT portfolio management. The elements for analysis include the following:

- **Life cycle (LC)**—A series of stages that characterize the course of existence of an enterprise investment (e.g., product, project, program)
- **Life cycle cost (LCC)**—The estimated costs of maintenance/updates, failure and maintaining interoperability with mainstream and emerging technologies
- **Benefit analysis (BA)**—The user costs (or benefits) and business operational costs (or benefits) derived from the information system(s)

2.11 Quality Assurance and Quality Management of IT

The integrity and reliability of enterprise IT processes are directly attributed to QA processes in place and integrated within the enterprise. The QA program and respective policies, procedures and processes are encompassed within a planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements.

The IS auditor must understand QA and quality management concepts, structures and enterprise roles and responsibilities.

2.11.1 Quality Assurance

QA personnel verify that system changes are authorized, tested and implemented in a controlled manner before being introduced into the production environment according to the enterprise's change release management policies. With tools like source code management software, personnel also oversee the proper segregation of developer access to production environments, maintenance of program versions and source code integrity.

The terms quality assurance and quality control are often used interchangeably to refer to ways of ensuring the quality of a service or product. The terms, however, do have different meanings:

- **Quality assurance (QA)**—A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. QA helps the IT department ensure personnel follow prescribed quality processes. For example, QA sets up procedures (e.g., ISO 9001-compliant) to facilitate

©ISACA. All Rights Reserved.

the widespread use of quality management/assurance practices.
- **Quality control (QC)**—The observation techniques and activities used to fulfill requirements for quality. QC is responsible for conducting tests or reviews to verify and ensure that software is free from defects and meets user expectations. This can be done at various stages of the development of an application system but must be done before the programs are moved into production. For example, QC helps to ensure that programs and documentation adhere to the standards and naming conventions.

The QA function within an enterprise is in charge of developing, promulgating and maintaining standards for the IT function. It also provides training in QA standards and procedures. The QC group assists by periodically checking the accuracy and authenticity of the input, processing and output of various applications.

To enable the QA function to play an effective role, the QA group should be independent within the enterprise. This function may be a part of the larger control entity in some enterprises. In smaller enterprises, having a separate QA function may not be possible, in which case, individuals may possess more than one role. However, under no circumstances should an individual review their own work. Additionally, the review should not be performed by an individual whose role would create a SoD conflict (e.g., a DBA performing a quality review of application system changes that would impact the database).

2.11.2 Quality Management

Quality management is how IT department processes are controlled, measured and improved. Processes in this context are defined as a set of tasks that, when properly performed, produce the desired results. Areas of control for quality management may include:
- Software development, maintenance and implementation
- Acquisition of hardware and software
- Day-to-day operations
- IT control performance
- Service management
- Security
- HR management
- General administration

The IT department development and maintenance of defined and documented processes are evidence of effective governance of information resources. Insistence in the observance of processes and related process management techniques is key to the effectiveness and efficiency of the IT organization. Various standards have emerged to assist IT organizations in achieving these results. Quality standards are increasingly being used to assist IT organizations in achieving an operational environment that is predictable, measurable, repeatable and certified for their IT resources.

2.11.3 Operational Excellence

Operational excellence teams are responsible for improving the efficiency and effectiveness of the enterprise's operations. They identify and eliminate waste, streamline processes and improve communication and collaboration. Operational excellence teams also may use data and analytics to identify areas for improvement.

The specific responsibilities of an operational excellence team will vary depending on the industry and the focus area of the team. However, some common responsibilities of operational excellence teams include:
- Developing and implementing best practices
- Providing training and support to other employees
- Conducting research and development
- Managing knowledge and information
- Serving as a resource for other employees and stakeholders

Operational excellence teams can play a vital role in helping enterprises to improve their performance and achieve their goals. By developing and implementing best practices, operational excellence teams can help enterprises to improve their efficiency, reduce costs and improve customer satisfaction.

 ©ISACA. All Rights Reserved.

Case Study

An IS auditor was asked to review the alignment between IT and business goals for Accenco, a small but rapidly growing financial institution. The IS auditor requested information, including goals and objectives for the business and IT. The information that the auditor received was limited to a short, bulleted list of business goals and presentation slides of IT goals that were used in reporting meetings. The IS auditor found in the documentation provided that over the past two years, the risk management committee (composed of senior management) met on only three occasions. No minutes of what was discussed were kept for these meetings. When the IT budget for the upcoming year was compared to the strategic plans for IT, it was noted that several of the initiatives mentioned in the plans for the upcoming year were not included in the budget for that year.

The IS auditor also discovered that Accenco does not have a full-time CIO. The organizational chart of the entity denotes an IS manager reporting to the CFO, who, in turn, reports to the board of directors. The board plays a major role in monitoring IT initiatives in the entity, and the CFO frequently communicates the progress of IT initiatives.

From reviewing the SoD matrix, it is apparent that application programmers must obtain approval from only the DBA to directly access production data. The IS auditor also noted that the application programmers must provide the developed program code to the program librarian, who then migrates it to production. IS audits are carried out by the internal audit department, which reports to the CFO, at the end of every month, as part of the business performance review process. The entity's financial results are reviewed in detail and signed off by the business managers for the correctness of the data contained therein.

1. Which of the following should be of **GREATEST** concern to the IS auditor about Accenco's IT business strategy?

   A. Strategy documents are informal and incomplete.
   B. The risk management committee seldom meets and does not keep minutes.
   C. Budgets do not appear adequate to support future IT investments.
   D. There is no full-time CIO.

2. Which of the following would be the **MOST** significant issue to address related to Accenco's IT business strategy?

   A. The behavior related to the application programmers' access and migration code
   B. The lack of IT policies and procedures
   C. The risk management practices as compared to peer enterprises
   D. The reporting structure for IT

3. Given the circumstances described, what would be of **GREATEST** concern from an IT governance perspective?

   A. The enterprise does not have a full-time CIO.
   B. The enterprise does not have an IT steering committee.
   C. The board of directors plays a major role in monitoring IT initiatives.
   D. The information systems manager reports to the CFO.

4. Given the circumstances described, what would be of **GREATEST** concern from a SoD perspective?

   A. Application programmers must obtain approval only from the DBA for direct-write access to data.
   B. Application programmers must turn over the developed program code to the program librarian for migration to production.
   C. The internal audit department reports to the CFO.
   D. Business performance reviews must be signed off only by the business managers.

©ISACA. All Rights Reserved.

5. Which of the following would **BEST** address data integrity from a mitigating control standpoint?

   A. Application programmers are required to obtain approval from the DBA for direct access to data.
   B. Application programmers must hand over the developed program codes to the program librarian for transfer to production.
   C. The internal audit department reports to the CFO.
   D. Business performance results must be reviewed and signed off by the business managers.

6. In this small enterprise, assume that the CFO performs the CIO role. What should an IS auditor suggest regarding the governance structure?

7. The IS budgeting process should be integrated with business processes and aligned with enterprise budget cycles. What advice would an IS auditor give to the enterprise to ensure that the budget covers all aspects and can be accepted by the board?

8. The internal auditor reports to the CFO, who owns IT initiatives and operations. The reporting relationship inhibits the auditor's independence. What compensating controls can be enabled to improve the audit efforts?

Answers on page 160

Page intentionally left blank

Chapter 2 Answer Key

Case Study

1. **A. IT loses sight of the enterprise direction without explicit strategy documents, making project selection harder and service levels difficult to define. Overall, IT becomes suboptimal in delivery and value realization.**
   B. The failure of the risk management committee to hold regular meetings and produce good documentation implies a lack of good risk governance. Risk follows when setting the business and IT objectives.
   C. Although an inadequate budget for future IT investments raises concern, this is less important than an incomplete strategy.
   D. The lack of a full-time CIO may be a concern, but it is not as important as an incomplete strategy.

2. A. The behavior related to application programmers' access and migration code represents a lack of IT policies and procedures.
   B. The lack of IT policies and procedures makes IT-related work inconsistently delivered. The policy reflects management intentions and norms set by the strategy. The procedures are instrumental to day-to-day IT delivery.
   C. Risk management practices do not have to compare to peer enterprises.
   D. Although the reporting structure for IT is important, it is not as critical as IT policies and procedures.

3. A. Not having a full-time CIO may be a concern but is not as concerning as the information systems manager reporting to the CFO.
   B. The lack of an IT steering committee may cause issues but is not as big a concern as the information systems manager reporting to the CFO.
   C. The board of directors playing a major role in IT initiatives is not a major concern.
   D. The IS manager should ideally report to the board of directors or the CEO to provide sufficient independence. The reporting structure that requires the IS manager to report to the CFO is not desirable and could compromise certain controls.

4. **A. Application programmers should obtain approval from the business owners before accessing data. DBAs are only custodians of the data and should provide only the access authorized by the data owner.**
   B. Although this may be an issue, it is not as big a SoD concern as the DBA approving direct-write access.
   C. The internal audit department reporting to the CFO is not as big a SoD concern as the DBA approving direct-write access.
   D. This is not as big a SoD concern as the DBA approving direct-write access.

5. A. This does not best mitigate tampering with data.
   B. Handing program code to the librarian does not best mitigate tampering with data.
   C. The reporting structure does not mitigate data tampering.
   D. Sign-off on data contained in the financial results by the business managers at the end of the month would detect any significant discrepancies that can result from the tampering of data through inappropriate direct access of the data gained without the approval or knowledge of the business managers.

6. **Possible answer:** The CFO may act as the CIO in a small enterprise. Having the internal control department report to a different executive (e.g., HR or risk management) is better. The governance function should exist to carry out the IT strategy and the IT steering committee direction. SoD should be maximized to the degree possible. Compensating controls, such as supervisory or peer reviews, can be applied to current controls.
7. **Possible answer:** An IT budgeting and investment process should be defined and align with the Accenco enterprise cycles (e.g., fiscal year, quarterly reviews). The financial management process should include budgeting activity that states its budgeting approach, the cost structure following the chart of accounts and the approval chain. The business case process should be used to justify the process and persuade the board to approve it.
8. **Possible answer:** In this case, the internal auditor should seek further assurance (e.g., monitoring of IS controls by tools, benchmarking efforts by the procurement team, *ad hoc* external auditing or senior management review from the board).

 ©ISACA. All Rights Reserved.

Chapter 3

Information Systems Acquisition, Development and Implementation

Overview

Domain 3 Exam Content Outline 162
Learning Objectives/Task Statements 162
Suggested Resources for Further Study 162
Self-Assessment Questions 162
Chapter 3 Answer Key 166

Part A: Information Systems Acquisition and Development

3.1 Project Governance and Management 169
3.2 Business Case and Feasibility Analysis 184
3.3 System Development Methodologies 186
3.4 Control Identification and Design 216

Part B: Information Systems Implementation

3.5 System Readiness and Implementation Testing 225
3.6 Implementation Configuration and Release Management 232
3.7 System Migration, Infrastructure Deployment and Data Conversion 233
3.8 Postimplementation Review 239

Case Study

Case Study 241
Chapter 3 Answer Key 244

©ISACA. All Rights Reserved.

Overview

This chapter on information systems (IS) acquisition, development and implementation provides an overview of key processes and methodologies used by enterprises when creating and changing application systems and infrastructure components.

Domain 3 represents 12 percent of the CISA examination (approximately 18 questions).

Domain 3 Exam Content Outline

Part A: Information Systems Acquisition and Development

1. Project Governance and Management
2. Business Case and Feasibility Analysis
3. System Development Methodologies
4. Control Identification and Design

Part B: Information Systems Implementation

1. System Readiness and Implementation Testing
2. Implementation Configuration and Release Management
3. System Migration, Infrastructure Deployment and Data Conversion
4. Post-implementation Review

Learning Objectives/Task Statements

Within this domain, an IS auditor should be able to:

- Evaluate audit processes as part of quality assurance and improvement programs.
- Evaluate the IT strategy for alignment with the organization's strategies and objectives.
- Evaluate IT resource and project management for alignment with the organization's strategies and objectives.
- Determine whether the organization has defined ownership of IT risk, controls and standards.
- Evaluate whether the business cases related to information systems meet business objectives.
- Evaluate controls at all stages of the information systems development life cycle.
- Evaluate the readiness of information systems for implementation and migration into production.
- Conduct post-implementation reviews of systems to determine whether project deliverables, controls and requirements are met.
- Evaluate whether effective processes are in place to support end users.
- Evaluate the organization's policies and practices related to asset life cycle management.

Suggested Resources for Further Study

Baxter, C.; "IS Audit in Practice: Implementing Emerging Technologies—Agile SDLC Still Works," *ISACA Journal*, vol. 4, 1 July 2022, *https://www.isaca.org/resources/isaca-journal/issues/2022/volume-4/implementing-emerging-technologies*

ISACA, *COBIT Focus Area: DevOps Using COBIT 2019*, USA, 2020

ISACA, *Software Development Certificate Program*, *https://www.isaca.org/credentialing/software-development-fundamentals-certificate*

ISACA, *Systems Development and Project Management Audit Program*, 2009

ISACA, *White Papers*, *https://www.isaca.org/resources/insights-and-expertise/white-papers*

Khan, M.; "Evolving Technology Calls for More Disciplined Approach From Auditors," ISACA Now Blog, 19 October 2017, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/evolving-technology-calls-for-more-disciplined-approach-from-auditors*

Subramanian, S.; B. Swaminathan; "Security Assurance in the SDLC for the Internet of Things," *ISACA Journal*, vol. 3, 1 May 2017, *https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/security-assurance-in-the-sdlc-for-the-internet-of-things*

Self-Assessment Questions

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often, a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Note that these questions are not actual or retired exam items. See section About This Manual at the beginning of this manual for more guidance regarding practice questions.

 ©ISACA. All Rights Reserved.

1. To assist in testing an essential banking system being acquired, an enterprise has provided the vendor with sensitive data from its existing production system. An information systems (IS) auditor's **PRIMARY** concern is that the data should be:

   A. sanitized.
   B. complete.
   C. representative.
   D. current.

2. Which of the following is the **PRIMARY** purpose for conducting parallel testing?

   A. To determine whether the system is cost-effective
   B. To enable comprehensive unit and system testing
   C. To highlight errors in the program interfaces with files
   D. To ensure that the new system meets user requirements

3. When conducting a review of business process reengineering (BPR), an IS auditor finds that an important preventive control has been removed. In this case, the IS auditor should:

   A. inform management of the finding and determine whether management is willing to accept the potential material risk of not having that preventive control.
   B. determine if a detective control has replaced the preventive control during the process, and, if it has not, report the removal of the preventive control.
   C. recommend that this and all control procedures that existed before the process was reengineered be included in the new process.
   D. develop a continuous audit approach to monitor the effects of the removal of the preventive control.

4. Which of the following data validation edits is effective in detecting transposition and transcription errors?

   A. Range check
   B. Check digit
   C. Validity check
   D. Duplicate check

5. Which of the following weaknesses would be considered the **MOST** significant in enterprise resource planning (ERP) software used by a financial enterprise?

   A. Access controls have not been reviewed.
   B. Limited documentation is available.
   C. Two-year-old backup media have not been replaced.
   D. Database backups are performed once a day.

6. When auditing the requirements phase of a software acquisition, an IS auditor should:

   A. assess the reasonability of the project timetable.
   B. assess the vendor's proposed quality processes.
   C. ensure that the best software package is acquired.
   D. review the completeness of the specifications.

7. An enterprise decides to purchase a software package instead of developing it. In such a case, the design and development phases of a traditional system development life cycle (SDLC) are replaced with:

   A. selection and configuration phases.
   B. feasibility and requirements phases.
   C. implementation and testing phases.
   D. nothing, because replacement is not required.

8. User specifications for a software development project using the traditional (waterfall) system development life cycle methodology have not been met. Which of the following areas is the **MOST** likely source of the cause of this issue?

   A. Quality assurance (QA)
   B. Requirements
   C. Development
   D. User training

9. When introducing thin client architecture, which of the following types of risk regarding servers is significantly increased?

   A. Integrity
   B. Concurrency
   C. Confidentiality
   D. Availability

©ISACA. All Rights Reserved.

10. Which of the following is **MOST** commonly associated with an agile development methodology?

A. Reliance on detailed documentation
B. Reliance on strict standard operating procedures
C. Lack of user requirements
D. Heavy reliance on tacit knowledge

Answers on page 166

Page intentionally left blank

Chapter 3 Answer Key

Self-Assessment Questions

1. **A. Test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.**
   B. Although it is important that the data set be complete, the primary concern is that test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.
   C. Although it is important to encompass a representation of the transactional data, the primary concern is that test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.
   D. Although it is important that the data set represent current data being processed, the primary concern is that test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.

2. A. Parallel testing may show that the old system is more cost-effective than the new system, but this is not the primary reason.
   B. Unit and system testing are completed before parallel testing.
   C. Program interfaces with files are tested for errors during system testing.
   D. The purpose of parallel testing is to ensure that the implementation of a new system will meet user requirements.

3. **A. Management should be informed immediately to determine whether they are willing to accept the potential material risk of not having that preventive control in place.**
   B. The existence of a detective control instead of a preventive control usually increases the risk that a material problem may occur.
   C. Often, during business process reengineering (BPR), many nonvalue-added controls are eliminated. This is good, unless the controls increase the business and financial risk.
   D. An IS auditor may want to monitor, or recommend that management monitor, the new process, but this should be done only after management has been informed and accepts the risk of not having the preventive control in place.

4. A. A range check is checking data that match a predetermined range of values.
   B. A check digit is a numeric value that is calculated mathematically and appended to data to ensure that the original data have not been altered (e.g., an incorrect, but valid, value substituted for the original). This control is effective in detecting transposition and transcription errors.
   C. An availability check is programmed checking of the data validity in accordance with predetermined criteria.
   D. In a duplicate check, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

5. **A. A lack of review of access controls in a financial enterprise can have serious consequences given the types of data and assets that can be accessed.**
   B. A lack of documentation may not be as serious as not having properly reviewed access controls.
   C. It may not be possible to retrieve data from two-year-old backup media.
   D. It may be acceptable to the business to perform database backups once a day, depending on the volume of transactions.

6. A. A project timetable normally is not found in a requirements document.
   B. Assessing the vendor quality processes comes after the requirements have been completed.
   C. The decision to purchase a package from a vendor comes after the requirements have been completed.
   D. The purpose of the requirements phase is to specify the functionality of the proposed system; therefore, an information systems (IS) auditor would concentrate on the completeness of the specifications.

7. **A. With a purchased package, the design and development phases of the traditional life cycle are replaced with selection and configuration phases. A proposal from the supplier of packaged systems is requested and evaluated against predefined criteria for selection, before a decision is made to purchase the software. After the software is purchased, it is configured to meet the enterprise's requirements.**
   B. The other phases of the system development life cycle (SDLC), such as feasibility study,

 ©ISACA. All Rights Reserved.

requirements definition, implementation and postimplementation, remain unaltered.
C. The other phases of the SDLC, such as feasibility study, requirements definition, implementation and postimplementation, remain unaltered.
D. In this scenario, the design and development phases of the traditional life cycle are replaceable with selection and configuration phases.

8. A. Quality assurance (QA) has its focus on formal aspects of software development, such as adhering to coding standards or a specific development methodology.
B. To fail at user specifications implies that requirements engineering has been done to describe the users' demands. Otherwise, there would not be a baseline of specifications against which to check.
C. Project management failed to either set up or verify controls that provide for software or software modules under development that adhere to those user specifications.
D. A failure to meet user specifications might show up during user training or acceptance testing but is not the cause.

9. A. Because the other elements do not need to change, the integrity risk is not increased.
B. Because the other elements do not need to change, the concurrency risk is not increased.
C. Because the other elements do not need to change, the confidentiality risk is not increased.
D. The main change when using thin client architecture is making the servers critical to the operation. Therefore, the probability that one of them fails is increased and, as a result, the availability risk is increased.

10. A. Project documentation is generally second to actual functionality for agile development methodology.
B. Strict standard operating procedures would be detrimental to a developer's ability to think creatively and collaboratively.
C. All development methodologies require some form of requirements definition. Agile relies on clear requirements being defined up front.
D. Tacit knowledge (i.e., implicit knowledge gained from experience and difficult to document) is leveraged greatly by agile methods to increase collaboration and creativity of development teams.

©ISACA. All Rights Reserved.

Page intentionally left blank

Part A: Information Systems Acquisition and Development

To provide assurance that enterprise objectives are being met by the management practices of its information systems, the IS auditor needs to understand how an enterprise evaluates, develops, implements, maintains and disposes of its information systems and related components.

Note

A CISA candidate should have a sound understanding of the IS (hardware and software) acquisition, development and implementation process. This understanding should extend beyond a definitional knowledge of terms and concepts and include the ability to identify vulnerabilities and risk and recommend appropriate controls to effectively mitigate risk. A thorough understanding of the phases of project management is also required. In addition, a CISA candidate should have a good understanding of various application systems and architectures and the related processes, risk and controls.

3.1 Project Governance and Management

In any enterprise, several projects typically run concurrently. To identify the relationships among those projects, a common approach is to establish a project portfolio and/or a program management structure. This assists in identifying common objectives for the business organization, identifying and managing risk, and identifying resource connections.

All projects require governance structures, policies and procedures and specific control mechanisms to ensure strategic and tactical alignment with the respective enterprise's goals, objectives and risk management strategy. Without proper governance, all aspects of a project may be compromised. Project governance structures should involve the project and the functional line organization. All governance decisions about the project should be driven through the business case, and there must be periodic review of the benefits achieved.

Effective and efficient project management requires that projects be managed based on hard factors, such as deliverables, quality, costs and deadlines; soft factors, such as team dynamics, conflict resolution, leadership issues, cultural differences and communication; and environmental factors, such as the political and power issues in the sponsoring enterprise, managing the expectations of stakeholders, and the larger ethical and social issues that may surround a project.

In major transformation programs, specialist third parties are engaged to provide technical leadership to embed the technology, underpinning the development and implementation of the technical solution (e.g., SAP and infrastructure as a service [IaaS] solutions). In such instances, it is important to ensure that third-party project teams focus on the alignment of the technical solution to business requirements of the enterprise rather than attempting to force a "one-size-fits-all" technical solution on the enterprise.

Project management structures are dependent on the size and complexity of the enterprise. Accordingly, some roles and responsibilities may be grouped or restructured. Under such circumstances, the role of an IS auditor is to ensure that rules of system development that relate to separation of duties (SoD) and responsibilities, are not compromised.

There are many approaches and standards to project management. Because differences in scope, content and wording are significant among each of these approaches and standards, IS auditors must be familiar with the standard in use in their enterprise prior to involvement in specific projects.

Note

CISA candidates will not be tested on their knowledge of any particular project management approach or standard. However, candidates must understand the basic elements of project management structures, policies and procedures and, more specifically, related controls.

3.1.1 Project Management Practices

Project management is the application of knowledge, skills, tools and techniques to a broad range of activities to achieve a stated objective, such as meeting the defined user requirements, budget and deadlines for an IS project. Project management is a business process in a project-oriented enterprise. The project management process begins with the project charter and ends with the completion of the project. Project management knowledge and practices are best described in terms of their component processes of initiating, planning, executing, controlling, monitoring and closing a project.

The complexity of project management requires careful and explicit design of the project management process. Thus, all design issues applicable for business

©ISACA. All Rights Reserved.

process engineering should be applied for the project management process.

3.1.2 Project Management Structure

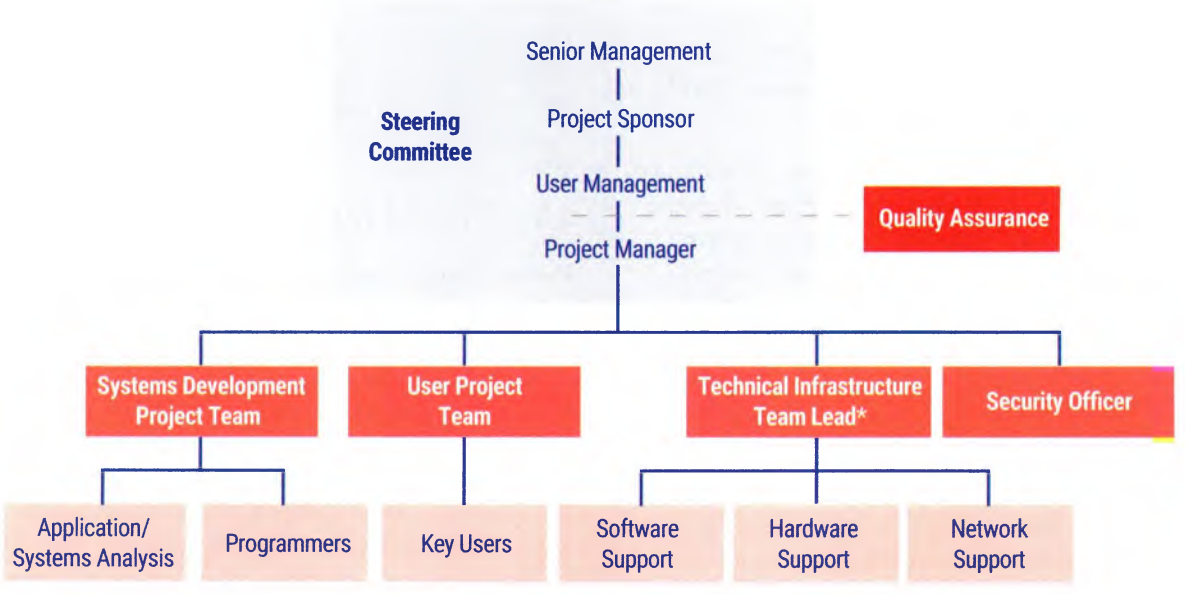
Three types of project management organizational structures outline the authority and control within an enterprise:

1. **Functional-structured organization**—In a functional-structured organization, the project manager does not have formal management authority. The work is broken down into departments and a project manager is allowed to advise peers and team members only about which activities should be completed.
2. **Project-structured organization**—In a project-structured organization, the project manager has formal authority over those taking part in the project. This includes authority over the project's budget, schedule and team.
3. **Matrix-structured project organization**—In a matrix-structured organization, management authority is shared between the project manager and the department heads.

IS projects may be initiated from within any part of the enterprise, including the IT department. An IS project has specific objectives, deliverables and start and end dates. Most IS projects are divisible into explicit phases (e.g., system development life cycle [SDLC]).

Requests for major projects should be submitted to and prioritized by an IT steering committee. The committee then identifies a project manager. The project manager does not need to be an IT staff member and should be given complete operational control over the project and be allocated the appropriate resources, including IT professionals and other staff from user departments, for the successful completion of the project. An IS auditor may be included on the project team as the control expert. The IS auditor may also provide an independent, objective review to ensure that the level of involvement (commitment) of the responsible parties is appropriate. In such cases, the IS auditor is not performing an audit but is participating in the project in an advisory role. Depending on the level of the IS auditor's involvement, they may become ineligible to perform audits of the application when it becomes operational. An example of a project's organizational structure is shown in **figure 3.1**.

Figure 3.1—Project Management, Sample Organization Chart



*Defined as "system development management"

 ©ISACA. All Rights Reserved.

3.1.3 Project Management Roles and Responsibilities

Figure 3.2 shows the various roles and responsibilities of groups/individuals that may be involved in the project management process.

Figure 3.2—Project Management Roles and Responsibilities

Role	Responsibilities
Project steering committee	• Provides overall direction and ensures appropriate representation of the major stakeholders in the project outcome • Is ultimately responsible for all deliverables, project costs and schedules • Includes a senior representative from each business area that will be significantly impacted by the proposed new system or system modification • Requires the project manager to be a member of this committee • Gives authority to each member to make decisions related to system designs that will affect their respective departments • Includes the project sponsor, who assumes overall ownership and accountability of project and chairs the steering committee • Reviews project progress regularly and holds emergency meetings when required • Serves as project coordinator and advisor; therefore, members should be available to answer questions and make user-related decisions about system and program design • Takes corrective action if necessary due to project progress and issues escalated to the committee
Senior management	• Demonstrates commitment to the project, which ensures involvement by those needed to complete the project • Approves necessary resources to complete the project
Project sponsor	• Provides funding for the project • Works closely with the project manager to define the critical success factors and metrics for measuring success of the project • Assumes ownership of data and application • Is typically the senior manager in charge of the primary business unit that the application will support
User management	• Assumes ownership of the project and resulting system • Allocates qualified representatives to the team • Actively participates in business process redesign, system requirements definition, test case development, acceptance testing and user training • Reviews and approves system deliverables as they are defined and implemented
User project team	• Completes assigned tasks • Communicates effectively with the systems developers by actively involving themselves in the development process as subject matter experts • Works according to local standards • Advises the project manager of expected and actual project plan deviations.

©ISACA. All Rights Reserved.

Figure 3.2—Project Management Roles and Responsibilities (cont.)

Role	Responsibilities
Project manager	• Provides day-to-day management and leadership of the project • Ensures that project activities remain in line with the overall direction • Ensures appropriate representation of the affected departments • Ensures that the project adheres to local standards • Ensures that deliverables meet the quality expectations of key stakeholders • Resolves interdepartmental conflicts • Monitors and controls costs and the project timetable • Often facilitates the definition of the project scope, manages the budget and controls the activities via a project schedule • Has a line responsibility for personnel when projects are staffed by personnel dedicated to the project
Quality assurance (QA)	• Reviews results and deliverables within each phase and at the end of each phase and confirms compliance with requirements. The points where reviews occur depend on the: ▪ System development life cycle (SDLC) methodology used ▪ Structure and magnitude of the system ▪ Impact of potential deviations • May review appropriate process-based activities related to either project management or the use of specific software engineering processes within a particular life cycle phase. This is crucial to completing a project on schedule and within budget and in achieving a given software process maturity level. • Has the objective to ensure the quality of the project by measuring the adherence of the project staff to the enterprise SDLC, advise on deviations and propose recommendations for process improvements or greater control points when deviations occur
Systems development management	• Provides technical support for hardware and software environments by developing, installing and operating the requested system • Provides assurance that the system is compatible with the enterprise computing environment and strategic IT direction • Assumes operating support and maintenance activities after installation
Systems development project team	• Completes assigned tasks • Communicates effectively with users by actively involving them in the development process • Works according to local standards • Advises the project manager of necessary project plan deviations
Security officer (or security team)	• Ensures that system controls and supporting processes provide an effective level of protection, based on the data classification set in accordance with enterprise security policies and procedures • Consults throughout the life cycle on appropriate security measures that should be incorporated into the system • Reviews security test plans and reports prior to implementation • Evaluates security-related documents developed for reporting the system security effectiveness for accreditation • Periodically monitors the security system effectiveness during its operational life
Information system security engineer	• Applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risk associated with these vulnerabilities • Defines the needs, requirements, architectures and designs to construct network, platform and application constructs according to the principles of both defense in breadth and security in depth

 ©ISACA. All Rights Reserved.

Figure 3.2—Project Management Roles and Responsibilities (cont.)

Role	Responsibilities
Privacy officer (or privacy team)	• Ensures that applicable data privacy considerations are made to ensure that the rights of data subjects are upheld, by ensuring that proper system controls and supporting processes provide required privacy-related requirements in line with the enterprise privacy program

Note

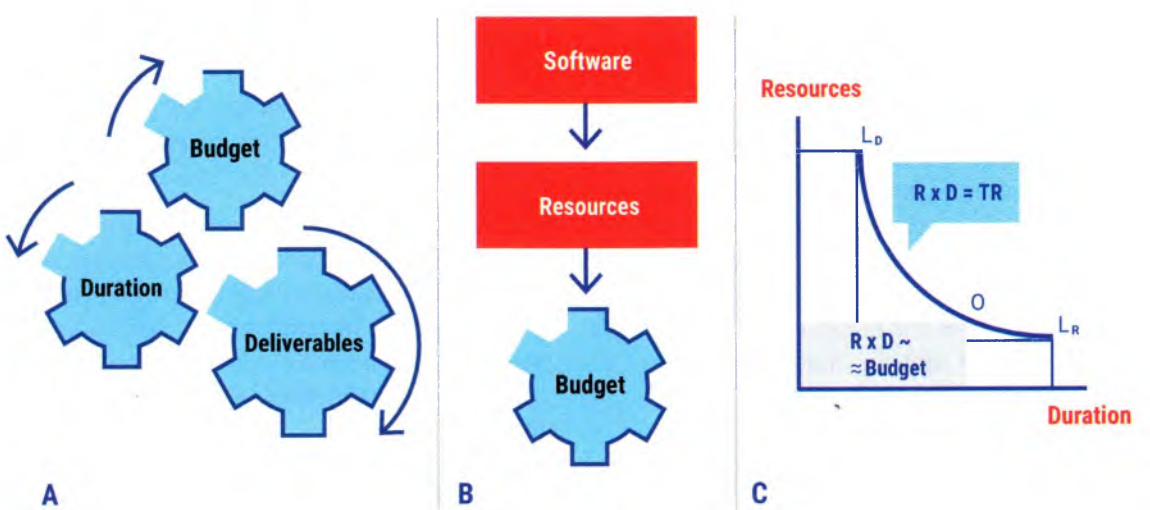
A CISA candidate should be familiar with the general roles and responsibilities of groups or individuals involved in the project management process.

3.1.4 Project Management Techniques

Several project management techniques and tools are available to assist the project manager in controlling the time and resources used in the development of a system and may vary from a simple manual effort to a more elaborate computerized process. The size and complexity of the project may require different approaches. Project management techniques also provide systematic quantitative and qualitative approaches to software size estimating, scheduling, allocating resources and measuring productivity. These tools and techniques typically aid in areas described in later sections in this chapter.

Various elements of a project should always be considered before selecting a technique. Their relationships are shown in **figure 3.3**.

Figure 3.3—Relationships Between Project Management Elements



Source: Personas & Técnicas Multimedia SL, 2009. All rights reserved. Used with permission.

Project management should pay attention to three key intertwining elements: deliverables, duration and budget (**figure 3.3**A). Their relationship is very complex but is shown in an oversimplified and schematized manner in the figure. Project duration and budget must be commensurate with the nature and characteristics of the deliverables. In general, there will be a positive correlation between highly demanding deliverables, a long duration and a high budget.

Budget is determined (**figure 3.3**B) from the resources required to carry out the project by multiplying fees or costs by the amount of each resource. Resources required by the project are estimated at the beginning of the project using software/project size-estimation techniques.

Size estimation yields a total-resources calculation. Project management decides on the resources allocated at any particular moment in time. In general, it is convenient to assign an almost fixed number of resources, aiming to minimize costs (direct and administration). **Figure 3.3**C assumes that there is a fixed number of resources during the entire project. The curve shows resources assigned (R) × duration (D) = total resources (TR, a constant quantity), which is the classic man × month dilemma curve. Any point along the curve meets the condition R × D = TR. At any point O on the curve, the area of the rectangle will be TR, proportional to the budget. If few resources are used, the project will take a long time (a point close to LR); if many resources are used, the project will take a shorter time (a point close to LD). LR and LD are two practical limits—a duration that is too long may not seem possible; use of too many (human) resources at once would be unmanageable.

3.1.5 Portfolio/Program Management

A project portfolio is defined as all of the projects being carried out in an enterprise at a given point in time. A program is a group of projects and tasks that are closely linked together through common strategies, objectives, budgets and schedules. Portfolios, programs and projects are often controlled by a project management office (PMO), which governs the processes of project management but is not typically involved in the management of the content. Like projects, programs have a limited time frame (i.e., a defined start and end date) and organizational boundaries. A differentiator is that programs are more complex; usually have a longer duration, a higher budget and higher risk associated with them; and are of higher strategic importance.

A typical IS-related program may be the implementation of a large-scale enterprise resource planning (ERP) system that includes projects that address technology infrastructure, cloud considerations, operations, organizational realignment, business process reengineering (BPR) and optimization, training, and development. Mergers and acquisitions (M&As) may serve as an example of a non-IS-related program that impacts the gaining and/or divesting enterprises' IS architectures and systems, organizational structure, and business processes.

The objective of program management is the successful execution of programs, including the management of program:

- Scope, financials (costs, resources, cash flow, etc.), schedules, objectives and deliverables
- Context and environment
- Communication and culture
- Organization

To make autonomous projects possible while making use of synergies between related projects in the program, a specific program organization is required. Typical program roles are:

- Program owner
- Program manager
- Program team

The program owner role is distinct from the project owner role. Typical communication structures in a program are program-owner's meetings and program-team's meetings. Methodology and processes used in program management are very similar to those in project management and run in parallel to each other. However, they must not be combined and must be handled and carried out separately. To formally start a program, some form of written assignment from the program sponsor (owner) to the program manager and the program team is required. Because programs most often emerge from projects, such an assignment is of paramount importance to set the program context, boundaries and formal management authority. In contrast to program management, in which all relevant projects are closely coupled, this is not a requirement in a project portfolio. Projects of a program belong to an enterprise's project portfolio, as do projects that are not associated with a program.

To manage portfolios, programs and projects, an enterprise requires specific and well-designed structures, such as expert pools, a PMO and project portfolio groups. Specific integrative tools, such as project management guidelines, standard project plans and project management marketing instruments, are also used.

3.1.6 Project Management Office

The PMO, as an owner of the project management and program management process, must be a permanent structure and adequately staffed to provide professional support in these areas to maintain current, and develop new, procedures and standards. The objective of the PMO is to improve project and program management quality and secure project success, but it can focus only on activities and tasks and not on project or program content.

An IS auditor should be able to differentiate between auditing project content and procedural aspects of a

program or project. The objectives of project portfolio management are:

- Optimization of the results of the project portfolio (not of the individual projects)
- Prioritizing and scheduling projects
- Resource coordination (internal and external)
- Knowledge transfer throughout the projects

Project Portfolio Database

A project portfolio database is mandatory for project portfolio management. It must include project data, such as owner, schedules, objectives, project type, status and cost. Project portfolio management requires specific project portfolio reports. Typical project portfolio reports are a project portfolio bar chart, a profit-versus-risk matrix and a project portfolio progress graph.

Example

1. An enterprise is migrating from legacy applications to an ERP system and has the strategic goal of delivering cutting-edge computers and maintaining high cash flow to continue to fund research and development. To do so, the enterprise is using its:
   a. Internal pool of application developers to code its strategic business process of the manufacture of newly designed computers to deliver finished goods and sales-order-to-cash-receipts, considering the sensitivity of its business model.
   b. Vendors to code the nonstrategic business processes of procure to pay and financial accounting.
2. The enterprise is also pursuing a program for outsourcing transactional processes to a third-party service provider for online sales and a payment portal.

In this context, activities A.1, A.2 and B, individually, are projects. Activities A.1 and A.2 represent a single program, because they are part of the single larger activity of migrating from legacy applications to ERP, and activity B is part of another larger program to outsource noncore manufacturing processes. Activities A.1, A.2 and B (assuming these are the only activities underway in the entity) represent the portfolio for the entity.

3.1.7 Project Benefits Realization

The objective of benefits realization is to ensure that IT and the enterprise fulfill their value management responsibilities, particularly that:

- IT-enabled business investments achieve the promised benefits and deliver measurable business value.
- Required capabilities (solutions and services) are delivered:
  - On time, with respect to schedule and time-sensitive market, industry and regulatory requirements.
  - Within budget.
- IT services and other IT assets continue to contribute to business value.

See chapter 2 Governance and Management of IT for more details on benefits realization.

For projects, a planned approach to benefits realization is required, looking beyond project cycles to longer-term cycles that consider the total business benefits and total business costs throughout the life of the new system. Benefits rarely come about exactly like envisioned in plans. An enterprise has to keep checking and adjusting strategies. Key elements of project benefits realization are:

- Describing benefits management or benefits realization
- Assigning a measure and target
- Establishing a tracking/measuring regimen
- Documenting the assumption
- Establishing key responsibilities for realization
- Validating the benefits predicted in the enterprise
- Planning the benefit that is to be realized

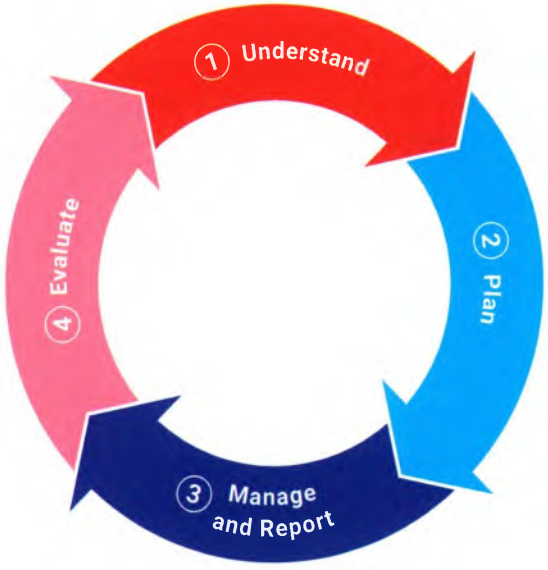
Generally, benefits realization at the project level encompasses four phases, as shown in **figure 3.4**.

Project benefits realization is a compromise among major factors, such as cost, quality, development/delivery time, reliability and dependability. Strategy makers perform a comprehensive study, evaluate which factors are qualifying or winning, and then compare those factors with strengths, weaknesses and competencies of services available to complete and maintain systems. Most large enterprises employ structured project management principles to support changes to their IS environment.

As a starting point, an IS auditor should understand how the enterprise defines value or a return on investment (ROI) for development-related projects. If an enterprise fails to consistently meet its ROI objectives, this may suggest weakness in its SDLC and related project management practices.

©ISACA. All Rights Reserved.

Figure 3.4—Four Phases of Benefits Realization



Source: State of New South Wales, *Benefits Realisation Management Framework: Part 3: Guidelines*, Australia, 2018, *https://www.nsw.gov.au/sites/default/files/2020-11/brmf%20guidelines.pdf*. Used with permission from © State of New South Wales. For current information, go to *www.nsw.gov.au*.

Example

An enterprise is planning to invest in an application that will enable customers to manage their orders online. The following is relevant for the ROI calculation:

1. Business costs
   a. Cost of developing the online application
   b. Cost of controls to ensure integrity of data at rest and in process, while ensuring nonrepudiation
2. Business benefits
   a. Increase in operating profits attributable to expected spike in business driven by customer satisfaction (percent of revenue)
   b. Reduction in operating costs (in terms of dedicated personnel who previously interacted with customers and executed changes)

ROI may be measured as value of benefit over costs, which then can be compared with the enterprise cost of funds, to make a go/no-go decision. This ROI framework can then be used as a benchmark to evaluate the progress of the project and identify causes, if the actual ROI is not aligning with the planned ROI.

Project benefits realization is a continuous process that must be managed just like any business process. Assessment of the benefits realization processes with the business case should be a key element of benefits realization processes. Benefits realization often includes a postimplementation review after the implementation of systems. Time must be allowed for initial technical problems to be resolved and for the project benefits to accrue as users become familiar with the new processes and procedures. Project benefits realization must be part of the governance and management of a project and include business sponsorship.

3.1.8 Project Initiation

A project is initiated by a project manager or sponsor gathering the information required to gain approval for the project to be created. This is often compiled into terms of reference or a project charter that states the objective of the project, the stakeholders of the new system, the project manager and sponsor. Approval of a project initiation document (PID) or a project request document (PRD) is the authorization for a project to begin. Depending on the size and complexity of the project and the affected parties, the initiation of a project may be achieved by:

- **One-on-one meetings**—One-on-one meetings and a project start workshop help to facilitate two-way communication between the project team members and the project manager.
- **Kick-off meetings**—A kick-off meeting may be used by a project manager to inform the team of what must be done for the project. Communications involving significant project events should be documented as part of the project artifacts (i.e., project charter meeting, kick-off meeting, gate reviews, stakeholder meetings, etc.).
- **Project start workshops**—A preferred method to ensure that communication is open and clear among the project team members is to use a project start workshop to obtain cooperation from all team members and buy-in from stakeholders. This helps develop a common overview of the project and communicates the project culture early in the project.
- **A combination of the three**—An enterprise may choose to use two or more of these methods to initiate a project.

3.1.9 Project Objectives

Project objectives are the specific action statements that support attainment of project goals. All project goals will have one or more objectives identified as the actions

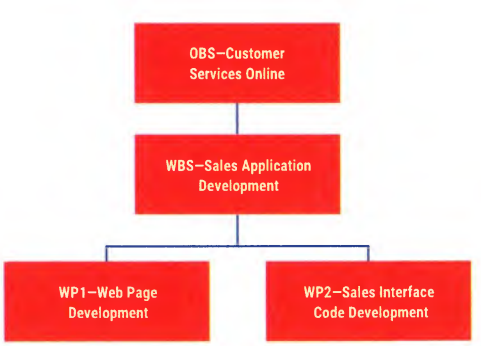
needed to reach that goal. The project objective is the means to meet the project goal.

A project must have clearly defined results that are specific, measurable, attainable, realistic and timely (SMART). A commonly accepted approach to define project objectives is to start off with an object breakdown structure (OBS). It represents the individual components of the solution and their relationships to each other in a hierarchical manner, either graphically or in a table. An OBS can help, especially when dealing with intangible project results, such as organizational enterprise development, to ensure that a material deliverable is not overlooked.

After the OBS has been compiled or a solution is defined, a work breakdown structure (WBS) is designed to structure all the tasks that are necessary to build up the elements of the OBS during the project. The WBS represents the project in terms of manageable and controllable units of work, serves as a central communications tool in the project and forms the baseline for cost and resource planning.

In contrast to the OBS, the WBS does not include basic elements of the solution to build but shows individual work packages (WPs) instead. The structuring of the WBS is process-oriented and in phases. The level of detail of the WBS serves as the basis for the negotiations of detailed objectives among the project sponsor, project manager and project team members. **Figure 3.5** shows an example of this process.

Figure 3.5—Defining Project Objectives



Detailed specifications regarding the WBS can be found in WPs. Each WP must have a distinct owner and a list of main objectives and may have a list of additional objectives and out-of-scope objectives. The WP specifications should include dependencies on other WPs and a definition of how to evaluate performance and goal achievement. An example of a WBS is shown in **figure 3.6**.

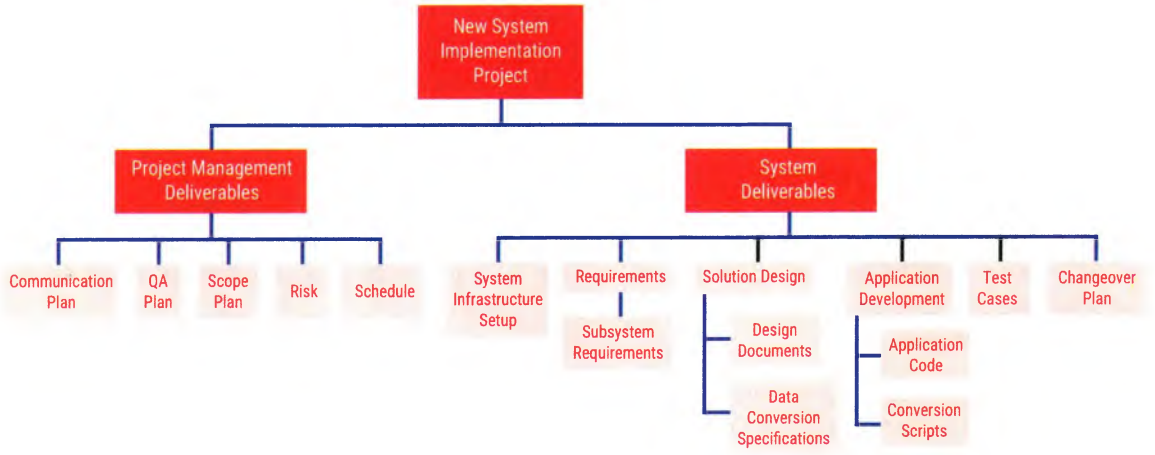
Key things to remember with WBS and respective WPs include the following:

- The top WBS level represents the final deliverable or project.
- Subdeliverables contain WPs that are assigned to an enterprise's department or unit.
- All elements of the WBS do not need to be defined to the same level.
- WPs define the work, duration and costs for the tasks required to produce the subdeliverable.
- WPs should not exceed a duration of 10 days.
- WPs need to be independent of each other in the WBS.
- WPs are unique and should not be duplicated across the WBS.

To support communications, task lists are often used. A task list is a list of actions to be carried out in relation to WPs and includes assigned responsibilities and deadlines. The task list aids the individual project team members in operational planning and in making agreements. These task lists are typically compiled into a project schedule at the planning phase of a project and are used in the controlling phase of the project to monitor and track the progress and completion of the WPs. Project schedules are living documents and should indicate the tasks for a WP, the start and finish dates, percentage completed, task dependencies and the names of individuals scheduled to work on those tasks. A project schedule will also indicate the stage boundaries explained in section 3.2 Business Case and Feasibility Analysis.

©ISACA. All Rights Reserved.

Figure 3.6—Sample Work Breakdown



3.1.10 Project Planning

A project must be planned and controlled. A project manager should determine the following:

- Scope of the project (with agreement from stakeholders)
- Various tasks that need to be performed to produce the expected business application system
- Sequence or order in which these tasks need to be performed
- Duration or time window for each task
- Priority of each task
- IT and non-IT supporting resources that are available and required to perform these tasks
- Budget or cost for each of these tasks
- Source and means of funding for labor, services, materials, and plant and equipment resources involved in the project

Several different sizing and measurement techniques are described in the sections that follow.

Information System Development Project Cost Estimation

Normally relatively large in scope and size, an IS development project focuses on a more complete and integrated solution (hardware, software, facilities, services, etc.). Therefore, these types of projects require much greater planning regarding estimating and budgeting.

Four commonly used methodologies to estimate the cost of an IS acquisition and development project are:

- **Analogous estimating**—By using estimates from prior projects, the project manager can develop the estimated cost for a new project. This is the quickest estimation technique.
- **Parametric estimating**—The project manager looks at the same past data that were used in analogous estimating and leverages statistical data (estimated employee hours, material costs, technology, etc.) to develop the estimate. This approach is more accurate than analogous estimation.
- **Bottom-up estimating**—In this method, the cost of each activity in the project is estimated to the greatest detail (i.e., starting at the bottom), and then all the costs are added to arrive at the cost estimate of the entire project. Although the most accurate estimate, this is the most time-consuming approach.
- **Actual costs**—Like analogous estimation, this approach takes an extrapolation from the actual costs that were incurred on the same system during past projects.

Software Size Estimation

Software size estimation relates to methods of determining the relative physical size of the application software to be developed. Estimates can be used to guide the allocation of resources, judge the time and cost required for its development, and compare the total effort required by the resources.

Traditionally, software sizing has been performed using single-point estimations (based on a single parameter), such as source lines of code (SLOC). For complex systems, single-point estimation techniques have not worked because they do not support more than one parameter in different types of programs, which, in turn, affects the cost, schedule and quality metrics. To

overcome this limitation, multiple-point estimations have been designed.

Current technologies now take the form of more abstract representations, such as diagrams, objects, spreadsheet cells, database queries and graphical user interface (GUI) widgets. These technologies are more closely related to functionality deliverables than to work or lines that need to be created.

Function Point Analysis

The function point analysis (FPA) technique is a multiple-point technique used for estimating complexity in developing large business applications.

The results of FPA are a measure of the size of an IS based on the number and complexity of the inputs, outputs, files, interfaces and queries with which a user sees and interacts. This is an indirect measure of software size and the process by which it is developed versus direct size-oriented measures, such as SLOC counts.

Function points (FPs) are computed by first completing a table (**figure 3.7**) to determine whether a particular entry is simple, average or complex. Five FP count values are defined, including the number of user inputs, user outputs, user inquiries, files and external interfaces.

Note

Enterprises that use function point (FP) methods develop criteria for determining whether a particular entry is simple, average or complex.

After the FP count values are entered in the table, the count total in deriving the function point is computed through an algorithm that considers complexity adjustment values (i.e., rating factors) based on responses to questions related to issues such as reliability, criticality, complexity, reusability, changeability and portability. FPs derived from this equation are then used in a manner analogous to SLOC counts as a measure for cost, schedule, productivity and quality metrics (e.g., productivity = FP/person-month, quality = defects/FP and cost = $/FP).

FPA is an indirect measurement of the software size.

Note

The CISA candidate should be familiar with the use of FPA; however, the CISA exam does not test the specifics on how to perform an FPA calculation.

FPA behaves reasonably well in estimating business applications but not as well for other types of software (such as operating systems [OSs], process control, communications and engineering). Other estimation methods are more appropriate for such software (e.g., the constructive cost model [COCOMO]).

Figure 3.7—Computing Function Point Metrics

Measurement Parameter	Count	Weighting Factor			
		Simple	Average	Complex	Results
Number of user inputs		□ 3	4	6	=____
Number of user outputs		□ 4	5	7	=____
Number of user inquiries		□ 3	4	6	=____
Number of files		□ 7	10	15	=____
Number of external interfaces		□ 5	7	10	=____
Count total:					

©ISACA. All Rights Reserved.

Cost Budgets

A system development project should be analyzed to estimate the amount of effort that will be required to carry out each task. The estimates for each task should contain some or all of the following elements:

- Personnel hours by type (e.g., system analyst, programmer, clerical)
- Machine hours (predominantly computer time, but also duplication facilities, office equipment and communication equipment)
- Other external costs, such as third-party software, licensing of tools for the project, consultant or contractor fees, training costs, certification costs (if required), and occupation costs (if extra space is required for the project)

Having established a best estimate of expected work efforts by task (i.e., actual hours, minimum/maximum) for personnel, costs budgeting now becomes a two-step process to achieve the following results:

1. Obtain a phase-by-phase estimate of human and machine effort by summing the expected effort for the tasks within each phase.
2. Multiply the effort expressed in hours by the appropriate hourly rate to obtain a phase-by-phase estimate of systems development expenditure.

Other costs may require tenders or quotes.

Software Cost Estimation

Cost estimation is a result of software size estimation and helps to properly scope a project. Automated techniques for cost estimation of projects at each phase of IS development are available. To use these products, an IS is usually divided into main components, and a set of cost drivers is established. Components include:

- Source code language
- Execution time constraints
- Main storage constraints
- Data storage constraints
- Computer access
- Target machine used for development
- Security environment
- Staff experience

After all the drivers are defined, the program will develop cost estimates of the IS and total project.

Scheduling and Establishing the Time Frame

While budgeting involves totaling the human and machine effort involved in each task, scheduling involves establishing the sequential relationship among tasks. This is achieved by arranging tasks according to the following two elements:

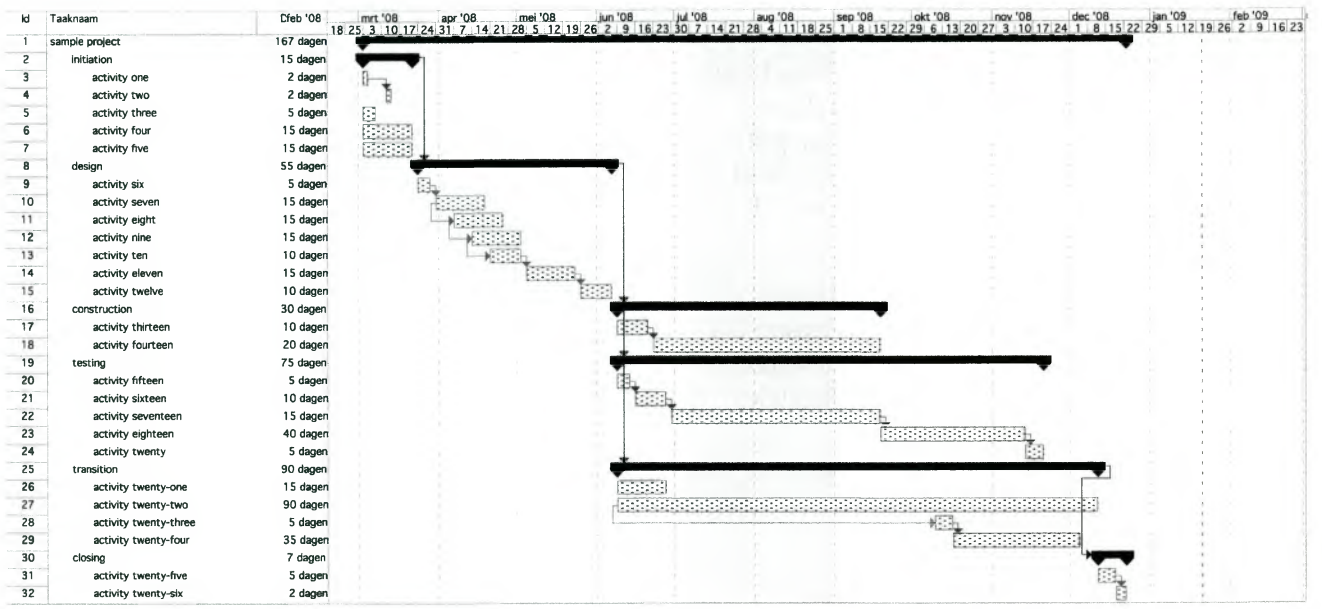
- Earliest start date, by considering the logical sequential relationship among tasks and attempting to perform tasks in parallel, wherever possible
- Latest expected finish date, by considering the estimate of hours per the budget and the expected availability of personnel or other resources, and allowing for known, elapsed-time considerations (e.g., holidays, recruitment time, full-time/part-time employees)

The schedule can be graphically represented using various techniques, such as Gantt charts, the critical path method (CPM), or program evaluation and review technique (PERT) diagrams. During the project execution, the budget and schedule should be revisited to verify compliance and identify variances at key points and milestones. Any variances to the budget and schedule should be analyzed to determine the cause and corrective action to take in minimizing or eliminating the total project variance. Variances and the variance analysis should be reported to management on a timely basis.

Gantt Charts

Gantt charts (**figure 3.8**) aid in scheduling the activities (tasks) needed to complete a project. The charts show when an activity should begin and when it should end along a timeline. The charts also show which activities can occur concurrently and which activities must be completed sequentially. Gantt charts also can reflect the resources assigned to each task and by what percent allocation, and aid in identifying activities that have been completed early or late by comparison to a baseline. Progress of the entire project can be ascertained to determine whether the project is behind, ahead or on schedule compared to the baseline project plan. Gantt charts can also be used to track the achievement of milestones or significant accomplishments for the project, such as the end of a project phase or completion of a key deliverable.

Figure 3.8—Sample Gantt Chart



Critical Path Methodology

The critical path is the sequence of activities that produces the longest path through a project. All project schedules have (at least) one critical path, usually only one in nonmanipulated project schedules. Critical paths are important because, if everything goes according to schedule, they help estimate the shortest possible completion time for the overall project. Activities that are not in the critical path have slack time, which is the difference between the latest possible completion time of each activity that will not delay the completion of the overall project and the earliest possible completion time based on all predecessor activities. Activities on a critical path have zero slack time. By working through the network forwards and backwards, the earliest possible completion times for the activities and the project are determined.

All project schedules have a critical path. Because the activities of a project are ordered and independent, a project can be represented as a network in which activities are shown as branches connected at nodes immediately preceding and immediately following activities. A path through the network is any set of successive activities that go from the beginning to the end of the project. A single number that best estimates the amount of time that an activity will consume is associated with each activity in the network.

Most CPM packages facilitate the analysis of resource utilization per time unit (e.g., day, week) and resource leveling, which is a way to level off resource peaks and valleys. Resource peaks and valleys are expensive due to management, hiring, firing, and/or overtime, and idle resource costs. A constant base resource utilization is preferable. There are few, if any, scientific (algorithmic) resource-leveling methods available, but there is a battery (which CPM packages offer) of efficient heuristic methods that yield satisfactory results.

Program Evaluation Review Technique

PERT is a CPM-type technique that uses three estimates of each activity duration. The three estimates are reduced to a single number (by applying a mathematical formula), and then the classic CPM algorithm is applied. PERT is often used in system development projects with uncertain durations (e.g., pharmaceutical research or complex software development).

A diagram illustrating the use of the PERT network management technique is shown in **figure 3.9**, in which events are points in time or milestones for starting and completing activities (arrows). To determine a task's completion, three estimates are shown for completing each activity. The first is the best-case (optimistic) scenario and the third is the worst-case (pessimistic) scenario.

The second estimate is the most likely scenario. This estimate is based on experience attained from projects similar in size and scope.

©ISACA. All Rights Reserved.

To calculate the PERT time estimate for each given activity, the following calculation is applied:

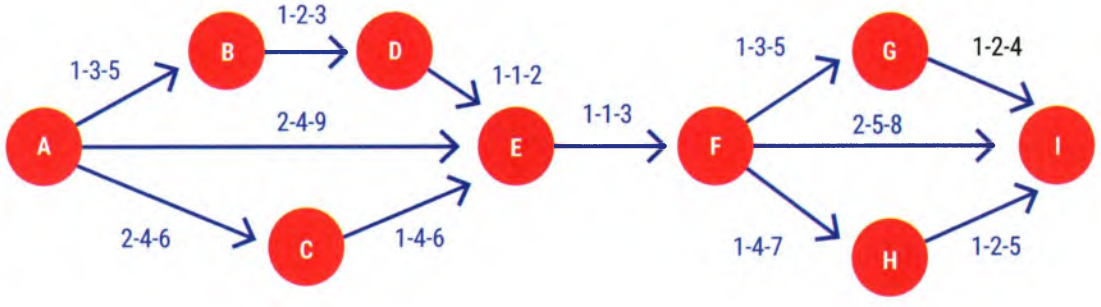
[Optimistic + Pessimistic + 4(most likely)]/6

Using PERT, a critical path is also derived. The critical path is the longest path through the network; there is only one critical path in a network. The critical path is the route along which the project can be shortened (accelerated) or lengthened (delayed). In **figure 3.9**, the critical path is A, C, E, F, H and I.

The advantage of PERT over CPM in the example provided is that the formula is based on the reasonable assumption that the three-time estimates follow a beta statistical distribution and, accordingly, probabilities (with associated confidence levels) can be associated with the total project duration.

When designing a PERT network for system development projects, the first step is to identify all the activities and related events/milestones of the project and their relative sequence. For example, an event or result may be the completion of the operational feasibility study or the point at which the user accepts the detailed design. The analyst must be careful not to overlook any activity. Additionally, some activities such as analysis and design must be preceded by others before program coding can begin. The list of activities determines the detail of the PERT network. The analyst may prepare many diagrams that provide increasingly detailed time estimates.

Figure 3.9—PERT Network-Based Chart



Timebox Management

Timebox management is a project management technique for defining and deploying software deliverables within a relatively short and fixed time period and with predetermined specific resources. There is a need to balance software quality and meet the delivery requirements within the timebox. Timebox management can be used to accomplish prototyping or rapid application development (RAD)-type approaches in which key features are to be delivered in a short time frame. Key features include interfaces for future integrations. The major advantage of this approach is that it prevents project cost overruns and delays from scheduled delivery. The project does not necessarily eliminate the need for a quality process. The design and development phase is shortened due to the use of newer developmental tools and techniques. The preparation of test cases and testing requirements are easily documented as a result of end-user participation. System test and user acceptance testing (UAT) are normally performed together.

3.1.11 Project Execution

After planning efforts have been completed, the program manager, in coordination with the PMO, starts the actual project execution of the planned tasks as described in the plans, processes and procedures. The program and project management team initiates monitoring of internal team production and quality metrics and monitors these metrics from contractors and vendors. A key success factor is the project's oversight of the integrated team in the IT system requirements, architecture, design, development, testing, implementation and transitioning to production operations.

 ©ISACA. All Rights Reserved.

3.1.12 Project Controlling and Monitoring

The controlling and monitoring activities of a project include management of scope, resource usage and risk. It is important that new requirements for the project be documented and, if approved, allocated appropriate resources. Control of change during a project ensures that projects are completed within stakeholder requirements of time, use of funds and quality objectives. Stakeholder satisfaction should be addressed with effective and accurate requirements capture, proper documentation, baselining and skilled steering committee activity.

To monitor and measure the development effort, metrics are required. The first step is to identify resources (e.g., people with requisite skills, development tools, facilities) for IS and software development. This will help in estimating and budgeting system and software development resources.

Management of Scope Changes

Managing the scope of projects requires careful documentation in the form of a WBS. This documentation forms part of the project plan or the project baseline. Changes to the scope almost invariably lead to changes in required activities and impact deadlines and budget. Therefore, it is necessary to have a change management process, including a formal change request submitted to the project manager. Only stakeholders are allowed to submit change requests. Copies of all change requests should be archived in the project file. The project manager judges the impact of each change request on project activities (scope), schedule and budget. The change advisory board then evaluates the change request (on behalf of the sponsor) and decides whether to recommend the change. If the change is accepted, the project manager is instructed to update the project plan to reflect the requested change. The updated project plan must be formally confirmed by the project sponsor—accepting or rejecting the recommendation of the change advisory board.

Management of Resource Usage

Resource usage is the process by which the project budget is being spent. To determine whether actual spending is in line with planned spending, resource usage must be measured and reported. In addition to spending, productivity must be monitored to determine if resource allocation is on task. Whether this is happening can be checked with a technique called earned value analysis (EVA).

EVA consists of comparing the metrics at regular intervals during the project, such as:

- Budget to date
- Actual spending to date
- Estimate to complete
- Estimate at completion

For example, if a single-task project is planned to take three working days, with eight hours spent each day, the resource will have spent eight hours after the first day, with 16 hours remaining. To know if the project is on track, the employee should be asked how much additional time is required to complete the task. If the answer exceeds 16, the project is overrun and not on track.

Management of Risk

Risk is defined as an uncertain event or condition that would impact relevant aspects of the project. There are two main categories of project risk: the category that impacts the business benefits (and, therefore, endangers the reasons for the project's existence) and the category that impacts the project itself. The project sponsor is responsible for mitigating the first category of risk and the project manager is responsible for mitigating the second category.

See chapter 2 Governance and Management of IT for more information.

3.1.13 Project Closing

A project has a finite life, so, at some point, it must be closed, and a new or modified system will be handed over to the users and/or system support staff. At this point, any outstanding issues will need to be assigned. The project sponsor should be satisfied that the system produced is acceptable and ready for delivery.

Key questions to consider include:

- When will the project manager issue the final project closure notification?
- Who will issue the final project notification?
- How will the project manager help the project team transition to new projects or release them to their regular assigned duties?
- What will the project manager do for actions, risk and issues that remain open? Who will pick up these actions and how will these be funded?

Hand-off of relevant documentation and duties will occur at this stage, and the project team and other relevant stakeholders will identify lessons learned from the project.

©ISACA. All Rights Reserved.

Review may be a formal process, such as a post project review. A postimplementation review, in contrast, is typically completed after the project has been in use (or in production) for some time—long enough to realize its business benefits and costs and measure the project overall success and impact on the business units. Metrics used to quantify the value of the project include total cost of ownership (TCO) and ROI.

3.1.14 IS Auditor's Role in Project Management

To achieve a successful project outcome, the audit function should play an active role, where appropriate, in the life cycle development of a new system or business application. This will facilitate efforts to ensure that proper controls are designed and implemented in the new system (e.g., continuous concurrent controls for paperless ecommerce systems). An IS auditor needs to understand the system or application being developed to identify potential vulnerabilities and points requiring control. If controls are lacking or the process is disorderly, it is an IS auditor's role to advise the project team and senior management of the deficiencies. It may also be necessary to advise those engaged in IS acquisition and development activities of appropriate controls or processes to implement and follow.

An IS auditor's role may take place during the project or on completion. Tasks generally include the following:

- Meet with key systems development and user project team members to determine the main components, objectives and user requirements of the system to identify the areas that require controls.
- Discuss the selection of appropriate controls with systems development and user project team members to determine and rank the major risk to and exposures of the system.
- Discuss references to authoritative sources with systems development and user project team members to identify controls to mitigate the risk to and exposures of the system.
- Evaluate available controls and participate in discussions with systems development and user project team members to advise the project team regarding the design of the system and implementation of controls.
- Periodically meet with systems development and user project team members and review the documentation and deliverables to monitor the systems development process to ensure that controls are implemented, user and business requirements are met and the systems development/acquisition methodology is being followed. Review and evaluate application system audit trails to ensure that documented controls are in place to address all security, edit and processing controls. Tracking information in a change management system includes:
  - History of all work order activity (date of work order, programmer assigned, changes made and date closed)
  - History of logons and logoffs by programmers
  - History of program deletions
  - Adequacy of SoD and quality assurance (QA) activities
- Identify and test existing controls to determine the adequacy of production library security to ensure the integrity of the production resources.
- Review and analyze test plans to determine if defined system requirements are being verified.
- Analyze test results and other audit evidence to evaluate the system maintenance process to determine whether control objectives were achieved.
- Review appropriate documentation, discuss with key personnel and use observation to evaluate system maintenance standards and procedures to ensure their adequacy.
- Discuss and examine supporting records to test system maintenance procedures to ensure that they are being applied as described in the standards.
- Participate in postimplementation reviews.

3.2 Business Case and Feasibility Analysis

A business case provides the information required for an enterprise to decide whether a project should proceed. Depending on the enterprise and the size of the investment, the development of a business case is either the first step in a project or a precursor to the start of a project. A business case should adequately describe the business reasons or benefits for a project and be of sufficient detail to describe the justification for initiating and continuing a project. It should answer the question: Why should this project be undertaken and/or continued? A business case should be a key element of the decision process throughout the life cycle of any project. If, at any stage, the business case is thought to no longer be valid, the project sponsor or IT steering committee should consider whether the project should proceed. In a well-planned project, there will be decision points, often called stage gates or kill points, at which a business case is formally reviewed to ensure that it is still valid. If the business case changes during an IT project, the project should be reapproved through the departmental planning and approval process.

 ©ISACA. All Rights Reserved.

After the initial approval has been given to move forward with a project, an analysis begins to clearly define the need and identify alternatives for addressing the need. This analysis is known as the feasibility study. An initial business case would normally derive from a feasibility study undertaken as part of the project initiation/planning. This is an early study of a problem to assess if a solution is practical and meets requirements within established budgets and schedule requirements. A feasibility study will normally include the following six elements:

1. **Project scope**—Definition of the business problem and/or opportunity to be addressed. It should be clear, concise and to the point.
2. **Current analysis**—Definition and establishment of an understanding of a system, a software product, etc. Based on this analysis, it may be determined that the current system or software product is working correctly, some minor modifications are needed, or a complete upgrade or replacement is required. At this point in the process, the strengths and weaknesses of the current system or software product are identified.
3. **Requirements**—Definition of project requirements based on stakeholder needs and constraints. Defining requirements for software differs from defining requirements for systems. The following are examples of needs and constraints used to define requirements:
   a. Business, contractual and regulatory processes
   b. End-user functional needs
   c. Technical and physical attributes defining operational and engineering parameters
4. **Approach**—Definition of a course of action to satisfy the requirements for a recommended system and/or software solution. This step clearly identifies the alternatives that were considered and the rationale for why the preferred solution was selected. This is the process wherein the use of existing structures and commercial alternatives are considered (e.g., build-versus-buy decisions).
5. **Evaluation**—Examination of the cost-effectiveness of the project based on the previously completed elements within the feasibility study. The final report addresses the cost-effectiveness of the approach selected. Elements of the final report include:
   a. The estimated total cost of the project if the preferred solution is selected, and the alternates to provide a cost comparison, including:
      1. Estimate of employee hours required to complete
      2. Material and facility costs
      3. Vendors and third-party contractors' costs
   b. Project schedule start and end dates
   c. A cost and evaluation summary encompassing cost-benefit analysis, ROI, etc.
6. **Review**—Reviews (formal) of the previously completed elements of the feasibility study to validate the completeness and accuracy of the feasibility study and render a decision to either approve or reject the project or ask for corrections before making a final decision. The review and report are conducted with all key stakeholders. If the feasibility study is approved, all key stakeholders sign the document. Rationale for rejection of the feasibility study should be explained and attached to the document as part of a lessons learned list for use in future project studies.

3.2.1 IS Auditor's Role in Business Case Development

An IS auditor should understand how a business defines business cases used during feasibility studies and resultant determinations regarding ROI for IS development-related projects. If an enterprise fails to consistently meet its ROI objectives, this may suggest weaknesses in its system development approach and related project management practices.

An IS auditor plays an important role in the review and evaluation of a feasibility study. This is to ensure that the process and decisions were made in an effective and unbiased manner. The following are tasks typically performed by an IS auditor when reviewing a feasibility study:

- Review and evaluate the criticality of the business and IS process requirements.
- Determine if a solution can be achieved with the systems already in place. If not, review the evaluation of alternative solutions for reasonableness.
- Determine the reasonableness of the chosen solution based on their strengths and weaknesses.
- Determine whether all cost justifications/benefits are verifiable and reflect anticipated costs and benefits to be realized.
- Review the documentation produced for reasonableness.

As it applies to the requirements definition within a feasibility study, an IS auditor should perform the following functions:

- Obtain the detailed requirements definition document and verify its accuracy and completeness through interviews with the relevant user departments.
- Identify the key team members on the project team and verify that all affected user groups have/had appropriate representation.

©ISACA. All Rights Reserved.

- Verify that project initiation and cost have received proper management approval.
- Review the conceptual design specifications (e.g., transforms, data descriptions) to ensure that they address the needs of the user.
- Review the conceptual design to ensure that control specifications have been defined.
- Determine whether a reasonable number of vendors received a proposal covering the project scope and user requirements.
- Review the UAT specifications.
- Determine whether the application is a candidate for the use of an embedded audit routine. If so, request that the routine be incorporated in the conceptual design of the system.

3.3 System Development Methodologies

A systems development methodology is a structure that an enterprise uses to plan and control the development of IS, software and new business applications. Facing increasing system complexity and the need to implement new systems more quickly to achieve benefits before the business changes, system and software development practitioners adopted many ways of organizing IS and software projects.

3.3.1 Business Application Development

Business application development is part of a life cycle process with defined phases applicable to deployment, maintenance and retirement. In this process, each phase is an incremental step that lays the foundation for the next phase, which ensures effective management control in building and operating business application systems.

A developed business application system is one of two major types:

- **Organization-centric**—The objective of organization-centric applications is to collect, collate, store, archive and share information with business users and various applicable support functions on a need-to-know basis. Thus, sales data are made available to accounts, administration, governmental levy payment departments, etc. Regulatory levy fulfillment (i.e., tax compliance) is also addressed by the presence of organization-centric applications. Organization-centric application projects usually use the SDLC or other, more detailed software engineering approaches for development.
- **End-user-centric**—The objective of an end-user-centric application is to provide different views of data for their performance optimization. This objective includes decision support systems (DSSs) and geographic information systems (GISs). Most of these applications are developed using alternative development approaches.

A business application development project is generally initiated by one or more of the following situations:

- New opportunity that relates to a new or existing business process
- Problem that relates to an existing business process
- New opportunity that will enable the enterprise to take advantage of technology
- Problem with the current technology
- Alignment of business applications with business partners/industry standard systems and respective interfaces

All these situations are tightly coupled with key business drivers, which are the attributes of a business function that drive the behavior and implementation of that business function to achieve the strategic business goals. Thus, all critical business objectives (from the enterprise strategy) have to be translated into key business drivers for all parties involved in business operations during a systems development project. Objectives should be SMART (see section 3.5.9 Project Objectives) so that general requirements will be expressed in a scorecard form, which allows objective evidence to be collected to measure the business value of an application and to prioritize requirements. A key benefit of this approach is that all affected parties will have a common and clear understanding of the objectives and how they contribute to enterprise support. Additionally, conflicting key business drivers (e.g., cost versus functionality) and mutually dependent key business drivers can be detected and resolved in early stages of the project.

Business application projects should be initiated using well-defined procedures or activities as part of a defined process to communicate business needs to management. These procedures often require detailed documentation identifying the need or problem, specifying the desired solution and relating the potential benefits to an enterprise. All internal and external factors affected by the problem and their effect on an enterprise should be identified.

3.3.2 SDLC Models

Several different SDLC models exist, including:

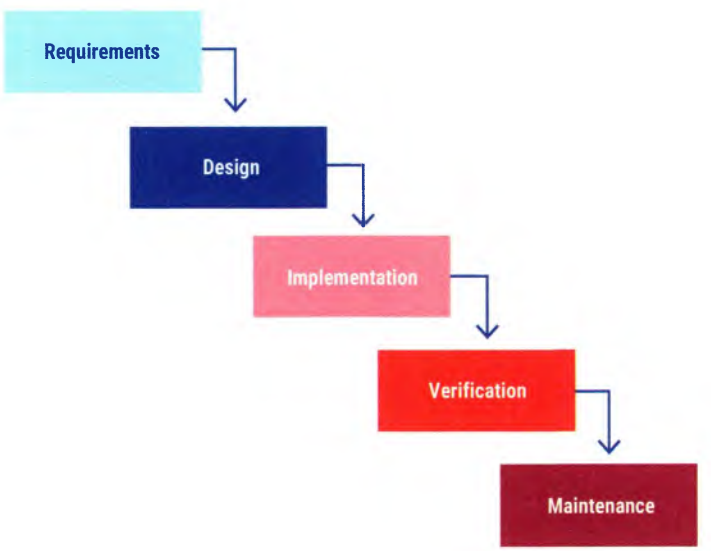
- Traditional waterfall
- V-shaped
- Iterative

The traditional SDLC waterfall model and variants of the model normally involve a life cycle verification approach

 ©ISACA. All Rights Reserved.

that ensures that potential mistakes are corrected early and not solely during final acceptance testing. This life cycle approach is the oldest and most commonly used model for developing business applications. This approach works best when project requirements are likely to be stable and well defined. It facilitates the determination of a system architecture relatively early in the development effort. The approach is based on a systematic, sequential approach to system and/or software development (**figure 3.10**). The traditional approach is useful in web applications in which prototypes of screens are necessary to aid in the completion of requirements and design.

Figure 3.10—Waterfall SDLC Model



The primary advantage of the waterfall approach is that it provides a template into which methods for the requirements (i.e., definition, design, programming, etc.) can be placed. However, some of the problems encountered with this approach include:

- Unanticipated events that result in iterations, creating problems in implementing the approach
- Difficulty obtaining an explicit set of requirements from the customer/user, which the approach requires
- Managing requirements and convincing the user about the undue or unwarranted requirements in the system functionality, which may lead to conflict in the project
- The necessity of customer/user patience, which is required because, with this approach, a working version of the system's programs will not be available until late in the project's life cycle
- A changing business environment that alters or changes the customer/user requirements before they are delivered

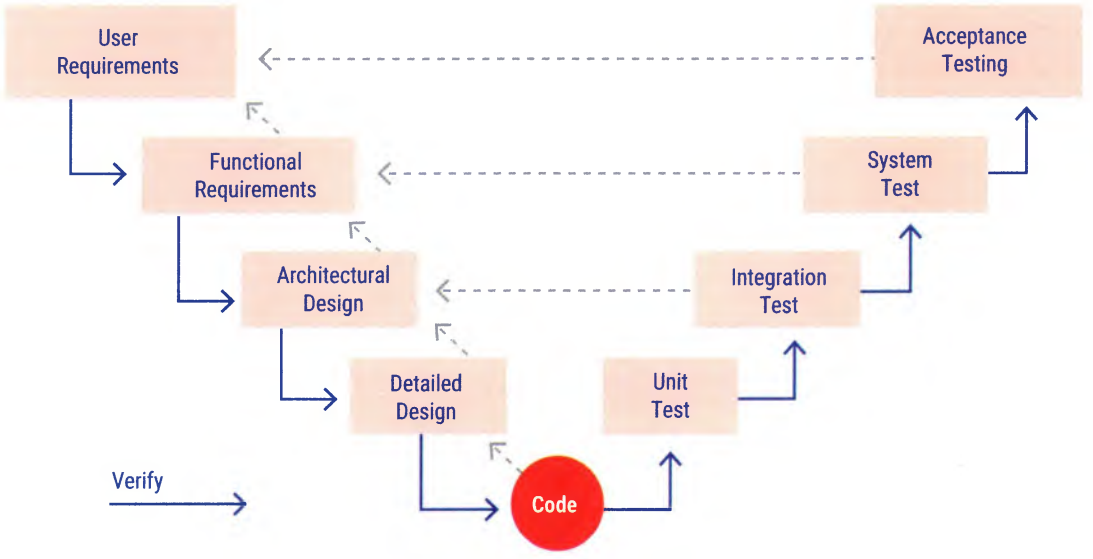
A verification and validation model, also called the V-model or V-shaped model, also emphasizes the relationship between development phases and testing levels (**figure 3.11**). The most granular testing—the unit test—occurs immediately after programs have been written. Following this model, testing validates the detailed design. System testing relates to the architectural specification of the system while final UAT references the requirements.

The V-shaped model provides many advantages, particularly for smaller projects. This is a highly disciplined model with strict phases and verification and validation activities throughout the development life cycle. This emphasis on discipline and testing can give greater assurance that user requirements are met and security is maintained during development. However, some of the problems encountered with this approach include the following:

- The inflexibility of the V-model may make it hard to leverage for complex projects or projects with a high-probability of change to occur during development.
- Concurrent events or development dependencies may cause delays to the overall development timeline.
- An overreliance on documentation may lead to less time being spent on development.

©ISACA. All Rights Reserved.

Figure 3.11—Verification and Validation



The iterative model is a cyclical process in which business requirements are developed and tested in iterations until the entire application is designed, built and tested. During each iteration, the development process goes through each phase, from requirements through testing, and each subsequent cycle incrementally improves the process, as shown in **figure 3.12**. This model is suitable for large projects and allows for independent features to be delivered to users periodically. However, some of the problems encountered with this approach include the following:

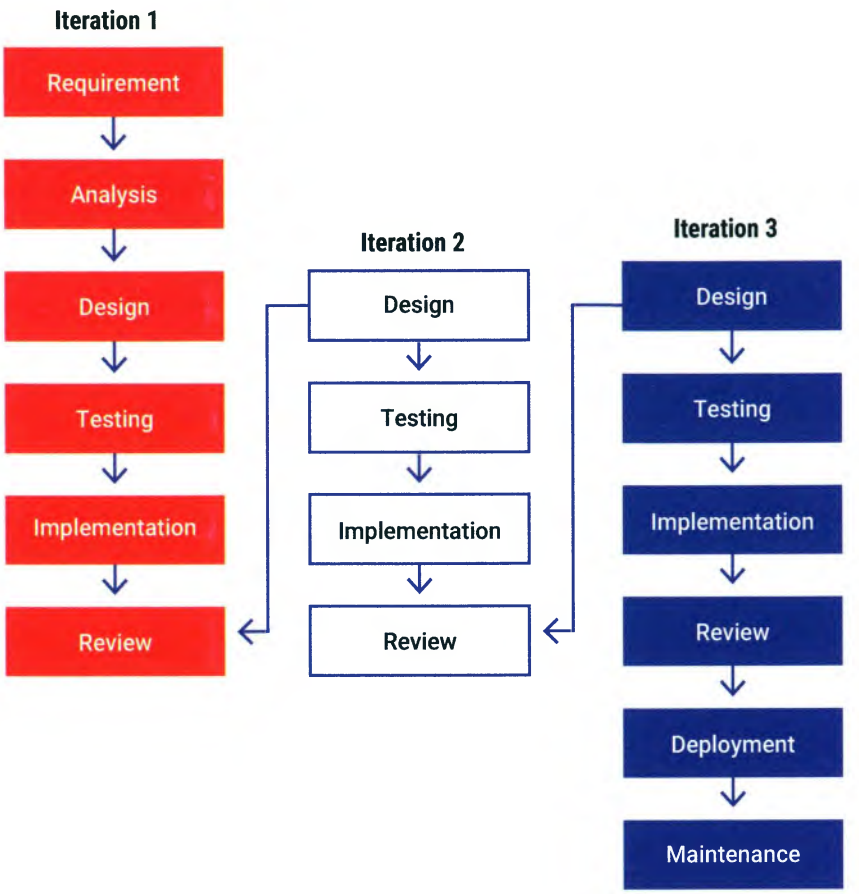
- Additional and more complex project management may be required.
- Risk analysis is required more often and likely by an efficient and highly qualified resource.
- Overall project completion date may be ambiguous.

Note

A CISA candidate should understand systems development models and how they are used to evaluate the existence and effectiveness of critical system development controls. A CISA candidate should also understand how a selected methodology is used and whether the process will properly address the project requirements.

 ©ISACA. All Rights Reserved.

Figure 3.12—Iterative Model



3.3.3 SDLC Phases

The SDLC approach has six phases (**figure 3.13**), each with a defined set of activities and outcomes. Each phase has defined goals and activities to perform with assigned responsibilities, expected outcomes and target completion dates. Other interpretations may use a slightly different number of phases with different names.

Figure 3.13—Traditional System Development Life Cycle (SDLC) Approach

SDLC Phase	General Description
Phase 1—Feasibility Study	Determine the strategic benefits of implementing the system either in productivity gains or in future cost avoidance, identify and quantify the cost savings of a new system and estimate a payback schedule for costs incurred in implementing the system. Further, consider and assess intangible factors, such as readiness of the business users and maturity of the business processes. This business case provides the justification for proceeding to the next phase.
Phase 2—Requirements Definition	Define the problem or need that requires resolution and the functional and quality requirements of the solution system. This can be either a customized approach or vendor-supplied software package, which entails following a defined and documented acquisition process. In either case, the user needs to be actively involved.

©ISACA. All Rights Reserved.

Figure 3.13—Traditional System Development Life Cycle (SDLC) Approach (cont.)

SDLC Phase	General Description
Phase 3A—Software Selection and Acquisition (purchased systems)	Based on requirements defined, prepare a request for proposal (RFP) outlining the entity requirements to invite bids from prospective suppliers for systems that are intended to be procured from vendors or solution providers.
Phase 3B—Design (in-house development)	Based on the requirements defined, establish a baseline of system and subsystem specifications that describe the parts of the system, how they interface and how the system will be implemented using the chosen hardware, software and network facilities. Generally, the design also includes program and database specifications and will address any security considerations. Additionally, establish a formal change control process to prevent uncontrolled entry of new requirements into the development process.
Phase 4A—Configuration (purchased systems)	If it is a packaged system, configure the system to tailor it to the enterprise's requirements. This is best done through the configuration of system control parameters rather than changing program code. Software packages are extremely flexible, making it possible for one package to suit many enterprises simply by switching functionality on or off and setting parameters in tables. There may be a need to build interface programs that will connect the acquired system with existing programs and databases.
Phase 4B—Development (in-house development)	Use the design specifications to begin programming and formalizing supporting operational processes of the system. Conduct various levels of testing in this phase to verify and validate what has been developed. This generally includes all unit and system testing and several iterations of user acceptance testing (UAT).
Phase 5—Final Testing and Implementation	Establish the actual operation of the new information system, with the final iteration of UAT and user sign-off. Also in this phase, the system may go through a certification and accreditation process to assess the effectiveness of the business application in mitigating risk to an appropriate level and providing management accountability over the effectiveness of the system to meet its intended objectives and to establish an appropriate level of internal control.
Phase 6—Postimplementation	Following the successful implementation of a new or extensively modified system, implement a formal process that assesses the adequacy of the system and projected cost-benefit or return on investment (ROI) measurements from the feasibility stage findings and deviations. In so doing, IS project and end-user management can provide lessons learned and/or plans for addressing system deficiencies, and recommendations for future projects regarding system development and project management processes followed.

The actual phases for each project may vary depending on whether a developed or acquired solution is chosen. For example, system maintenance efforts may not require the same level of detail or number of phases as new applications. The phases and deliverables should be decided during the early planning stages of the project.

Over the years, business application development has occurred largely using traditional SDLC phases. As purchased packages have become more common, the design and development phases of the traditional life cycle are being replaced with selection and configuration phases.

The following subsections describe each phase, its purpose and relationship to prior phases, the general activities performed and expected outcomes.

Phase 1—Feasibility Study

A feasibility study is concerned with analyzing the benefits and solutions for the identified problem area. This study develops a business case that states the strategic benefits of implementing the system either in productivity gains or in future cost avoidance, identifies and quantifies the cost savings of the new system, and estimates a payback schedule for the cost incurred in implementing the system or shows the projected ROI.

Intangible benefits, such as improved morale, may also be identified; however, benefits should be quantified whenever possible.

A feasibility study achieves the following:

- Defines a time frame for the implementation of the required solution

 ©ISACA. All Rights Reserved.

- Determines an optimum alternative risk-based solution for meeting business needs and general information resource requirements (e.g., whether to develop or acquire a system). Such processes can easily be mapped to SDLC and RAD.
- Determines whether an existing system can correct the situation with slight or no modification (e.g., workaround)
- Determines whether a vendor product offers a solution to the problem
- Determines the approximate cost to develop the system to correct the situation
- Determines whether the solution fits the business strategy

Factors impacting whether to develop or acquire a system include the following:

- Date the system needs to be functional
- Cost to develop the system as opposed to buying it
- Resources, staff (availability and skill sets) and hardware required to develop the system or implement a vendor solution
- In a vendor system, the license characteristics (e.g., yearly renewal or perpetual) and maintenance costs
- Other systems that need to supply information to or use information from the vendor system and will need the ability to interface with the system
- Compatibility with strategic business plans
- Compatibility with risk appetite and regulatory compliance needs
- Compatibility with the enterprise's IT infrastructure
- Likely future requirements for changes to functionality offered by the system
- Expertise in the specific area where the system is intended to add value

The result of the completed feasibility study should be a comparative report that shows the results of criteria analyzed (e.g., costs, benefits, risk, resources required and organizational impact) and recommends one of the alternatives/solutions and a course of action.

Closely related to a feasibility study is the development of an impact assessment. An impact assessment is a study of the potential future effects of a development project on current projects and resources. The resulting document should list the advantages and limitations of pursuing a specific course of action.

Phase 2—Requirements Definition

Requirements definition is concerned with identifying and specifying the business requirements of the system chosen for development during the feasibility study. Requirements include descriptions of:

- What a system should do
- How users will interact with a system
- Conditions under which the system will operate
- Information criteria the system should meet

This phase also deals with overarching issues that are sometimes called nonfunctional requirements (e.g., access control). Many IT security and privacy weaknesses can be corrected with a critical focus on security and data privacy within the context of the SDLC, especially during the requirements definition phase.

To successfully complete the requirements definition phase, the project team should perform the following activities:

- Identify and consult stakeholders to determine their requirements.
- Identity any relevant data privacy and governance requirements.
- Analyze requirements to detect and correct conflicts (mainly, differences between requirements and expectations) and determine priorities.
- Identify system boundaries and how the system should interact with its environment.
- Identify any relevant security requirements.
- Convert user requirements into system requirements (e.g., an interactive user interface prototype that demonstrates the screen look and feel).
- Record requirements in a structured format. Historically, requirements have been recorded in a written requirements specification, possibly supplemented by some schematic models. Commercial requirements management tools now are available that allow requirements and related information to be stored in a multiuser database.
- Verify that requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable. Because of the high cost of rectifying requirements' problems in downstream development phases, effective requirements reviews have a large payoff.
- Resolve conflicts between stakeholders.
- Resolve conflicts between the requirements set and the resources that are available.

The users in this process specify their information resource needs and how they wish to have them addressed by the system (e.g., access controls, regulatory

©ISACA. All Rights Reserved.

requirements, management information needs and interface requirements).

From this interactive process, a general preliminary design of the system may be developed and presented to user management for review and approval. A project schedule is created for developing, testing and implementing the system. Also, commitments are obtained from the system's developers and affected user departments to contribute the necessary resources to complete the project. It is important to note that all management and user groups must be actively involved in the requirements definition phase to prevent problems, such as expending resources on a system that will not satisfy the business requirements. User involvement is necessary to obtain commitment and full benefit from the system. Without management sponsorship, clearly defined requirements and user involvement, the benefits may never be realized.

An IS auditor should pay close attention to the degree the enterprise's system security engineering team is involved in the development of security controls throughout the data life cycle within the business application. This means that the controls are in place regarding applicable confidentiality, integrity and availability of data from creation/receipt to processing, storage and, ultimately, destruction. This includes whether adequate audit trails are defined as part of the system because these affect the auditor's ability to identify issues for proper follow-up. The IS auditor may also identify regulatory, statutory and legal requirements for the solution being developed.

Phase 3A—Software Selection and Acquisition

At this point in the project, it may be appropriate to evaluate the risk and benefits of developing a new system versus acquiring from a vendor a suitable system that is complete, tested and proven. Consideration should be given to the ability of the enterprise to undertake the proposed development project, the costs and risk of doing so and the benefits of having total ownership and control over the new system rather than becoming dependent on a vendor. Software acquisition is not a phase in the standard SDLC. However, if a decision is reached to acquire rather than develop software, software acquisition is the process that should occur after the requirements definition phase. The decision is generally based on various factors, such as the cost differential between development and acquisition, availability of generic software and the time gap between development and acquisition. Note that if the result of the decision to develop/acquire is to purchase a vendor-supplied software package, the user must be actively involved in the package evaluation and selection process.

Phase 3B—Design

Based on the general preliminary design and user requirements defined in the requirements definition phase, a detailed design should be developed. Generally, a programming and analysis team is assigned the tasks of defining the software architecture (depicting a general blueprint of the system) and then detailing or decomposing the system into its constituent parts (e.g., modules and components). This approach is an enabler for effective allocation of resources to design the system and define how the system will satisfy all its information requirements. Depending on the complexity of the system, several iterations in defining system-level specifications may be needed to get down to the level of detail necessary to start development activities, such as coding.

Key design phase activities include the following:

- Developing system flowcharts and entity relationship models to illustrate how information will flow through the system
- Determining the use of structured design techniques (i.e., processes to define applications through a series of data or process flow diagrams) that show various relationships from the top level down to the details
- Describing inputs and outputs, such as screen designs and reports. If a prototyping tool is going to be used, it is most often used in the screen design and presentation process (via online programming facilities) as part of an integrated development environment (IDE).
- Determining processing steps and computation rules when addressing functional requirement needs
- Determining data file or database system file design
- Preparing program specifications for various types of requirements or information criteria defined
- Developing test plans for the various levels of testing:
  - Unit (program)
  - Subsystem (module)
  - Integration (system)
  - Interface with other systems
  - Loading and initializing files
  - Stress
  - Security
  - Backup and recovery
- Developing data conversion plans to convert data and manual procedures from the old system to the new system. Detailed conversion plans will alleviate implementation problems that arise due to

incompatible data, insufficient resources or staff who are unfamiliar with the operations of the new system.
- Performing a risk assessment of data flows, including implications of personal data protection regulations where the new system processes and shares personal data with third-party systems.

Risk Associated With Software Development

Many types of risk can occur when designing and developing software systems, including:
- **Strategic risk**—Arises when the business goals are identified and weighted without taking the enterprise strategy into account. The strategic importance of the business goals depends on the strategic importance of the related business area.
- **Business risk (or benefit risk)**—Relates to the likelihood that the new system may not meet the users' business needs, requirements and expectations. For example, the business requirements that were to be addressed by the new system are still unfulfilled, and the process has been a waste of resources. In such a case, even if the system is implemented, it will most likely be underused and not maintained, making it obsolete in a short period of time.
- **Project risk (or delivery risk)**—Arises if the project activities to design and develop the system exceed the limits of the financial resources set aside for the project and, as a result, the project may be completed late or not at all. Software project risk exists at multiple levels:
  - Within the project (e.g., risk associated with not identifying the right requirements to deal with the business problem, or opportunity, that the system is meant to address and not managing the project to deliver within time and cost constraints)
  - With suppliers (e.g., risk associated with a failure to clearly communicate requirements and expectations, resulting in suppliers delivering late, at more than the expected cost and/or with deficient quality)
  - Within the enterprise (e.g., risk associated with stakeholders not providing needed inputs or committing resources to the project and changing enterprise priorities and politics)
  - With the external environment (e.g., risk associated with impacts on the projects caused by the actions and changing preferences of customers, competitors, government/regulators and economic conditions)
  - With the technology chosen (e.g., sudden displacement of the technology that was chosen by a more cost-efficient technology or insufficient compatibility in the marketplace, resulting in barriers to potential clients' use of the new system)

The primary cause of these problems is a lack of discipline in managing the software development process or the use of a methodology inappropriate to the system being developed. In such instances, an enterprise is not providing the infrastructure and support that is necessary to help projects avoid these problems. Therefore, successful projects, if occurring, are not repeatable, and SDLC activities are not defined and followed adequately (i.e., insufficient maturity). However, with effective management, SDLC management activities can be controlled, measured and improved.

An IS auditor should be aware that merely following an SDLC management approach does not ensure the successful completion of a development project. An IS auditor should also review the project management discipline related to the following:
- The project meets cooperative goals and objectives.
- Project planning is performed, including effective estimates of resources, budget and time.
- Scope creep is controlled and there is a software baseline to prevent requirements from being added into the software design or having an uncontrolled development process.
- Management is tracking software design and development activities.
- Senior management support is provided to the software project's design and development efforts.
- Periodic review and risk analysis are performed in each project phase.

Use of Structured Analysis, Design and Development Techniques

The use of structured analysis, design and development techniques is closely associated with the traditional, classic SDLC approach to software development. These techniques provide a framework for identifying and representing the data and process components of an application by using various graphic notations at different levels of abstraction until the abstraction level that enables programmers to code the system is reached. For example, early in a project, the following activities occur in defining the requirements for a new system:
- Develop system context diagrams (e.g., high-level business process flow schema).
- Perform hierarchical data flow/control flow decomposition.
- Develop control transformations.
- Develop minispecifications.
- Develop data dictionaries.

©ISACA. All Rights Reserved.

- Define all external events—inputs from external environment.
- Define single transformation data flow diagrams (DFDs) from each external event.

The next level of design provides greater detail for building the system, including developing system flowcharts, inputs/outputs, processing steps and computations, and program and data file or database specifications. It should be noted that representation of functions is developed in a modularized top-down fashion. This enables programmers to systematically develop and test modules in a linear fashion.

An IS auditor should be particularly concerned with whether the processes under a structured approach are well defined, documented and followed when using the traditional SDLC approach to business application development.

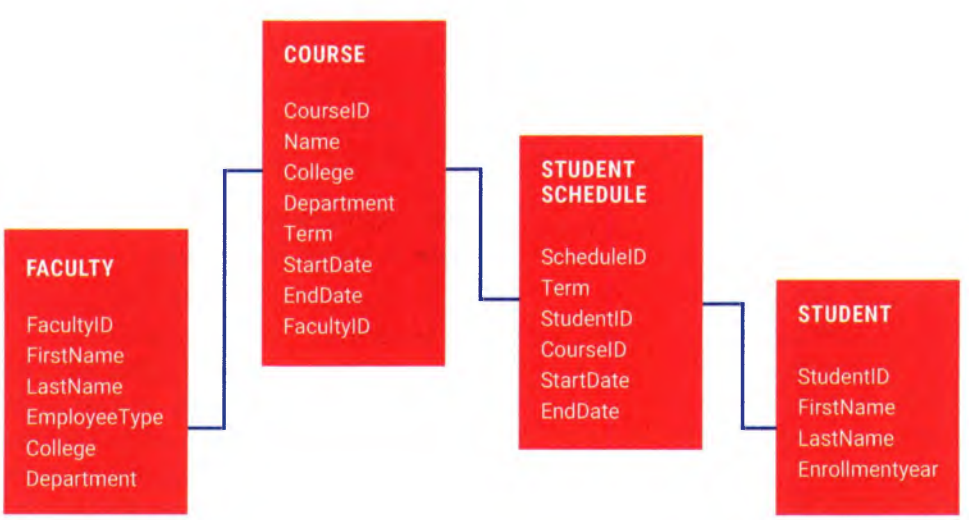
Entity Relationship Diagrams

An important tool in the creation of a general preliminary design is the use of entity relationship diagrams (ERDs). An ERD depicts a system's data and how these data interrelate. An ERD can be used as a requirements analysis tool to obtain an understanding of the data that a system needs to capture and manage. In this case, the ERD represents a logical data model. An ERD can also be used later in the development cycle as a design tool that helps document the actual database schema that will be implemented. Used in this way, the ERD represents a physical data model.

As the name suggests, the essential components of an ERD are entities and relationships. Entities are groupings of like data elements or instances that may represent actual physical objects or logical constructs. An entity is described by attributes, which are properties or characteristics common to all or some of the instances of the entity. Particular attributes, either singularly or in combination, form the keys of an entity. The entity's primary key uniquely identifies each instance of the entity. Entities are represented on ERDs as rectangular boxes with an identifying name.

A sample ERD is shown in **figure 3.14**.

Figure 3.14—Sample Entity Relationship Diagram



Source: ISACA, *Software Development Fundamentals*, USA, 2021

Software Baselining

The software design phase represents the optimum point for software baselining to occur. The term software baseline means the cutoff point in the design and is also referred to as design freeze. User requirements are reviewed, item by item, and considered in terms of time and cost. The changes are undertaken after considering various types of risk, and change does not occur without undergoing formal strict procedures for approval based on a cost-benefit impact analysis. Failure to adequately manage the requirements for a system through baselining

 ©ISACA. All Rights Reserved.

can result in several types of risk. Foremost among these is scope creep—the process through which requirements change during development.

Software baselining also relates to the point when formal establishment of the software configuration management process occurs. At this point, software work products are established as configuration baselines with version numbers. This includes functional requirements, specifications and test plans. All of these work products are configuration items and are identified and brought under formal change management control. This process is used throughout the application-system life cycle, where SDLC procedures for analysis, design, development, testing and deployment are enforced on new requirements or changes to existing requirements.

User Involvement in the Design

After business processes have been documented and it is understood how those processes might be executed in a new system, involvement of users during the design phase is limited.

Given the technical discussion that usually occurs during a design review, end-user participation in the review of detailed design work products is normally not appropriate. However, developers should be able to explain how the software architecture will satisfy system requirements and outline the rationale for key design decisions. Selected hardware and software configurations may have cost implications, of which stakeholders need to be aware, and control implications that are of interest to an IS auditor.

After the detailed design has been completed, including user approvals and software baselining, the design is distributed to the system developers for coding.

IS Auditor's Role in Project Design

The IS auditor is primarily focused on whether an adequate system of controls is incorporated into system specifications and test plans, and whether continuous online auditing functions are built into the system (particularly for ecommerce applications and other types of paperless environments). Additionally, an IS auditor is interested in evaluating the effectiveness of the design process itself (e.g., the use of structured design techniques, prototyping, test plans and software baselining) to establish a formal software change process that effectively freezes the inclusion of any changes to system requirements without a formal review and approval process. The key documents coming out of this phase include system, subsystem, program and database specifications; test plans; and a defined and documented formal software change control process.

An IS auditor should perform the following functions:

- Review the system flowcharts for adherence to the general design.
- Verify that appropriate approvals were obtained for any changes, and all changes were discussed and approved by appropriate user management.
- Review for appropriateness the input, processing and output controls designed into the system.
- Interview the key users of the system to determine their understanding of how the system will operate and assess their level of input into the design of screen formats and output reports.
- Assess the adequacy of audit trails to provide traceability and accountability of system transactions.
- Verify the integrity of key calculations and processes.
- Verify that the system can identify and process erroneous data correctly.
- Review the QA results of the programs developed during this phase.
- Verify that all recommended corrections to programming errors were made and the recommended audit trails or embedded audit modules (EAMs) were coded into the appropriate programs.
- Perform a risk assessment.

Phase 4A—Configuration

System configuration, as it relates to the SDLC, consists of defining, tracking and controlling changes in an acquired system to meet the needs of the business. For ERP systems, the task often involves the modification of configuration tables and some development, primarily to ensure that the ERP system is integrated into the existing IT architecture. Configuration options may be limited or unique depending on the choice of on-premises or cloud-provided infrastructure. System configuration is supported by the change management policies and processes, which define:

- Roles and responsibilities
- Classification and prioritization of all changes based on business risk
- Assessment of impact
- Authorization and approval of all changes by the business process owners and IT
- Tracking and status of changes
- Impact on data integrity (e.g., all changes to data files being made under system and application control rather than by direct user intervention)

©ISACA. All Rights Reserved.

Phase 4B—Development

The development phase uses the detailed design developed in phase 3B. Responsibilities in this phase rest primarily with the programmers and systems analysts who are building the system. Key activities performed in a test/development environment include:

- Coding and developing program and system-level documents
- Debugging and testing the programs developed
- Developing programs to convert data from the old system for use on the new system
- Creating user procedures to handle transition to the new system
- Training selected users on the new system because their participation will be needed
- Ensuring that modifications are documented and applied accurately and completely to vendor-acquired software to ensure that future updated versions of the vendor's code can be applied
- Identifying secure coding and configuration standards to ensure security by design

Programming Methods and Techniques

To enhance the quality of programming activities and future maintenance capabilities, program coding standards should be applied. Program coding standards are essential to writing, reading and understanding code, simply and clearly, without having to refer to design specifications. Elements of program coding standards include methods and techniques for internal (source-code level) documentation, methods for data declaration and an approach to statement construction and techniques for input/output (I/O). The programming standards applied are an essential control because they serve as a method of communicating among members of the program team, and between the team and users during system development. Program coding standards minimize system development setbacks resulting from personnel turnover, provide the material needed to use the system effectively and are required for efficient program maintenance and modifications.

Additionally, traditional structured programming techniques should be applied in developing quality and easily maintained software products. They are a natural progression from the top-down structuring design techniques previously described. Like the design specifications, structured application programs are easier to develop, understand and maintain because they are divided into subsystems, components, modules, programs, subroutines and units. Generally, the greater the extent to which each software item described performs a single, dedicated function (cohesion) and retains independence from other comparable items (coupling), the easier it is to maintain and enhance a system because it is easier to determine where and how to apply a change and reduce the chances of unintended consequences.

Online Programming Facilities (Integrated Development Environment)

To facilitate effective use of structured programming methods and techniques, an online programming facility should be available as part of an IDE. This allows programmers to code and compile programs interactively with a remote computer or server from a terminal or a client's PC workstation. Through this facility, programmers can enter, modify and delete programming codes and compile, store and list programs (source and object) on the development computer. The online facilities can also be used by non-IS staff to update and retrieve data directly from computer files.

Online programming facilities are used on PC workstations. The program library is on a server, such as a mainframe library management system, but the modification/development and testing are performed on the workstation. This approach can lower the development costs, maintain rapid response time and expand the programming resources and aids available (e.g., editing tools, programming languages, debugging aids). From the perspective of control, this approach introduces the potential weaknesses of:

- Proliferation of multiple versions of programs
- Reduced program and processing integrity through the increased potential for unauthorized access and updating
- Possibility that valid changes can be overwritten by other changes

In general, an online programming facility allows faster program development and helps to enforce the use of standards and structured programming techniques. Online systems improve the programmer's problem-solving abilities, but online systems create vulnerabilities resulting from unauthorized access. Access control software should be used to help reduce the risk.

Programming Languages

Application programs must first be coded in statements, instructions or a programming language that is easy for a programmer and can be read by the computer. These statements (source code) are then translated by the language translator/compiler into a binary machine code

 ©ISACA. All Rights Reserved.

or machine language (object code) that the computer can execute.

Programming languages commonly used for developing application programs include the following:

- High-level, general-purpose programming languages, such as Common Business-Oriented Language (COBOL) and the C programming language
- Object-oriented languages for business purposes, such as C++, Eiffel and Java
- IDEs such as Visual Studio or Jbuilder, which provide coding templates automatically
- Web scripting languages (e.g., Hypertext Markup Language [HTML], JavaScript, Cascading Style Sheets [CSS])
- Data-centric programming languages (e.g., R, Scala, Interactive Data Language [IDL], Statistical Analysis System [SAS])
- Scripting languages, such as shell, Perl, Tcl, Python, JavaScript and VBScript. In web development, scripting languages are used commonly to write common gateway interface (CGI) scripts that are used to extend the functionality of web server application software (e.g., to interface with search engines, create dynamic web pages and respond to user input).
- High-level assembler languages designed for a specific processor type that are usually used for embedded applications (e.g., slot machines, vending machines, aerospace devices)
- Fourth-generation, high-level programming languages (4GLs), which consist of a database management system (DBMS), embedded database manager and a nonprocedural report and screen generation facility. 4GLs provide fast iteration through successive designs. Examples of 4GLs include FOCUS, Natural and dBase.
- Decision support or expert systems languages (e.g., EXPRESS, Lisp and Prolog)
- Low code/no code (LCNC) and the implications of removing traditional developers from the development process

Program Debugging

Many programming bugs are detected during the system development process after a programmer runs a program in the test environment. The purpose of debugging programs during system development is to ensure that all program abends (unplanned ending of a program due to programming errors) and program coding flaws are detected and corrected before the final program goes into production. A debugging tool is a program that will assist a programmer in debugging, fixing or fine-tuning the program under development. Compilers have some potential to provide feedback to a programmer, but they are not considered debugging tools. Debugging tools fall into three main categories:

- **Logic path monitors**—Report on the sequence of events performed by the program, thus providing the programmer with clues on logic errors.
- **Memory dumps**—Provide a picture of the internal memory's content at one point in time. This is often produced at the point where the program fails or is aborted, providing the programmer with clues on inconsistencies in data or parameter values. A variant, called a trace, will do the same at different stages in the program execution to show changes in machine-level structures, such as counters and registers.
- **Output analyzers**—Help check results of program execution for accuracy. This is achieved by comparing expected results with the actual results.

Phase 5—Final Testing and Implementation

During the implementation phase, the actual operation of the new IS is established and tested. Final UAT is conducted in this environment. The system may also go through a certification and accreditation process to assess the business application's effectiveness at mitigating risk to an appropriate level and provide management accountability over the effectiveness of the system in meeting its intended objectives and establishing an appropriate level of internal control. This includes applicable security testing (e.g., penetration testing, controls validation).

After a successful full-system test, the system is ready to migrate to the production environment. A date for system migration is determined and production turnover takes place. In the case of large enterprises and complex systems, this may require a separate project and a phased approach.

Planning for the implementation should begin well in advance of the actual implementation date, and a formal implementation plan should be constructed in the design phase and revised accordingly as development progresses. Each step in setting up the production environment should be stipulated, including who will be responsible, how the step will be verified and the backout procedure if problems are experienced. If the new system interfaces with other systems or is distributed across multiple platforms, some final commissioning tests of the production environment may be desirable to prove end-to-end connectivity. If such tests are run, care will be needed to ensure that test transactions do not remain in production databases or files.

©ISACA. All Rights Reserved.

In the case of acquired software, the implementation project should be coordinated by user management with the help of IS management, if required. The total process should not be delegated to the vendor, to avoid possible unauthorized changes or introduction of malicious code by the vendor's employees/representatives.

After operations are established, the next step is to perform site acceptance testing, which is a full-system test conducted on the actual operations environment. UAT supports the process of ensuring that the system is production-ready and satisfies all documented requirements. A security test, such as a penetration test, may also be performed at this stage.

Phase 6—Postimplementation Review

Following the successful implementation of a new or extensively modified system, it is beneficial to verify the system has been properly designed and developed and that proper controls have been built into the system. A postimplementation review should meet the following objectives:

- Assessing the adequacy of the system
  - Does the system meet user requirements and business objectives?
  - Have controls been adequately defined and implemented?
- Evaluating the projected cost benefits or ROI measurements
- Developing recommendations that address the system's inadequacies and deficiencies
- Developing a plan for implementing the recommendations
- Assessing the development project process
  - Were the chosen methodologies, standards and techniques followed?
  - Were appropriate project management techniques used?

3.3.4 IS Auditor's Role in SDLC Project Management

Throughout the project management process, an IS auditor should analyze the associated risk and exposures inherent in each phase of the SDLC and ensure that the appropriate control mechanisms are in place to minimize risk in a cost-effective manner. Caution should be exercised to avoid recommending controls that cost more to administer than the associated risk they are designed to minimize.

When reviewing the SDLC process, an IS auditor should obtain documentation from the various phases and attend project team meetings, offering advice to the project team throughout the system development process. An IS auditor should also assess the project team's ability to produce key deliverables by the promised dates.

Typically, an IS auditor should review the adequacy of the following project management activities:

- Levels of oversight by project committee/board
- Risk management methods within the project
- Issue management
- Cost management
- Processes for planning and dependency management
- Reporting processes to senior management
- Change control processes
- Stakeholder management involvement
- Sign-off process (at a minimum, signed approvals from systems development and user management responsible for the cost of the project and/or use of the system)

Additionally, adequate and complete documentation of all phases of the SDLC process should be evident. Typical types of documentation include:

- Objectives defining what is to be accomplished during each phase
- Key deliverables by phases with project personnel assigned direct responsibilities for these deliverables
- Project schedule with highlighted dates for the completion of key deliverables
- Economic forecast for each phase, defining resources and the cost of the resources required to complete it

3.3.5 Software Development Methods

There are several different methods of designing and developing a software system. The choice of a particular method is driven by considerations such as enterprise policy, developer knowledge and preference, and the technology being used. The selection of a software development method is generally independent of the selection of a project organization model. An object-oriented approach can be used on a project organized into distinct phases, such as a traditional waterfall model of software development or an agile project method in which each short iteration delivers working software.

Prototyping/Evolutionary Development

Prototyping, also known as heuristic or evolutionary development, is the process of quickly putting together a working model (a prototype) to test various aspects of a design, illustrate ideas or features, and gather early user feedback. It enables the developer and customer to understand and react to risk at each

 ©ISACA. All Rights Reserved.

evolutionary level (using prototyping as a risk reduction mechanism). It combines the best features of classic SDLC by maintaining the systematic stepwise approach and incorporates it into an iterative framework that more realistically reflects the real world.

The initial emphasis during the development of the prototype is usually placed on the reports and screens, which are the system aspects most used by the end users. This allows the end user to see a working model of the proposed system within a short time. There are two basic methods or approaches to prototyping:

1. Build the model to create the design (i.e., the mechanism for defining requirements). Then, based on that model, develop the system design with all the performance, quality and maintenance features needed.
2. Gradually build the actual system that will operate in production using a 4GL that has been determined to be appropriate for the system being built.

The problem with the first approach is that there can be considerable pressure to implement an early prototype. Often, users observing a working model cannot understand why the early prototype must be refined further. They often do not understand that the prototype needs to be expanded to handle transaction volumes, client-server network connectivity, and backup and recovery procedures, while providing for security, data privacy, auditability and control.

The second approach typically works with small applications using 4GL tools. However, for larger efforts, it is necessary to develop a design strategy for the system even if a 4GL is used. The use of 4GL techniques alone will cause the same difficulties (e.g., poor quality, poor maintainability and low user acceptance) encountered when developing business applications using conventional approaches.

Another overall disadvantage of prototyping is that it often leads to functions or extras being added to the system that are not included in the initial requirements document. All major enhancements beyond the initial requirements document should be reviewed to ensure that they meet the strategic needs of the enterprise and are cost-effective. Otherwise, the final system may be functionally rich but inefficient.

A potential risk with prototyped systems is that the finished system will have poor controls. By focusing mainly on what the user wants and what the user sees, system developers may miss some of the controls, such as backup recovery, security and audit trails, that come out of the traditional system development approach.

Change control often becomes much more complicated with prototyped systems. Changes in designs and requirements happen so quickly that they are seldom documented or approved, and the system can escalate to a point of not being maintainable.

Although an IS auditor should be aware of the risk associated with prototyping, an IS auditor should also be aware that this method of system development can provide the enterprise with significant time and cost savings.

Rapid Application Development

RAD is a methodology that enables an organization to develop strategically important systems quickly, while reducing development costs and maintaining quality. This is achieved by using a series of proven application development techniques within a well-defined methodology. These techniques include the use of:

- Small, well-trained development teams
- Evolutionary prototypes
- Integrated power tools that support modeling, prototyping and component reusability
- A central repository
- Interactive requirements and design workshops
- Rigid limits on development time frames

RAD supports the analysis, design, development and implementation of individual application systems. However, RAD does not support the planning or analysis required to define the information needs of the enterprise as a whole or of a major business area of the enterprise. RAD provides a means of developing systems faster while reducing cost and increasing quality. This is done by automating large portions of the SDLC, imposing rigid limits on development time frames and reusing existing components. The RAD methodology has four major stages:

- **Concept definition stage**—Defines the business functions and data subject areas that the system will support and determines the system scope
- **Functional design stage**—Uses workshops to model the system's data and processes and build a working prototype of critical system components
- **Development stage**—Completes the construction of the physical database and application system, builds the conversion system and develops user aids and deployment work plans
- **Deployment stage**—Includes final-user testing and training, data conversion and the implementation of the application system

©ISACA. All Rights Reserved.

RAD uses prototyping as its core development tool no matter which underlying technology is used. In contrast, object-oriented software development (OOSD) and data-oriented system development (DOSD) use continuously developing models but have a focus on content solution space (e.g., how to best address the problem to make the code reusable and maintainable) and can be applied using a traditional waterfall approach. It should also be noted that BPR attempts to convert an existing business process rather than make dynamic changes.

Agile Development

Agile development is an alternative method for software development. Assuming that all requirements cannot be articulated upfront, agile approaches, such as the Scrum methodology, propose a more iterative and incremental approach instead of the sequential approach of the SDLC. Scrum aims to move planning and directing tasks from the project manager to the team, leaving the project manager to work on removing the obstacles to the team's ability to achieve its objectives. Other agile methods include Extreme Programming (XP), Crystal, Adaptive Software Development (ASD), Feature Driven Development (FDD) and Dynamic Systems Development Method (DSDM). These processes are termed agile because they are designed to flexibly handle changes to the system being developed or the project that is performing the development.

Agile development processes have many common characteristics:

- The use of small, time-boxed subprojects or iterations. In this instance, each iteration forms the basis for planning the next iteration.
- Replanning the project at the end of each iteration (referred to as a sprint in Scrum), including reprioritizing requirements, identifying any new requirements and determining within which release delivered functionality should be implemented.
- Relatively greater reliance, compared to traditional methods, on tacit knowledge—the knowledge in people's heads—as opposed to external knowledge that is captured in project documentation.
- A heavy influence on mechanisms to effectively disseminate tacit knowledge and promote teamwork. Therefore, teams are kept small, comprise business and technical representatives and are located physically together. Team meetings to verbally discuss progress and issues occur daily, but with strict time limits.
- At least some of the agile methods stipulate pair-wise programming (two persons code the same part of the system) as a means of sharing knowledge and as a quality check.
- A change in the role of the project manager, from one primarily concerned with planning the project, allocating tasks and monitoring progress to that of a facilitator and advocate.
- Responsibility for planning and control is delegated to the team members.

Agile development does not ignore the concerns of traditional software development but approaches them from a different perspective. Agile development:

- Only plans for the next iteration in detail, rather than planning subsequent development phases
- Uses an adaptive approach to requirements and does not emphasize managing a requirements baseline
- Focuses on quickly proving an architecture by building functionality versus formally defining, early on, software and data architecture in increasingly more detailed models and descriptions
- Assumes limits to defect testing but attempts to validate functions through a frequent-build test cycle and corrects problems in the next subproject before too much time and cost are incurred
- Does not emphasize defined and repeatable processes, but instead performs and adapts its development based on frequent inspections

Object-Oriented System Development

OOSD is the process of solution specification and modeling in which data and procedures can be grouped into an entity known as an object. An object's data is referred to as its attributes, and its functionality is referred to as its methods. This contrasts with the traditional (structured SDLC) approach that considers data separately from the procedures that act on them (e.g., program and database specifications). Proponents of OOSD claim that the combination of data and functionality is aligned with how humans conceptualize everyday objects.

OOSD is a programming technique, not a software development methodology. OOSD can be done while following any of the widely diverse set of software methodologies. A particular programming language or use of a particular programming technique does not imply or require use of a particular software development methodology.

Objects usually are created from a general template called a class. The template contains the characteristics of the class without containing the specific data that need to be inserted into the template to form the object. Classes are the basis for most design work in objects. Classes

are either superclasses (i.e., root or parent classes) with a set of basic attributes, or methods or subclasses, which inherit the characteristics of the parent class and may add (or remove) functionality as required. In addition to inheritance, classes may interact through sharing data, referred to as aggregate or component grouping, or sharing objects.

Aggregate classes interact through messages, which are requests for services from one class (called a client) to another class (called a server). The ability of two or more objects to interpret a message differently at execution, depending on the superclass of the calling object, is termed polymorphism.

To realize the full benefits of using object-oriented programming, it is necessary to employ object-oriented analysis and design approaches. Dealing with objects should permit analysts, developers and programmers to consider larger logical chunks of a system and clarify the programming process.

The major advantages of OOSD are as follows:
- Ability to manage an unrestricted variety of data types
- Provision of a means to model complex relationships
- Capacity to meet the demands of a changing environment

A significant development in OOSD is the use of Unified Modeling Language (UML). UML is a general-purpose notational language for specifying and visualizing complex software for large object-oriented projects, but it may be used for other purposes. This signals a maturation of the object-oriented development approach. Although object-orientation is not yet pervasive, it can accurately be said to have entered the computing mainstream. Applications that use object-oriented technology are:
- Web applications
- Ebusiness applications
- Computer-aided software engineering (CASE) for software development
- Office automation for email and work orders
- Artificial intelligence (AI)
- Computer-assisted manufacturing (CAM) for production and process control

Component-Based Development

Component-based development can be regarded as an outgrowth of object-oriented development. Component-based development means assembling applications from cooperating packages of executable software that make their services available through defined interfaces (i.e., enabling pieces of programs, called objects, to communicate with one another regardless of the programming language in which they were written or what OS they are running). The basic types of components are:
- **In-process client components**—These components must run from within a parent/host container such as a mobile application, a virtual machine appliance or an applet.
- **Stand-alone client components**—Applications that expose services to other software can be used as components. Well-known examples are Microsoft Excel and Word.
- **Stand-alone server components**—Processes running on servers that provide services in standardized ways can be components by means of web application frameworks, application servers, web services, Lightweight Directory Access Protocol (LDAP) directory services, etc.
- **In-process server components**—These components run on servers within containers. Examples include Microsoft Transaction Server (MTS) and Oracle JavaBeans.

Tool developers support one or another of these standards with powerful visual tools now available for designing and testing component-based applications. Additionally, a growing number of commercially available application servers support MTS or Enterprise JavaBeans (EJB). There is a growing market for third-party components. A primary benefit of component-based development is the ability to buy proven, tested software from commercial developers. The range of components available has increased. The first components were simple in concept (e.g., buttons and list boxes). Components now provide much more diverse functionality. Databases are now available on the web to search for commercial components.

Components play a significant role in web-based applications. Applets are required to extend static HTML, ActiveX controls or Java. Both technologies are compatible with component development.

Component-based development:
- **Reduces development time**—If an application system can be assembled from prewritten components and only code for unique parts of the system needs to be developed, then this should prove faster than writing the entire system from scratch.
- **Improves quality**—Using prewritten components means a significant percentage of the system code has been tested already.
- **Allows developers to focus more strongly on business functionality**—An outcome of component-based development and its enabling technologies is

©ISACA. All Rights Reserved.

to further increase abstraction already achieved with high-level languages, databases and user interfaces. Developers are shielded from low-level programming details.
- **Promotes modularity**—By encouraging or forcing impassable interfaces between discrete units of functionality, it encourages modularity.
- **Simplifies reuse**—It avoids the need to be conversant with procedural or class libraries, allowing cross-language combination and allowing reusable code to be distributed in an executable format (i.e., no source is required). (To date, large-scale reuse of business logic has not occurred.)
- **Reduces development cost**—Less effort needs to be expended on design and build. Instead, the cost of software components can be spread across multiple users.
- **Supports multiple development environments**—Components written in one language can interact with components written in other languages or running on other machines.
- **Allows a satisfactory compromise between build and buy options**—Instead of buying a complete solution, which perhaps does not entirely fit requirements, it may be possible to purchase only needed components and incorporate these into a customized system.

To realize these advantages, attention to software integration should be paid early and continuously during the development process. No matter how efficient component-based development is, if system requirements are poorly defined or the system fails to adequately address business needs, the project will not be successful. Risk associated with component-based development include:
- Lack of interoperability standards between different components
- Reduced system reliability
- Unintended system use from software introducing a vulnerability risk
- Increased external exposure from connecting the system to the Internet
- Increased vulnerability and attack surface from integrating components with one another
- Problems in system updates
- Incompatibility of new version with user requirements
- Problems in licensing different components

Web-Based Application Development

Web-based application development is an important software development approach designed to achieve easier and more effective integration of code modules within and between enterprises. Historically, software written in one language on a particular platform has used a dedicated application programming interface (API). The use of specialized APIs has caused difficulties in integrating software modules across platforms. Technologies such as common object request broker architecture (CORBA) and component object model (COM) that use remote procedure calls (RPCs) have been developed to allow real-time integration of code across platforms. However, using these RPC approaches for different APIs remains complex. Web-based application development and associated Extensible Markup Language (XML) technologies are designed to further facilitate and standardize code module and program integration.

The other problem that web-based application development seeks to address is avoiding the need to perform redundant computing tasks with the inherent need for redundant code. One example of this is a change of address notification from a customer. Instead of having to update details separately in multiple databases (e.g., contact management, accounts receivable and credit control), it is preferable for a common update process to update the multiple places required. Web services are intended to make this relatively easy to achieve.

Web application development is different from traditional third- or fourth-generation program developments in many ways—from the languages and programming techniques used to the methodologies used to control the development work, to the way the users test and approve the development work. The risk of application development remains the same. For example, buffer overflows have been a risk since computer programming was invented (e.g., truncation issues with first-generation computer programs), are widely known, and can be exploited by almost anyone, almost anywhere in the world, courtesy of the Internet.

Like with traditional program development, a risk-based approach should be taken in the assessment of web application vulnerabilities: Identify the business goals and supporting IT goals related to the development, then identify what can go wrong. Previous experience can be used to identify risk related to inadequate specifications, poor coding techniques, inadequate documentation, inadequate quality control (QC) and QA (including testing inadequacies), lack of proper change control and controls over promotion into production, etc., and put these in the context of the web application languages, development processes and deliverables (perhaps with the support of best practice material/literature on web applications development). The focus should be on

application development risk, the associated business risk and technical vulnerabilities and how these could materialize and be controlled/addressed. Some controls will look the same for all application development activity, but many will need to reflect the way the development activity is taking place in the area under review.

With web-based application development, the XML language Simple Object Access Protocol (SOAP) is used to define APIs. SOAP will work with any OS and programming language that understands XML. SOAP is simpler than using the more complex RPC-based approach, with the advantage that modules are coupled loosely so that a change to one component does not normally require changes to other components.

The second key component of web development is the web services description language (WSDL), which is also based on XML. WSDL is used to identify the SOAP specification that is to be used for the code module API and the formats of the SOAP messages used for input and output to the code module. The WSDL also is used to identify the web service that is accessible via an enterprise intranet or across the Internet by being published to a relevant intranet or Internet web server.

The final component of web services is another XML-based language—universal description, discovery and integration (UDDI). UDDI is used to make an entry in a UDDI directory, which acts as an electronic directory that is accessible via an enterprise intranet or across the Internet and allows interested parties to learn of the existence of available web services.

Software Reengineering

Software reengineering is a process of updating an existing system by extracting and reusing design and program components. This process is used to support major changes in the way an enterprise operates, and there are a number of tools available to support it. Typical methodologies used in software reengineering generally fall into the following categories:

- BPR is the thorough analysis and significant redesign of business processes and management systems to establish a better performing structure that is more responsive to the customer base and market conditions, while yielding material cost savings.
- The service-oriented software reengineering methodology is based on the service-oriented computer architecture, and the reengineering processes apply many concepts of RAD leveraging responsible, accountable, consulted and informed (RACI) charts and UML modeling.

Reverse Engineering

Reverse engineering is the process of studying and analyzing an application, a software application or a product to see how it functions and to use that information to develop a similar system. This process can be carried out in different ways:

- Decompiling object or executable code into source code and using it to analyze the program
- Black-box testing the application to be reverse engineered to unveil its functionality

The major advantages of reverse engineering are:

- Faster development and reduced SDLC duration
- The possibility of introducing improvements by overcoming the reverse-engineered application drawbacks

An IS auditor should be aware of the following risk items:

- Software license agreements often contain clauses prohibiting the licensee from reverse engineering the software so that no trade secrets or programming techniques are compromised.
- Decompilers are relatively new tools with functions that depend on specific computers, OSs and programming languages. Any change in one of these components may require developing or purchasing a new decompiler.

DevOps and DevSecOps

DevOps refers to the integration of development and operations processes to eliminate conflicts and barriers. This integration can create numerous benefits, but it can also create new risk. Decisions to adopt DevOps should be made based on factors, such as an enterprise's climate, risk tolerance and culture, and on the scope of the development project. Because DevOps changes the environment and often impacts the enterprise's control environment and accepted level of risk, an IS auditor should ensure that there is proper SoD.

Implementing DevSecOps processes can be done in a logical and systematic manner and used to enhance the maturity of software development. This helps promote concepts, such as security-by-design, which in turn will reduce the overall likelihood of vulnerabilities being introduced during the development process. See section 5.12.10 DevSecOps for more information.

©ISACA. All Rights Reserved.

Business Process Reengineering and Process Change

In a generic process, some form of information enters the process and is processed, and the outcome is measured against the goal or objective of the process. The level of detail needed depends highly on the complexity of the process, the knowledge of the affected staff and the company's requirements regarding audit functionality (performance and compliance) of the process and whether it fits into an existing quality management system.

Any output produced by a process must be bound to a business objective and adhere to defined corporate standards. Monitoring of effectiveness (goal achievement), efficiency (minimum effort) and compliance must be done on a regular basis and should be included in management reports for review under the plan-do-check-act (PDCA) cycle.

BPR is the process of responding to competitive and economic pressures and customer demands to survive in the current business environment. This is usually done by automating system processes so that there are fewer manual interventions and manual controls. BPR achieved with the help of implementing an ERP system is often referred to as package-enabled reengineering (PER). Advantages of BPR are usually experienced when the reengineering process appropriately suits the business needs. BPR has increased in popularity as a method for achieving the goal of cost savings through streamlining operations.

The steps in a successful BPR are to:
- Define the areas to be reviewed.
- Develop a project plan.
- Gain an understanding of the process under review.
- Redesign and streamline the process.
- Implement and monitor the new process.
- Establish a continuous improvement process.

As a reengineering process takes hold, new results begin to emerge, such as:
- New business priorities based on value and customer requirements
- A concentration on process as a means of improving product, service and profitability
- New approaches to organizing and motivating people inside and outside the enterprise
- New approaches to the use of technologies in developing, producing and delivering goods and services
- New approaches to the use of information and powerful and more accessible information technologies
- Refined roles for suppliers including outsourcing, joint development, quick response, just-in-time inventory and support
- Redefined roles for clients and customers, providing them with more direct and active participation in the enterprise's business process

A successful BPR/process change project requires the project team to perform the following for the existing processes:
- Process decomposition to the lowest level required for effectively assessing a business process (typically referred to as an elementary process), which is a unit of work performed with a definitive input and output
- Identification of customers, process-based managers or process owners responsible for processes from beginning to end
- Documentation of the elementary process-related profile information including:
  - Duration
  - Trigger (which triggers the process to act)
  - Frequency
  - Effort
  - Responsibility (process owner)
  - Input and output
  - External interfaces
  - System interaction
  - Risk and control information
  - Performance measurement information
  - Identified problematic areas and their root causes

The existing baseline processes must be documented —preferably in the form of flowcharts and related profile documents—so they can be compared to the processes after reengineering. The newly designed business processes inevitably involve changes in the way(s) of doing business and can impact the finances, philosophy and personnel of the enterprise, its business partners and its customers.

Throughout the change process, the BPR team must be sensitive to enterprise culture, structure, direction and the components of change. Management must also be able to predict and/or anticipate issues and problems and offer appropriate resolutions that will accelerate the change process.

BPR teams can be used to facilitate and assist the staff in transitioning into the reengineered business processes. BPR professionals are valuable in monitoring progress

 ©ISACA. All Rights Reserved.

toward the achievement of the strategic plan of the enterprise.

A major concern in BPR is that key controls may be reengineered out of a business process. An IS auditor's responsibility is to identify the existing key controls and evaluate the impact of removing these controls. If the controls are key preventive controls, an IS auditor must ensure that management is aware of the removal of the control and is willing to accept the potential material risk of not having that preventive control.

When reviewing the enterprise's BPR efforts, an IS auditor must determine whether:

- The enterprise's change efforts are consistent with the overall culture and strategic plan.
- The reengineering team is trying to minimize any negative impact the change might have on the enterprise's staff.
- The BPR team has documented lessons to be learned after the completion of the BPR/process change project.

An IS auditor also provides a statement of assurance or conclusion with respect to the objectives of the audit.

Benchmarking Process

Benchmarking is about improving business processes. It is defined as a continuous, systematic process for evaluating the products, services or work processes of enterprises that are recognized as world-class references in a globalized world. Reference products, services or processes are systematically analyzed for one or more of the following purposes:

- Comparing and ranking
- Strategic planning; strengths, weaknesses, opportunities and threats (SWOT) analysis
- Investment decisions, enterprise takeovers, mergers
- Product or process design or redesign/reengineering
- BPR

The following steps are conducted in a benchmarking exercise:

1. **Plan**—The benchmarking team identifies the critical processes and gains an understanding of how they are measured, the kinds of data that are needed and how the data need to be collected.
2. **Research**—The team collects baseline data about the processes of its own enterprise before collecting the data about other enterprises. The next step is to identify the reference products or enterprises through sources such as business newspapers and magazines, quality award winners, trade journals and consultants. Depending on the team's own preferences and resources, and on the marketplace, several scenarios may result:
   a. Benchmarks that satisfy the enterprise's interest already exist at no charge from professional associations, journals or analysis firms.
   b. The enterprise may join or promote a survey launched by a single- or multi-industry specialized web portal (e.g., a bookmark portal).
   c. The enterprise may conduct or subcontract business intelligence.
   d. The enterprise may enter into an agreement with one or more benchmark partners who agree to share information.
3. **Observe**—The next step is to collect data and visit the benchmarking partner. There should be an agreement with the partner enterprise, a data collection plan and a method to facilitate proper observation.
4. **Analyze**—This step involves summarizing and interpreting the data collected and analyzing the gaps between an enterprise's process and its partner's process. Converting key findings into new operational goals is the goal of this stage.
5. **Adopt**—Adopting the results of benchmarking can be the most difficult step. In this step, the team needs to translate the findings into a few core principles and work down from principles, to strategies, to action plans.
6. **Improve**—Continuous improvement is the key focus in a benchmarking exercise. Benchmarking links each process in an enterprise with an improvement strategy and enterprise goals.

Note

Based on the information gathered during the research phase, steps three through six may be skipped or adapted.

3.3.6 System Development Tools and Productivity Aids

System development tools and productivity aids include CASE applications, code generators and 4GLs.

Computer-Aided Software Engineering

Application development efforts require collecting, organizing and presenting a substantial amount of data at the application, systems and program levels. A substantial amount of the application development effort involves translating this information into program logic and code for subsequent testing, modification and

©ISACA. All Rights Reserved.

implementation. This often is a time-consuming process, but it is necessary to develop, use and maintain computer applications.

CASE is the use of automated tools to aid in the software development process. Their use may include the application of software tools for software requirements capture and analysis, software design, code production, testing, document generation and other software development activities.

CASE products are generally divided into three categories:

1. **Upper CASE**—Products used to describe and document business and application requirements. This information includes data-object definitions and relationships and process definitions and relationships.
2. **Middle CASE**—Products used for developing detailed designs. These include screen and report layouts, editing criteria, data object organization and process flows. When elements or relationships change in the design, it is necessary to make only minor alterations to the automated design, and all other relationships are automatically updated.
3. **Lower CASE**—Products involved with the generation of program code and database definitions. These products use detailed design information, programming rules and database syntax rules to generate program logic, data file formats or entire applications.

Some CASE products cover two of these categories or all three of them. An example is an IDE, an application that facilitates more efficient program development by combining multiple capabilities and needs, such as being able to edit software and test in one location.

CASE tools provide a uniform approach to system development, facilitate storage and retrieval of documents and reduce the manual effort in developing and presenting system design information. This power of automation changes the nature of the development process by eliminating or combining some steps and altering the means of verifying specifications and applications.

An IS auditor needs to recognize the changes in the development process brought on by CASE. Some CASE systems allow a project team to produce a complete system from the DFDs and data elements without any traditional source code. In these situations, the DFDs and data elements become the source code.

An IS auditor should gain assurance that approvals are obtained for the appropriate specifications, users continue to be involved in the development process and investments in CASE tools yield benefits in quality and speed. Other key issues that an IS auditor needs to consider with CASE include the following:

- CASE tools help in the application design process but do not ensure that the design, programs and system are correct or that they fully meet the needs of the enterprise.
- CASE tools should complement and fit into the application development methodology, but a project methodology needs to be in place for CASE to be effective. It should be understood and used effectively by the enterprise's software developers.
- The integrity of data moved between CASE products or between manual and CASE processes needs to be monitored and controlled.
- Changes to the application should be reflected in stored CASE product data.
- Like a traditional application, application controls need to be designed.
- The CASE repository (the database that stores and organizes the documentation, models and other outputs from the different phases) needs to be secured on a need-to-know basis. Strict version control should be maintained on this database.

An IS auditor may use CASE tools because several features facilitate the audit process. DFDs may be used as an alternative to other flowcharting techniques. In addition, CASE tools can be used to develop interrogation software and EAMs. Repository reports should be used to gain an understanding of the system and review controls over the development process.

Code Generators

Code generators are tools that are often incorporated with CASE products, which generate program code based on parameters defined by a systems analyst or on data/entity flow diagrams developed by the design module of a CASE product. These products allow most developers to implement software programs with efficiency. An IS auditor should be aware of source code generated by such tools.

Fourth-Generation Languages

4GLs are used in software development to reduce the overall effort and cost. The common characteristics of 4GLs are:

- **Nonprocedural language**—Most 4GLs do not obey the procedural paradigm of continuous statement

 ©ISACA. All Rights Reserved.

execution and subroutine call and control structures. Instead, they are event-driven and make extensive use of object-oriented programming concepts such as objects, properties and methods.
  - For example, a COBOL programmer who wants to produce a report sorted in a given sequence must first open and read the data file, sort the file and finally produce the report. A typical 4GL treats the report as an object with properties, such as input file name and sort order, and methods, such as sort file and print report.
  - Care should be taken when using 4GLs. Unlike traditional languages, 4GLs can lack the lower-level detail commands necessary to perform certain types of data-intensive or online operations. These operations are usually required when developing major applications. For this reason, the use of 4GLs as development languages should be weighed carefully against traditional languages already discussed.
- **Environmental independence (portability)**—Many 4GLs are portable across computer architectures, OSs and telecommunications monitors. Some 4GLs have been implemented on mainframe processors and microcomputers.
- **Software facilities**—These facilities include the ability to design or paint retrieval screen formats, develop computer-aided training routines or help screens, and produce graphical outputs.
- **Programmer workbench concepts**—The programmer has access through the terminal to easy filing facilities, temporary storage, text editing and OS commands. This type of workbench approach is closely associated with the CASE application development approach. It is often referred to as an IDE.
- **Simple language subsets**—4GLs generally have simple language subsets that can be used by less-skilled users in an information center.

4GLs are often classified in the following ways:
- **Query and report generators**—These specialized languages can extract and produce reports (audit software). Recently, more powerful languages have been produced that can access database records, produce complex online outputs and be developed in an almost-natural language.
- **Embedded database 4GLs**—These depend on self-contained DBMSs. This characteristic often makes them more user-friendly but also may lead to applications that are not integrated well with other production applications. Examples include FOCUS, Rapid Access Management Information System (RAMIS) II and NCSS Owned, Maintained, And Developed (NOMAD) 2.
- **Relational database 4GLs**—These high-level language products are usually an optional feature on a vendor's DBMS product line. These allow the applications developer to make better use of the DBMS product, but they often are not end-user oriented. Examples include SQL+, MANTIS and Natural.
- **Application generators**—These development tools generate third-generation programming languages (i.e., 3GLs) such as COBOL and C. The application can be further tailored and customized. Data processing development personnel, not end users, use application generators.

3.3.7 Infrastructure Development/ Acquisition Practices

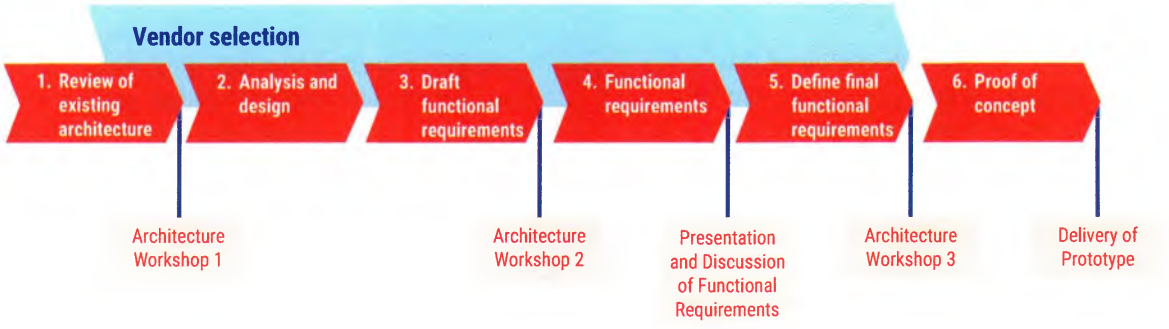
The physical architecture analysis, the definition of a new architecture and the necessary road map to move from one to the other are critical tasks for an IT department. The impact of these tasks is not only economic but also technological because it decides many other choices downstream, such as operational procedures, training needs, installation issues and TCO. Conflicting requirements—such as evolving toward a services-based architecture, legacy hardware considerations, secure data access independent of data location, zero data loss and 24/7 availability—ensure that no single platform satisfies all these requirements equally. Thus, physical architecture analysis cannot be based solely on price or isolated features. A formal, reasoned choice must be made. Information and communication technology (ICT) departments are often tasked with making these decisions. The suggested solution must accomplish the following:
- Ensure alignment of the ICT with enterprise standards.
- Provide appropriate levels of security and privacy.
- Integrate with current IT systems.
- Consider IT industry trends.
- Provide future operational flexibility to support business processes.
- Allow for projected growth in infrastructure without major upgrades.
- Include technical architecture considerations for information security, secure storage, etc.
- Ensure cost-effective, day-to-day operational support.
- Foster the usage of standardized hardware and software.
- Maximize ROI, cost transparency and operational efficiency.

©ISACA. All Rights Reserved.

Project Phases of Physical Architecture Analysis

Figure 3.15 shows the project phases of physical architecture analysis and the time at which the vendor selection process may take place.

Figure 3.15—Project Phases of Physical Architecture Analysis



Review of Existing Architecture

To start the process, the most current documents describing the existing architecture must be reviewed. Participants of the first workshop are specialists of the ICT department in all areas directly impacted by physical architecture. Examples are server, storage, security and overall IT infrastructure.

Special care must be taken in characterizing all the operational constraints that impact physical architecture, such as:

- Ground issues
- Size limits
- Weight limits
- Current power supply
- Environmental operating limitations (temperature and humidity minimum and maximum)
- Physical security issues

The output of the first workshop is a list of components of the current infrastructure and constraints defining the target physical architecture.

Analysis and Design

After reviewing the existing architecture, the analysis and design of the actual physical architecture is undertaken, adhering to good practices and meeting business requirements.

Draft Functional Requirements

With the first physical architecture design in hand, the first draft of functional requirements is composed. This material is the input for the next step and the vendor selection process.

Vendor and Product Selection

While the draft functional requirements are written, the vendor selection process proceeds in parallel.

Writing Functional Requirements

After finishing the draft functional requirements and feeding the second part of this project, the functional requirements document is written and introduced at the second architecture workshop with staff from all affected parties. The results are discussed and a list of the requirements that need to be refined or added are composed.

This is the last checkpoint before the sizing and the proof of concept (POC) starts, although the planning of the POC starts after the second workshop. With the finished functional requirements, the POC phase begins.

Proof of Concept

Establishing a POC is highly recommended to prove that the selected hardware, software and data are able to meet all expectations, including security requirements. The deliverable of the POC should be a running prototype,

 ©ISACA. All Rights Reserved.

including the associated document and test protocols describing the tests and their results.

To start, the POC should be based on the results of the procurement phase (described in a subsection below). For this purpose, a representative subset of the target hardware is used. The software to run the POC can be either test versions or software already supplied by the vendor; therefore, additional costs are expected to be minimal. To keep costs low, most elements of the framework are implemented in a simplified form. They will be extended to their final form in later phases.

The prototype should demonstrate the following features:

- Basic setup of the core security infrastructure
- Correct functionality of auditing components
- Basic but functional implementation of security measures as defined
- Secured transactions
- Characterization in terms of installation constraints and limits (server size, server current consumption, server weight, server room physical security)
- Performance
- Resiliency to include basic failover to a trusted operational state
- Funding and costing model
- Data and algorithm

Related implementation projects that prepare for deployment should also be part of the POC because they will be used in the same way as they are used in the production of physical architecture. At the end of this phase, a last workshop is held where the production sizing and layout is adapted to include POC conclusions.

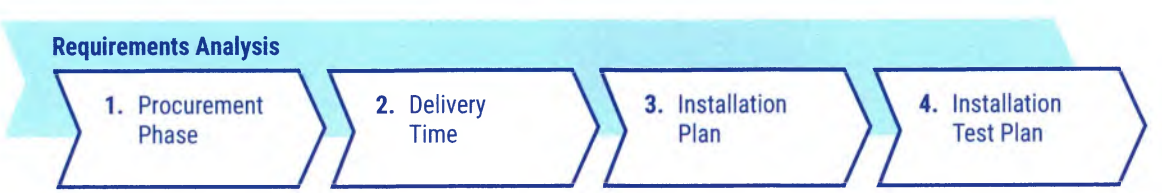
Additional considerations may apply if the entity goes in for an outsourcing/offshoring model for deployment and operation of applications. Also, the platform for operation of the IT environment (i.e., owned, cloud-based, virtualization) can give rise to additional considerations. For example, if the enterprise operates in a highly regulated industry or an industry that demands high levels of availability, adequate redundancy and safeguards for ensuring data privacy and confidentiality may have to be factored in while testing the POC.

Planning Implementation of Infrastructure

To ensure the quality of the results, it is necessary to use a phased approach to fit the entire puzzle together. It is also fundamental to set up the communication processes for other projects like those described earlier. Through these different phases, the components are fit together, and a clear understanding of the available and contactable vendors is established by using the selection process during the procurement phase and beyond. Furthermore, it is necessary to select the scope of key business and technical requirements to prepare for the next steps, which include the development of the delivery, installation and test plans. Moreover, to ensure a future proven solution, it is crucial to choose the right partners with the right skills.

As shown in **figure 3.16**, the requirements analysis is not part of this process but constantly feeds results into the process. If a Gantt chart is produced with these phases, most likely some phases overlap; therefore, the different phases must be considered an iterative process.

Figure 3.16—Project Phases of Planning the Implementation of Infrastructure



During the four phases, it is necessary to fit all the components together to prepare for projects downstream (e.g., data migration).

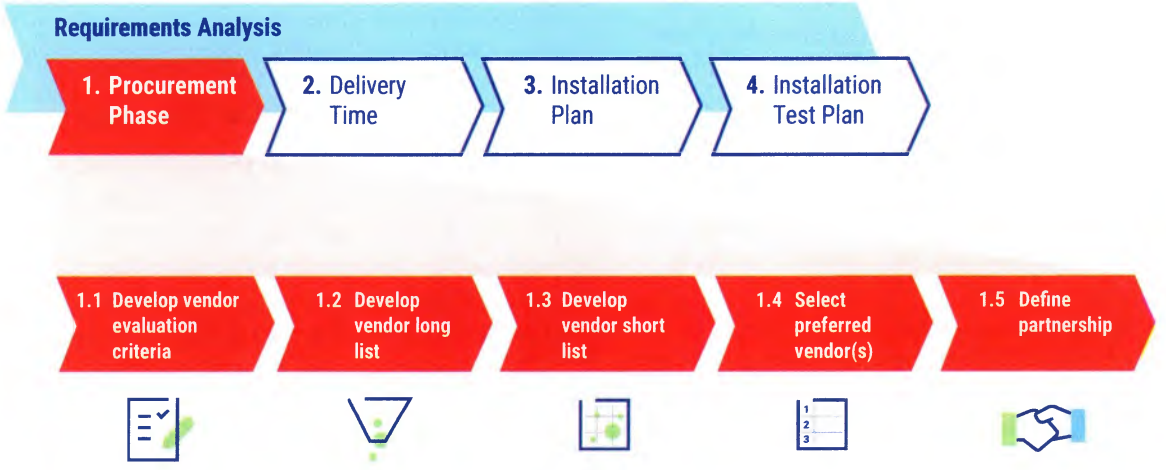
Procurement Phase

During the procurement phase, communication between the business and the analysis project is established to provide an overview of the chosen solution and determine the quantity structure of the deliverables. The requirements statements are also produced. Additionally,

©ISACA. All Rights Reserved.

the procurement process begins the service-level management process. During these activities, the preferred partners are invited to the negotiations process, and the deliverables, contracts and SLAs are signed (**figure 3.17**).

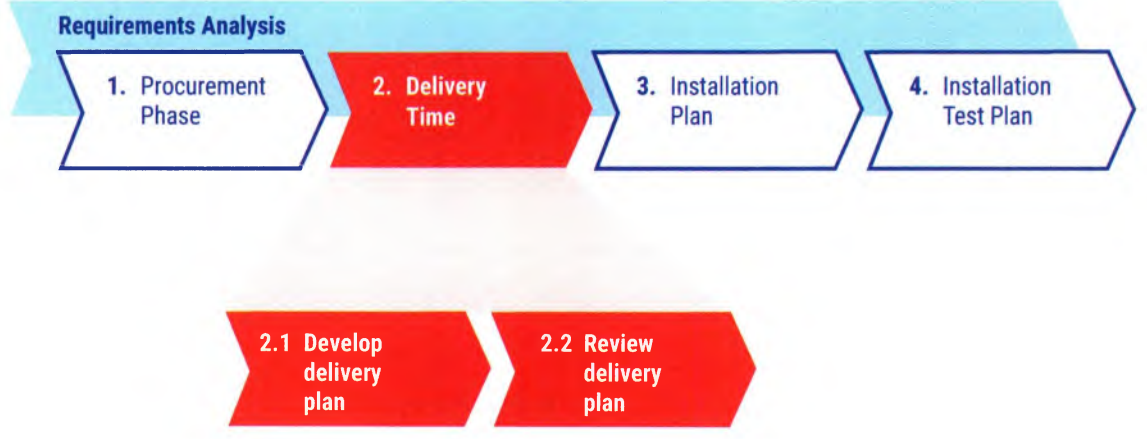
Figure 3.17—Procurement Phases



Delivery Time

During the delivery time phase, the delivery plan is developed (**figure 3.18**). This phase overlaps in some parts with the procurement phase.

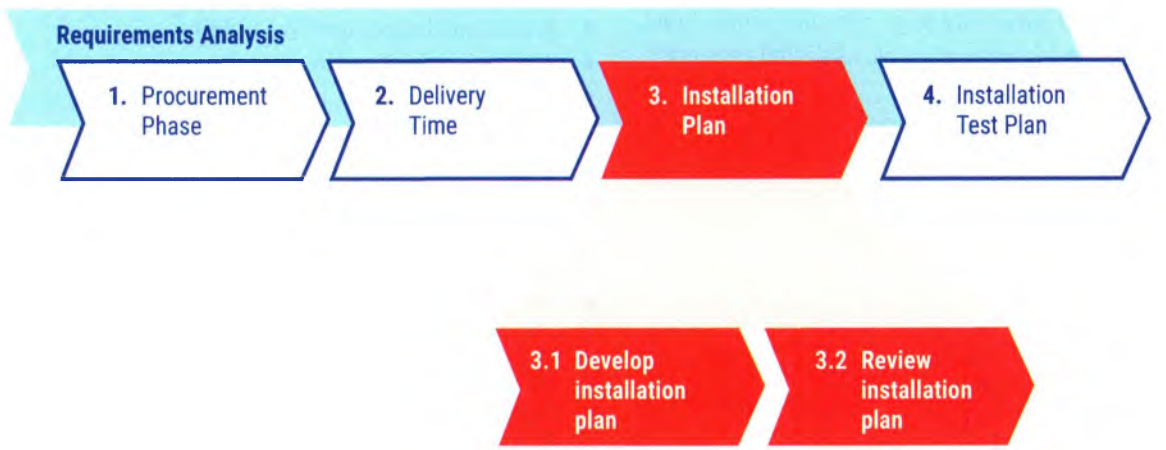
Figure 3.18—Delivery Time



 ©ISACA. All Rights Reserved.

The delivery plan should include topics such as priorities, goals and nongoals, key facts, principles, communication strategies, key indicators, and progress on key tasks and responsibilities.

Figure 3.19—Installation Plan



An additional step is to review the plan with the involved parties and with those responsible for the integration projects. This is an iterative process.

Installation Test Plan

Based on the known dependencies of the installation plan, the test plan is developed.

The test plan includes test cases, basic requirements' specifications, definition of the processes and, as much as possible, measurement information for the applications and the infrastructure. Part one of the project (analysis of the physical architecture) must be completed, and the needed infrastructure decisions must be made.

3.3.8 Hardware/Software Acquisition

Selection of a computer hardware and software environment frequently requires the preparation of specifications for distribution to hardware/software (HW/SW) vendors and criteria for evaluating vendor proposals. The specifications are sometimes presented to vendors in the form of an invitation to tender (ITT), also known as a request for proposal (RFP). The specifications must define, as completely as possible, the usage, tasks and requirements for the equipment needed and must include a description of the environment in which that equipment will be used.

Installation Plan

During the installation planning phase, the installation plan is developed in cooperation with all affected parties (**figure 3.19**).

Note

For the purposes of this section, the term hardware can also refer to cloud-related providers replacing the enterprise need for traditional hardware.

When acquiring a system, the specifications should include the following:

- Organizational descriptions indicating whether the computer facilities are centralized or decentralized, distributed, outsourced, manned or lights-out HW/SW evaluation assurance levels (EALs) for security robustness
- Information processing requirements, such as:
  - Major existing application systems and future application systems
  - Workload and performance requirements
  - Processing approaches (e.g., online/batch, client-server, real-time databases, continuous operation)
- Hardware requirements, such as:
  - Central processing unit (CPU) speed
  - Disk space requirements
  - Memory requirements

©ISACA. All Rights Reserved.

  - Number of CPUs required
  - Peripheral devices (e.g., direct access devices, such as magnetic disk drives, printers, digital video disc drives, USB peripherals and secure digital multimedia cards [SD/MMC]) required or to be excluded (usually for security reasons)
  - Data preparation/input devices that accept and convert data for machine processing
  - Direct entry devices (e.g., terminals, point-of-sale [POS] terminals or automated teller machines)
  - Networking capability (e.g., ethernet connections, modems and integrated services digital network [ISDN] connections)
  - Number of terminals or nodes that the system needs to support
- System software applications, such as:
  - OS software (current version and any required upgrades)
  - Utilities
  - Compilers
  - Program library software
  - Database management software and programs
  - Communications software
  - Access control software
  - Job scheduling software
- Support requirements, such as:
  - System maintenance (for preventive, detective [fault reporting] or corrective purposes)
  - Training (user and technical staff)
  - Backups (daily and disaster backups)
  - Patching
- Adaptability requirements, such as:
  - Hardware and software upgrade capabilities
  - Compatibility with existing hardware and software platforms
  - Changeover to other equipment capabilities
- Constraints, such as:
  - Staffing levels
  - Existing hardware capacity
  - Delivery dates
- Conversion requirements, such as:
  - Test time for the hardware and software
  - System conversion facilities
  - Cost/pricing schedule

Acquisition Steps

When purchasing (acquiring) HW/SW from a vendor, consideration should be given to the following:

- Testimonials or visits with other users
- Provisions for competitive bidding
- Analysis of bids against requirements
- Comparison of bids against each other using predefined evaluation criteria
- Analysis of the vendor's financial condition
- Analysis of the vendor's capability to provide maintenance and support (including training)
- Review of delivery schedules against requirements
- Pedigree of the hardware to verify that it is not sourced from gray market supply sources (i.e., through distribution sources that are legal but are unofficial, unauthorized or unintended by the original manufacturer) that can increase the risk of malware and other unknowns on the operability of the product
- Analysis of hardware and software upgrade capability
- Analysis of security and control facilities
- Evaluation of performance against requirements
- Review and negotiation of price
- Review of contract terms (including warranties, penalties and right-to-audit clauses)
- Preparation of a formal written report summarizing the analysis for each of the alternatives and justifying the selection based on benefits and cost

The criteria and data used for evaluating vendor proposals should be properly planned and documented. **Figure 3.20** lists some criteria that should be considered in the evaluation process.

Figure 3.20—Vendor Evaluation Criteria

Term	Definition
Project schedule	A timetable provided by the vendor that outlines their estimation of the start and end dates and milestones that must be met for the project to be completed. This needs to be compared to the planned schedule and project completion date of the client.
Turnaround time	The time that the help desk or vendor takes to fix a problem from the moment it is logged in
Response time	The time a system takes to respond to a specific query by the user
System reaction time	The time taken for logging into a system or getting connected to a network

 ©ISACA. All Rights Reserved.

Figure 3.20—Vendor Evaluation Criteria (cont.)

Term	Definition
Throughput	The quantity of useful work made by the system per unit of time. Throughput can be measured in instructions per second or some other unit of performance. When referring to a data transfer operation, throughput measures the useful data transfer rate and is expressed in kilobits per second (Kbps), megabits per second (Mbps) and gigabits per second (Gbps).
Workload	The capacity to handle the required volume of work or the volume of work that the vendor system can handle in a given time frame
Compatibility	The capability of an existing application to run successfully on the newer system supplied by the vendor
Capacity	The capability of the newer system to handle numerous simultaneous requests from the network for the application and the volume of data that it can handle from each of the users
Utilization	The system availability time versus the system downtime

When performing an audit of this area, an IS auditor should:

- Determine if the acquisition process began with a business need and whether the hardware requirements for this need were considered in the specifications.
- Determine if several vendors were considered and whether the comparison between them was done according to the aforementioned criteria.

3.3.9 System Software Acquisition

Every time a technological development has allowed for increased computing speeds or new capabilities, these have been absorbed immediately by the demands placed on computing resources by more ambitious applications. Consequently, improvements have led to decentralized, interconnected open systems through functions bundled in OS software to meet these needs. For example, network management and connectivity are features now found in most OSs.

It is IT management's responsibility to be aware of HW/SW capabilities because they may improve business processes and provide expanded application services to businesses and customers in a more effective way. Short- and long-term plans should document the IS management plan for migrating to newer, more efficient and more effective OSs and related systems software.

When selecting new system software, business and technical issues must be considered, including:

- Business, functional and technical needs and specifications
- Cost and benefit(s)
- Obsolescence
- Compatibility with existing systems
- Security
- Demands on existing staff
- Training and hiring requirements
- Future growth needs
- Impact on system and network performance
- Open source code versus proprietary code

The feasibility study should contain documentation that supports the decision to acquire the software. Depending on the software required, there can be four cases:

1. Software is required for a generic business process for which vendors are available and software can be implemented without customization.
2. Software (vendor's) needs to be customized to suit business processes.
3. Software needs to be developed by the vendor.
4. Software is available as a service through the cloud (software as a service [SaaS]). This is generally available for generic processes.

A project team with participation by technical support staff and key users should be created to write an RFP or ITT. An RFP needs to be prepared separately for each case mentioned previously. The invitation to respond to an RFP should be widely distributed to appropriate vendors and, if possible, posted via a public procurement medium (Internet or newspaper). This process allows the business to determine which of the responding vendor products offers the best solution at the most cost-effective price.

The RFP should include the areas shown in **figure 3.21**.

©ISACA. All Rights Reserved.

Figure 3.21—Request for Proposal Contents

Item	Description
Product versus system requirements	The chosen vendor's product should come as close as possible to meeting the defined requirements of the system. If no vendor's product meets all of the defined requirements, the project team, especially the users, need to decide whether to accept the deficiencies. An alternative to living with product's deficiencies is for the vendor or the purchaser to make customized changes to the product.
Product scalability and interoperability	The project management should not only look at vendor's product ability to meet the existing requirements for the project but also the ability of the product to grow and/or contract with the enterprise's business processes. Vendor products should be assessed regarding the applications' ability to interconnect with other systems whose interconnections are currently out of the project's scope but may be needed in the future.
Customer references	Project management should check vendor-supplied references to validate the vendor's claims of product performance and completion of work by the vendor.
Vendor security requirements	The vendor should be protecting data to a level suitable for the purchasing enterprise's risk tolerance. This is most applicable to software as a service (SaaS) or vendors who will have access to an enterprise's information system or data. Security requirements should outline applicable requirements to ensure the confidentiality, integrity and availability of an enterprise's data. Security requirements may also include a requirement to maintain compliance with applicable laws, regulations or contractual requirements. Additionally, requirements for the right to audit should be included.
Vendor viability/financial stability	The vendor supplying or supporting the product should be reputable and able to provide evidence of financial stability. A vendor may not be able to prove financial stability; if the product is new, the vendor presents a substantially higher risk to the enterprise.
Availability of complete and reliable documentation	The vendor should be willing and able to provide a complete set of system documentation for review prior to acquisition. The level of detail and precision found in the documentation may be an indicator of the detail and precision used within the design and programming of the system itself.
Vendor support	The vendor should have available a complete line of support products for the software package. This may include a 24-hour, seven-day-a-week help line, onsite training during implementation, product upgrades, automatic new version notification and onsite maintenance, if requested.
Source code availability	The source code should be received either from the vendor initially or there should be provisions for acquiring the source code if the vendor goes out of business. Usually, these clauses are part of a software escrow agreement in which a third party holds the software in escrow should such an event occur. The acquiring enterprise should ensure that product updates and program fixes are included in the escrow agreement.
Number of years of experience in offering the product	More years indicate stability and familiarity with the business that the product supports.
A list of recent or planned enhancements to the product, with dates	A short list suggests that the product is not being kept current.
Number of client sites using the product with a list of current users	A larger number suggests wide acceptance of the product in the marketplace.
Acceptance testing of the product	Such testing is crucial in determining whether the product really satisfies the system requirements. This is allowed before a purchasing commitment must be made.

When the product and related services are known in advance, a user enterprise often prefers an ITT so it can obtain the best combination of price and services. This is more applicable when procurement of hardware, network, database, etc., is involved. When the requirement is more toward a solution and related

 ©ISACA. All Rights Reserved.

support and maintenance, an enterprise generally prefers an RFP, so the capability, experience and approach can be measured against the requirement. This is more applicable in system integration projects, such as ERP and supply chain management (SCM) that involve delivery or escrowing of source code.

Often, prior to the development of an RFP, an enterprise will develop a request for information (RFI) to solicit software development vendors for advice in addressing problems with existing systems. Information obtained in this manner may be used to develop an RFP. The project team needs to carefully examine and compare the vendors' responses to the RFP. This comparison should be done using an objective method, such as a scoring and ranking methodology. After the RFP responses have been examined, the project team may be able to identify a single vendor whose product satisfies most or all of the stated requirements in the RFP. Otherwise, the team may narrow the list to two or three acceptable candidates (i.e., short list of vendors). In evaluating the best-fit solution and vendor against the given set of business requirements and conditions, a suitable methodology of evaluation should be adopted. The methodology should ensure objective, equitable and fair comparison of the products/vendors (e.g., a gap analysis to find out the differences between requirements and software, the parameters required to modify).

It is important to keep in mind the minimum and recommended requirements to use software, including:

- Required hardware, such as memory, disk space and server or client characteristics
- OS versions and patch levels supported
- Additional tools, such as import and export tools
- Databases supported

In addition, it is likely that more than one product/vendor fits the requirements, with advantages and disadvantages with respect to each other. To resolve such a situation, agenda-based presentations should be requested from the short-listed vendors. The agenda-based presentations are scripted business scenarios that are designed to show how the vendor will perform certain critical business functions. Vendors are typically invited to demonstrate their product and follow the sample business scenarios given to them to prepare. It is highly recommended to include adequate participation from various user groups when evaluating the product's/vendor's fit and the system's ease of use. The project team has an opportunity to check the intangible issues such as the vendor's knowledge of the product and the vendor's ability to understand the business issue. Having each short-listed vendor demonstrate its product following a scripted document also enables the project team to evaluate and finalize the product/vendor selection with knowledge and objectivity built into the process. The finalist vendor candidate is then requested to organize site visits to confirm the findings from the agenda-based presentations and check the system in a live environment. After the finalist is confirmed, a conference-room pilot should be conducted. A conference-room pilot enables the project team to understand the system with a hands-on session with business end users and identify the areas that need certain customizations or workarounds.

An IS auditor should encourage the project team to contact current users. The information obtained from these discussions or visits validates statements made in the vendor's proposal and can determine which vendor is selected. The discussions with the current users should concentrate on each vendor's:

- **Reliability**—Are the vendor's deliverables (enhancements or fixes) dependable?
- **Commitment to service**—Is the vendor responsive to problems with its product? Does the vendor deliver on time?
- **Commitment to providing training, technical support and documentation for its product**—What is the level of customer satisfaction?

After completing the activities cited, vendor presentations and final evaluations, the project team can make a product/vendor selection. The reasons for making a particular choice should be documented.

The last step in the acquisition process is to negotiate and sign a contract for the chosen product. Appropriate legal counsel should review the contract prior to its signing. The contract should contain the following items:

- Specific description of deliverables and their costs
- Commitment dates for deliverables
- Commitments for delivery of documentation, fixes, upgrades, new release notifications and training
- Commitments for data migration
- Allowance for a software escrow agreement, if the deliverables do not include source code
- Description of the support to be provided during installation/customization
- Criteria for user acceptance
- Provision for a reasonable acceptance testing period, before the commitment to purchase is made
- Allowance for changes to be made by the purchasing enterprise
- Maintenance agreement
- Allowance for copying software for use in business continuity efforts and for test purposes
- Payment schedule linked to actual delivery dates

©ISACA. All Rights Reserved.

- Confidentiality clauses
- Data protection and compliance clauses
- Right to ongoing audit (if applicable)

Managing the contract should also involve a major level of effort to ensure that deployment efforts are controlled, measured and improved on, where appropriate. This may include regular status reporting requirements. Additionally, the milestones and metrics to be reported against should be agreed on with the vendor.

IS Auditor's Role in Software Acquisition

An IS auditor should be involved in the software acquisition process to determine whether an adequate level of security controls has been considered prior to any agreement being reached. If security controls are not part of the software, it may become difficult to ensure data integrity for the information that will be processed through the system. Risk involved with the software package includes inadequate audit trails, password controls and overall security of the application. Because of the risk, an IS auditor should ensure that these controls are built into the software application.

An IS auditor should perform the following when reviewing software acquisition:

- Analyze the documentation from the feasibility study to determine whether the decision to acquire a solution was appropriate (including consideration of common criteria evaluations).
- Review the RFP to ensure that it covers the items listed in this section.
- Determine whether the selected vendor is supported by RFP documentation.
- Attend agenda-based presentations and conference-room pilots to ensure that the system matches the vendor's response to the RFP.
- Ensure that the contract is reviewed by legal counsel before it is signed.
- Review the RFP to ensure that security responses are included by the vendor.
- Ensure that evidence of compliance with applicable laws, regulations or contractual requirements was obtained (e.g., through an independent auditor's report).
- Determine whether the acquisition process adhered to the internal procurement policies and procedures.

3.4 Control Identification and Design

An IS auditor must be able to identify and understand controls designed to ensure the authorization, accuracy and completeness of data input to, processing by and output from various business and computer applications. An IS auditor also must be familiar with control techniques and how each may be evidenced in the form of reports, logs and audit trails.

3.4.1 Application Controls

Application controls are controls over the input, processing and output functions. They include methods for ensuring that:

- Only complete, accurate and valid data are entered and updated in a computer system.
- Processing accomplishes the correct task.
- Processing results meet expectations.
- Data are maintained.

Application controls may consist of edit tests, totals, reconciliations and identification and reporting of incorrect, missing or exception data. Automated controls should be coupled with manual procedures to ensure proper investigation of exceptions.

These controls help ensure data accuracy, completeness, validity, verifiability and consistency, thus achieving data integrity and data reliability. Implementation of these controls helps ensure that systems maintain integrity, applicable system functions operate as intended and information contained by the system is relevant, reliable, secure and available when needed.

Input/Origination Controls

Input control procedures must ensure that every transaction to be processed is entered, processed and recorded accurately and completely. These controls should ensure that only valid and authorized information is input and these transactions are processed only once. These include machine and manual inputs. In an integrated systems environment, output generated by one system is the input for another system. Therefore, the system receiving the output of another system as input/origination must, in turn, apply edit checks, validations and access controls to those data.

Input Authorization

Input authorization verifies that all transactions have been authorized and approved by management. Authorization of input helps ensure that only authorized data are entered for processing by applications. Authorization can be performed online when the data are entered into the system. A computer-generated report listing the items requiring manual authorization may also be generated. It is important that controls exist throughout processing to ensure that the authorized data

 ©ISACA. All Rights Reserved.

remain unchanged. This can be accomplished through various accuracy and completeness checks incorporated into the application's design.

Types of authorization include:

- **Signatures on batch forms or source documents**—Provide evidence of proper authorization
- **Online access controls**—Ensure that only authorized individuals may access data or perform sensitive functions.
- **Unique passwords**—Ensure that access authorization cannot be compromised through use of another individual's authorized data access. Individual unique passwords also provide accountability for data changes and are further enhanced through strong password requirements and/or the use of multifactor authentication (MFA).
- **Terminal or client workstation identification**—Limits input to specific terminals or workstations and individuals. Terminals or client workstations in a network can be configured with a unique form of identification, such as serial number or computer name, that is authenticated by the system.
- **Source documents**—Record the data. A source document may be a piece of paper, a turnaround document or an image displayed for online data input. A well-designed source document achieves several purposes. It increases the speed and accuracy with which data can be recorded, controls work flow, facilitates preparation of the data in machine-readable form for pattern recognition devices, increases the speed and accuracy with which data can be read and facilitates subsequent reference checking.
- **Input data validation**—Ensures that information is being received in the expected format and that there is no malicious or manipulative activity taking place with inputs.

Ideally, source documents should be preprinted or electronic forms to provide consistency, accuracy and legibility. Source documents should include standard headings, titles, notes and instructions. Source document layouts should:

- Emphasize ease of use and readability.
- Group similar fields together to facilitate input.
- Provide predetermined input codes to reduce errors.
- Contain appropriate cross-reference numbers or a comparable identifier to facilitate research and tracing.
- Use boxes to prevent field size errors.
- Include an appropriate area for management to document authorization.

All source documents should be appropriately controlled. Procedures should be established to ensure that all source documents have been input and considered. Prenumbering source documents facilitates this control.

Wherever human intervention is required for input, additional user-level security controls should be considered to ensure accountability of action taken. Accountability-related controls related to data input include:

- **SoD**—Ensures that no individual has the capability of performing more than one of the following processes: origination, authorization, verification or distribution. Observation and review of job descriptions and review of authorization levels and procedures may provide information regarding the existence and enforcement of SoD.
- **Activity reports**—Provide details, by user, of activity volume and hours. Activity reports should be reviewed to ensure that activity occurs only during authorized hours of operation.
- **Violation reports**—Record any unsuccessful and unauthorized access attempts. Violation reports should indicate the terminal location, date and time of attempted access. These reports should evidence managerial review. Repeated unauthorized access violations may indicate attempts to circumvent access controls. Testing may include a review of follow-up activities.

Batch Controls and Balancing

Batch controls group input transactions to provide control totals. The batch control can be based on the following:

- **Total monetary amount**—Verification that the total monetary value of items processed equals the total monetary value of the batch documents. For example, the total monetary value of the sales invoices in the batch agrees with the total monetary value of the sales invoices processed. This provides assurance on the completeness and accuracy of the sales value processed for the batch.
- **Total items**—Verification that the total number of items included on each document in the batch agrees with the total number of items processed. For example, the total number of units ordered in the batch of invoices agrees with the total number of units processed. This provides assurance on the completeness and accuracy of the units ordered in the batch processed.
- **Total documents**—Verification that the total number of documents in the batch equals the total number of documents processed. For example, the total number

©ISACA. All Rights Reserved.

of invoices in a batch agrees with the total number of invoices processed. This provides assurance on the completeness of the number of invoices processed.
- **Hash totals**—Verification that the total in a batch agrees with the total calculated by the system. Hash total is the total of nonvalue numeric fields in the batch (e.g., total amount of dates or customer number fields), which, by themselves, do not have informative value. This provides assurance on the completeness and accuracy of data entered for the numeric fields in the batch.

Batch header forms are a data preparation control. All input forms should be clearly identified with the application name and transaction codes. Batch balancing can be performed through manual or automated reconciliation. Batch totaling must be combined with adequate follow-up procedures. Adequate controls should exist to ensure that:
- Each transaction creates an input document.
- All documents are included in a batch.
- All batches are submitted for processing.
- All batches are accepted by the computer.
- Batch reconciliation is performed.
- Procedures for the investigation and timely correction of differences are followed.
- Controls exist over the resubmission of rejected items.

Types of batch balancing include:
- **Batch registers**—Enable recording of batch totals and subsequent comparison with system reported totals
- **Control accounts**—Control account use through an initial edit file to determine batch totals. The data are then processed to the master file, and a reconciliation is performed between the totals processed during the initial edit file and the master file.
- **Computer agreement**—Compares batch header details that record the batch totals to calculated totals, either accepting or rejecting the batch

Error Reporting and Handling

Input processing requires that controls be identified to verify that only correct data are accepted into the system and input errors are recognized and corrected.

Data conversion error corrections are needed during the data conversion process. Errors can occur due to duplication of transactions and inaccurate data entry. These errors can, in turn, impact the completeness and accuracy of the data. Corrections to data should be processed through normal data conversion processes and should be verified, authorized and reentered into the system as a part of the normal processing.

Input error handling can be processed by:
- **Rejecting only transactions with errors**—Only transactions containing errors are rejected; the rest of the batch is processed.
- **Rejecting the whole batch of transactions**—Any batch containing errors is rejected for correction prior to processing.
- **Holding the batch in suspense**—Any batch containing errors is not rejected; however, the batch is held in suspense, pending correction.
- **Accepting the batch and flagging error transactions**—Any batch containing errors is processed; however, those transactions containing errors are flagged for identification, enabling subsequent error correction.

Input control techniques include the following:
- **Transaction log**—Contains a detailed list of all updates. The log can be either manually maintained or provided through automatic computer logging. A transaction log can be reconciled to the number of source documents received to verify that all transactions have been input.
- **Reconciliation of data**—Controls whether all data received are properly recorded and processed
- **Documentation**—Records (written evidence) user, data entry and data control procedures
- **Error correction procedures**—Includes:
  - Logging of errors
  - Timely corrections
  - Upstream resubmission
  - Approval of corrections
  - Suspense file
  - Error file
  - Validity of corrections
- **Anticipation**—Anticipates (user or control group) the receipt of data
- **Transmittal log**—Documents transmission or receipt of data
- **Cancellation of source documents**—Procedures to cancel source documents, such as punching with holes or marking them to avoid duplicate entry
- **Input sanitization**—Checks user input prior to storing it in a database or using it for other purposes to prevent malicious code injection

Processing Procedures and Controls

Processing procedures and controls are meant to ensure the reliability of application program processing. An IS auditor should understand the procedures and controls

that can be exercised over processing to evaluate what exposures are covered by these controls and what exposures remain.

Data Validation and Editing Procedures

Procedures should be established to ensure that input data are validated and edited as close to the time and point of origination as possible. Preprogrammed input formats ensure that data are input to the correct field in the correct format. If input procedures allow supervisor overrides of data validation and editing, automatic logging should occur. A manager who did not initiate the override should review this log. Data validation is meant to identify data errors, incomplete or missing data and inconsistencies among related data items. Front-end data editing and validation can be performed if intelligent terminals are used.

Edit controls are preventive controls that are used in a program before data are processed. If not in place or not working effectively, the preventive controls are not effective. This may cause processing of inaccurate data. **Figure 3.22** describes various types of data validation edits.

Figure 3.22—Data Validation Edits and Controls

Edits	Description
Sequence check	The control numbers follow a sequential order, and any duplicated control numbers or control numbers outside of the sequence are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The invoices on one day begin with 12001 and end with 15045. If any invoice larger than 15045 is encountered during processing, that invoice is rejected as an invalid invoice number.
Limit check	Data should not exceed a predetermined amount. For example, payroll checks should not exceed US $4,000. If a check exceeds US $4,000, the data are rejected for further verification/authorization.
Range check	Data should be within a predetermined range of values. For example, product type codes range from 100 to 250. Any code outside this range are rejected as an invalid product type.
Validity check	Programmed checking of the data validity in accordance with predetermined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, the record is rejected.
Reasonableness check	Input data are matched to predetermined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives orders for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program is designed to print the record with a warning indicating that the order appears unreasonable.
Table lookups	Input data comply with predetermined criteria maintained in a computerized table of possible values. For example, the input clerk enters a city code of 1 to 10. This number corresponds with a computerized table that matches the code to a city name.
Existence check	Data are entered correctly and agree with valid predetermined criteria. For example, a valid transaction code must be entered in the transaction code field.
Key verification	The keying process is repeated by a separate individual using a machine that compares the original keystrokes to the repeated keyed input. For example, the worker number is keyed twice and compared to verify the keying process.
Check digit	A numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect, but valid, value is not substituted. This control is effective in detecting transposition and transcription errors. For example, a check digit is added to an account number so it can be checked for accuracy when it is used.
Completeness check	A field should always contain data rather than zeros or blanks. A check of each byte of that field should be performed to determine that some form of data, not blanks or zeros, is present. For example, a worker number on a new employee record is left blank. This is identified as a key field and the record is rejected, with a request that the field be completed before the record is accepted for processing.

©ISACA. All Rights Reserved.

Figure 3.22—Data Validation Edits and Controls (cont.)

Edits	Description
Duplicate check	New transactions are matched to those previously input to ensure that they have not already been entered. For example, a vendor invoice number agrees with previously recorded invoices to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.
Logical relationship check	If a particular condition is true, then one or more additional conditions or data input relationships may be required to be true and consider the input valid. For example, the hire date of an employee may be required to be more than 16 years past their date of birth.

Processing Controls

Processing controls are meant to ensure the completeness and accuracy of accumulated data. They ensure that data in a file or database remain complete and accurate, until changed because of authorized processing or modification routines. The following are processing control techniques that can be used to address the issues of completeness and accuracy of accumulated data:

- **Manual recalculations**—Manual recalculation of a sample of transactions to ensure that processing is accomplishing the anticipated task
- **Editing**—A program instruction or subroutine that tests the accuracy, completeness and validity of data. It may be used to control input or later processing of data.
- **Run-to-run totals**—Verification of data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer were accepted and then applied to the updating process.
- **Programmed controls**—Software that detects and initiates corrective action for errors in data and processing. For example, if the incorrect file or file version is provided for processing, the application program could display messages instructing that the proper file and version be used.
- **Reasonableness verification of calculated amounts**—An application program that verifies the reasonableness of calculated amounts. The reasonableness can be tested to ensure appropriateness to predetermined criteria. Any transaction that is determined to be unreasonable may be rejected pending further review.
- **Limit checks on amounts**—Predetermined limits that ensure amounts have been keyed or calculated correctly. Any transaction exceeding the limit may be rejected for further investigation.
- **Reconciliation of file totals**—Should be performed on a routine basis. Reconciliations may be performed through the use of a manually maintained account, a file control record or an independent control file.
- **Exception reports**—Generated by a program that identifies transactions or data that appear to be incorrect. These items may be outside a predetermined range or may not conform to specified criteria.

Data File Control Procedures

File controls should ensure that only authorized processing occurs to stored data. Types of controls over data files are shown in **figure 3.23**. Contents of data files, or database tables, generally fall into one of four categories:

- **System control parameters**—The entries in these files change the workings of the system and may alter controls exercised by the system (e.g., the tolerance allowed before an exceptional transaction is reported or blocked). Any change to these files should be controlled in a similar way to program changes.
- **Standing data**—These master files include data, such as supplier/customer names and addresses, that do not frequently change and are referred to during processing. These data should be authorized before entry or maintenance. Input controls may include a report of changed data that is checked and approved. Audit trails may log all changes.
- **Master data/balance data**—Running balances and totals that are updated by transactions should not be capable of adjustment except under strict approval and review controls. Audit trails are important here because there may be financial reporting implications for the change.
- **Transaction files**—These are controlled using validation checks, control totals, exception reports, etc.

Figure 3.23—Data File Controls

Method	Description
Before and after image reporting	Computer data in a file prior to and after a transaction is processed can be recorded and reported. The before and after images make it possible to trace the impact that transactions have on computer records.
Maintenance error reporting and handling	Control procedures should be in place to ensure that all error reports are properly reconciled and corrections are submitted on a timely basis. To ensure separation of duties (SoD), error corrections should be reviewed properly and authorized by personnel who did not initiate the transaction.
Source documentation retention	Source documentation should be retained for an adequate time period to enable retrieval, reconstruction or verification of data. Policies regarding the retention of source documentation should be enforced. Originating departments should maintain copies of source documentation and ensure that only authorized personnel have access. When appropriate, source documentation should be destroyed in a secure, controlled environment.
Internal and external labeling	Internal and external labeling of removable storage media is imperative to ensure that the proper data are loaded for processing. External labels provide the basic level of assurance that the correct data medium is loaded for processing. Internal labels, including file header records, provide assurance that the proper data files are used and allow for automated checking.
Version usage	For processing to be correct, it is critical that the proper version of a file and the correct file are used. For example, transactions should be applied to the most current database, while restart procedures should use earlier versions.
Data file security	Data file security controls prevent unauthorized access by unauthorized users that may have access to the application to alter data files. These controls do not provide assurances relating to the validity of data but ensure that unauthorized users who may have access to the application cannot alter stored data improperly.
One-for-one checking	Individual documents agree with a detailed listing of documents processed by the computer. It is necessary to ensure that all documents have been received for processing.
Prerecorded input	Certain information fields are preprinted on blank input forms to reduce initial input errors.
Transaction logs	All transaction input activity is recorded by the computer. A detailed listing, including date of input, time of input, user ID and terminal location, can then be generated to provide an audit trail. It also permits operations personnel to determine which transactions have been posted. This will help to decrease the research time needed to investigate exceptions and decrease recovery time if a system failure occurs.
File updating and maintenance authorization	Proper authorization for file updating and maintenance is necessary to ensure that stored data are correct, up to date and safeguarded adequately. Application programs may contain access restrictions in addition to the overall system access restrictions. The additional security may provide levels of authorization and an audit trail of file maintenance.
Parity checking	Data transfers in a computer system are expected to be made in a relatively error-free environment. However, when programs or vital data are transmitted, additional controls are needed. Transmission errors are controlled primarily by error-detecting or correcting codes. The former is used more often because error-correcting codes are costly to implement and are unable to correct all errors. Generally, error detection methods such as a check bit and redundant transmission are adequate. Redundancy checking is a common error-detection routine. A transmitted block of data containing one or more records or messages is checked for the number of characters or patterns of bits contained in it. If the numbers or patterns do not conform to predetermined parameters, the receiving device ignores the transmitted data and instructs the user to retransmit. Check bits are often added to the transmitted data by the telecommunications control unit and may be applied either horizontally or vertically. These checks are similar to the parity checks normally applied to data characters within on-premises equipment. A parity check on a single character generally is referred to as a vertical or column check, and a parity check on all the equivalent bits is known as a horizontal, longitudinal or row check. Use of both checks greatly improves the possibilities of detecting a transmission error, which may be missed when either of those checks is used alone.

©ISACA. All Rights Reserved.

The controls built into an application represent the management design of controls on how a business process should be run. While an application contains the rules for the business, the data that are the outcome of the processing are stored in the database. An entity may have the best controls built into the application, but if management personnel directly update data in the database, then the benefit of the best controls in the application will be overridden.

However, in some situations, enterprises may have to carry out direct updates to a database. For example, if, due to a systems outage, transactions cannot be processed in real time, it is not practical to insist that the backlog should be entered through the application (front end) when the system becomes available, before the transactions of the subsequent days are entered or processed. In such cases, management may decide to directly update the backlog transactions in the database (back end).

An IS auditor should ensure that there are controls in place to ensure that such direct back-end data fixes are supported by authorization of the business for completeness and accuracy and are processed subject to computer operations controls. The important point to remember is that, in any enterprise, the quality of application controls is only as good as the quality of controls around direct back-end data fixes.

3.4.2 Output Controls

Output controls provide assurance that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner.

Output controls include:

- **Logging and storage of negotiable, sensitive and critical forms in a secure place**—Negotiable, sensitive or critical forms should be properly logged and secured to provide adequate safeguards against theft, damage or disclosure. The form log should be routinely reconciled to have inventory on hand and any discrepancies should be properly researched.
- **Computer generation of negotiable instruments, forms and signatures**—The computer generation of negotiable instruments, forms and signatures should be properly controlled. A detailed listing of generated forms should be compared to the physical forms received. One should properly account for all exceptions, rejections and mutilations.
- **Report accuracy, completeness and timeliness**—Often reports are generated using third-party data analysis and reporting applications (e.g., Essbase). Even with the most reliable and accurate data sources, improperly configured, constructed and prepared reports are still a significant risk. Report design and generation specifications, templates and creation/change request processes are critical system output controls.
- **Reports generated from the system**—These represent the data that management relies on for business decisions and review of business results. Therefore, ensuring the integrity of data in reports is key for the reliability of information in information systems. An IS auditor should validate that the reports are accurate and provide correct representation of the source data.

IS auditors need to apply an assessment approach in validating reports depending on the situation (more evaluation is required when the organization has undergone a system change or when evaluating customized reports against standard reports of a widely used application). Methods to validate reports include the following:

- **Report distribution**—Output reports should be distributed according to authorized distribution parameters. Operations personnel should verify that reports are complete and delivered according to schedule. All reports should be logged prior to distribution. In most environments, processing output is spooled to a buffer or print spool on completion of job processing, where it waits for an available printer. Controls over access to the print spools are important to prevent reports from being deleted accidentally from print spools or directed to a different printer. In addition, changes to the output print priority can delay printing of critical jobs. Access to distributed reports can compromise confidentiality; therefore, physical distribution of reports should be controlled adequately. Reports containing sensitive data should be printed under secure, controlled conditions. Secure output drop-off points should be established. Output disposal should also be secured to ensure that no unauthorized access can occur. Electronic distribution should also be considered, and logical access controls should be put in place.
- **Balancing and reconciling**—Data processing application program output should be balanced routinely to the control totals. Audit trails should be provided to facilitate the tracking of transaction processing and the reconciliation of data.
- **Output error handling**—Procedures for reporting and controlling errors contained in the application program output should be established. The error report should be timely and delivered to the

originating department for review and error correction.

- **Output report retention**—A record retention schedule should be adhered to firmly. Any governing legal regulations should be included in the retention policy.
- **Verification of receipt of reports**—To provide assurance that sensitive reports are properly distributed, the recipient should sign a log as evidence of receipt of output.

An IS auditor should be aware of existing concerns regarding record-retention policies for the enterprise and address legal requirements. Output can be restricted to particular IT resources or devices (e.g., a particular printer).

©ISACA. All Rights Reserved.

Page intentionally left blank

Part B: Information Systems Implementation

IS implementation is when the system is installed and moved into the production environment after appropriate system and users' acceptance testing. This is the stage at which:

- End users are notified and trained.
- System testing occurs.
- Data entry or conversions occur.
- Postimplementation reviews occur.

3.5 System Readiness and Implementation Testing

Integral to IS implementation is the proper selection of testing methodologies, the development of testing plans fully traceable to requirements and the acquisition of essential resources to successfully complete testing. Once completed, testing provides confidence to stakeholders that a system or system component operates as intended and delivers the benefits realization as required at the start of a project.

An IS auditor should understand the application of various forms of testing. An IS auditor should also understand how QA monitoring and evaluation contribute to the quality of an organization's internal processes (e.g., project management, software development process or IT service) and the quality of the final products produced by these processes (e.g., the system implemented or software developed).

Testing is an essential part of the systems development process that verifies and validates that a program, subsystem or application performs the functions for which it has been designed. Testing also determines whether the units being tested operate without any malfunction or adverse effect on other components of the system.

The variety of systems development methodologies and organizational requirements provide for a large range of testing schemes or levels. Each set of tests is performed with a different set of data and under the responsibility of different people or functions. An IS auditor plays a preventive or detective role in the testing process.

3.5.1 Testing Classifications

The following tests relate, to varying degrees, to the approaches that can be performed based on the size and complexity of the modified system:

- **Unit testing**—The testing of an individual program or module. Unit testing uses a set of test cases that focus on the control structure of the procedural design. These tests ensure that the internal operation of the program performs according to specification.
- **Interface or integration testing**—A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure dictated by design. The term integration testing is also used to refer to tests that verify and validate the functioning of the application under test with other systems, in which a set of data is transferred from one system to another.
- **System testing**—A series of tests designed to ensure that modified programs, objects, database schema, etc., which collectively constitute a new or modified system, function properly. These test procedures are often performed in a nonproduction test/development environment by software developers designated as a test team. The following specific analyses may be carried out during system testing:
  - **Recovery testing**—Checking the system's ability to recover after a software or hardware failure
  - **Security testing**—Making sure the modified/new system includes provisions for appropriate access controls and does not introduce any security holes that might compromise other systems
  - **Load testing**—Testing an application with large quantities of data to evaluate its performance during peak hours
  - **Volume testing**—Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records (data) that the application can process
  - **Stress testing**—Studying the impact on the application by testing, with an incremental number of concurrent users/services on the application, to determine the maximum number of concurrent users/services that the application can process
  - **Performance testing**—Comparing the system performance to other equivalent systems using well-defined benchmarks
- **Final acceptance testing**—Performed after the system staff is satisfied with the system tests. Acceptance testing occurs during the implementation phase. During this testing phase, the defined methods

©ISACA. All Rights Reserved.

of testing to apply should be incorporated into the enterprise's QA methodology. QA activities should proactively encourage adequate levels of testing to be performed on all software development projects. Final acceptance testing has two major parts: quality assurance testing (QAT), focusing on technical aspects of the application, and UAT, focusing on functional aspects of the application. QAT and UAT have different objectives and, therefore, should not be combined.

QAT focuses on the documented specifications and the technology employed. It verifies that the application works as documented by testing the logical design and the technology itself. It also ensures that the application meets the documented technical specifications and deliverables. QAT is performed primarily by the IT department. The participation of the end user is minimal and on request. QAT does not focus on functionality testing.

UAT supports the process of ensuring that the system is production ready and satisfies all documented requirements. The methods include:

- Definition of test strategies and procedures
- Design of test cases and scenarios
- Execution of the tests
- Use of the results to verify system readiness

Acceptance criteria are defined elements that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should use the system in a manner as close to production as possible. For example, tests may be based around typical, predefined business process scenarios. If a new business process has been developed to accommodate the new or modified system, it should also be tested at this point. A key aspect of testing should also include testers seeking to verify that supporting processes integrate into the application in an acceptable fashion. Successful completion generally enables a project team to hand over a complete integrated package of application and supporting procedures.

Ideally, UAT should be performed in a secure testing or staging environment. A secure testing environment, in which both source code and executable code are protected, helps to ensure that unauthorized or last-minute changes are not made to the system without going through the standard system maintenance process. The nature and extent of the tests will be dependent on the magnitude and complexity of the system change.

Although acquired systems are tested by the vendor prior to distribution, these systems and any subsequent changes should be tested thoroughly by the end user and the system maintenance staff. These supplemental tests help ensure that programs function as designed by the vendor and the changes do not interact adversely with existing systems. In the case of acquired software, after attending to the changes during testing by the vendor, the accepted version should be controlled and used for implementation. In the absence of controls, the risk of introducing malicious patches/Trojan horse programs is very high.

Some enterprises rely on integrated test facilities (ITFs). Test data usually are processed in production-like systems. This confirms the behavior of the new application or modules in real-life conditions. These conditions include peak volume and other resource-related constraints. In this environment, IS performs tests with a set of fictitious data whereas client representatives use extracts of production data to cover the most possible scenarios and some fictitious data for scenarios that would not be tested by the production data. In some enterprises that use a subset of production data in a test environment, such production data may be altered to scramble the data so that the confidential nature of the data is obscured from the tester. This is often the case when the acceptance testing is done by team members who, under usual circumstances, would not have access to such production data.

After acceptance testing is complete, certification and accreditation processes are performed. These should be done after the system has been implemented and in operation for enough time to produce the evidence needed for these processes. This includes evaluating program documentation and testing effectiveness and results in a final decision for deploying the business application system. For information security issues, the evaluation process includes reviewing security plans, the risk assessments performed and test plans, and results in an assessment of the effectiveness of the security controls and processes to be deployed. Generally involving security staff and the business owner of the application, this process provides some degree of accountability to the business owner regarding the state of the system that they will accept for deployment. See section 3.7.5 Certification/Accreditation for more information.

When the tests are completed, an IS auditor should issue an opinion to management as to whether the system meets the business requirements, has implemented appropriate controls and is ready to be migrated to production. This report should specify the deficiencies

in the system that need to be corrected and should identify and explain the risk that the enterprise is taking by implementing the new system. See section 5.12.6 Security Testing Techniques for more information.

Other Types of Testing

Other types of testing include the following:

- **Alpha and beta testing**—The two phases of testing that software undergoes before being considered finished. The first stage, called alpha testing, is often performed only by users within the enterprise who are developing the software (i.e., systems testing). The second stage, called beta testing, a form of UAT, generally involves a limited number of external users. This involves real-world exposure, sending the beta version of the product to independent test sites or offering it free to interested users.
- **Pilot testing**—A preliminary test that focuses on specific and predetermined aspects of a system. It is not meant to replace other testing methods, but to provide a limited evaluation of the system. POCs are early pilot tests—usually over interim platforms and with only basic functionalities.
- **White box testing**—A test that assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic paths (i.e., applicable to unit and integration testing). However, testing all possible logic paths in large information systems is not feasible and would be cost prohibitive; therefore, white box testing is used on a select basis only.
- **Black box testing**—An integrity-based form of testing associated with testing components of an information system's functional operating effectiveness without regard to any specific internal program structure. It is applicable to integration (interface) and UAT processes.
- **Function/validation testing**—Similar to system testing but often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements (i.e., Are we building the right product?).
- **Regression testing**—The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be the same as the data used in the original.
- **Parallel testing**—The process of feeding test data into two systems—the modified system and an alternative system (possibly the original system)—and comparing the results. The purpose of parallel testing is to determine whether the new application performs in the same way as the original system and meets end-user requirements.
- **Sociability testing**—Tests to confirm that the new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems and, in a client server or web development, those that perform changes to the desktop environment.

3.5.2 Software Testing

Test plans identify the specific portions of the system to be tested and may include a categorization of types of deficiencies that can be found during the test. Categories of such deficiencies may be system defects, incomplete requirements, designs, specifications or errors in the test case itself. Test plans also specify severity levels of problems found and guidelines on identifying the business priority. The tester determines the severity of the problem found during testing. Based on the severity level, the problem may be fixed prior to implementation or may be noted for correction following implementation. The project sponsor, end-user management and the project manager decide early in the test phase on the severity definitions.

Test plans also identify test approaches, such as the following two reciprocal approaches, to software testing:

- **Bottom up**—Testing begins with atomic units, such as programs or modules, and works upward until a complete system testing has taken place. The advantages include:
  - There is no need for stubs or drivers.
  - Testing can be started before all programs are complete.
  - Errors in critical modules are found early.
- **Top down**—Testing follows the opposite path, either in depth-first or breadth-first search order. The advantages include:
  - Tests of major functions and processing are conducted early.
  - Interface errors can be detected sooner.
  - Confidence in the system is increased because programmers and users see a working system.

Generally, most application testing of large systems follows a bottom-up testing approach that involves

©ISACA. All Rights Reserved.

ascending levels of integration and testing (e.g., unit or program, subsystem/integration, system):

- **Conduct and report test results**—Describe resources implied in testing, including personnel involved and information resources/facilities used during the test and actual versus expected test results. Results reported and the test plan should be retained as part of the system's permanent documentation.
- **Address outstanding issues**—Identify errors and irregularities from the actual tests conducted. When such problems occur, the specific tests in question must be redesigned in the test plan until acceptable conditions occur when the tests are redone.

3.5.3 Data Integrity Testing

Data integrity testing is a set of substantive tests that examines accuracy, completeness, consistency and authorization of data presently held in a system. It employs testing similar to that used for input control. Data integrity tests indicate failures in input or processing controls. Controls for ensuring the integrity of accumulated data in a file can be exercised by regularly checking data in the file. When this checking is done against authorized source documentation, it is common to check only a portion of the file at a time. Because the whole file is regularly checked in cycles, the control technique is often referred to as cyclical checking.

Two common types of data integrity tests are relational and referential integrity tests:

- **Relational integrity tests**—Performed at the data element and record-based levels. Relational integrity is enforced through data validation routines built into the application or by defining the input condition constraints and data characteristics at the table definition in the database stage. Sometimes it is a combination of both.
- **Referential integrity tests**—Define existence relationships between entities in different tables of a database that needs to be maintained by the DBMS. It is required for maintaining interrelation integrity in the relational data model. Whenever two or more relations are related through referential constraints (primary and foreign key), it is necessary that references be kept consistent in the event of insertions, deletions and updates to these relations. Database software generally provides various built-in automated procedures for checking and ensuring referential integrity. Referential integrity checks involve ensuring that all references to a primary key from another table (i.e., a foreign key) exist in their original table. In nonpointer databases (e.g., relational), referential integrity checks involve making sure that all foreign keys exist in their original table.

Data Integrity in Online Transaction Processing Systems

In multiuser transaction systems, it is necessary to manage parallel user access to stored data typically controlled by a DBMS and deliver fault tolerance. Of particular importance are four online data integrity requirements known collectively as the ACID principle:

- **Atomicity**—From a user perspective, a transaction is either completed in its entirety (i.e., all relevant database tables are updated) or not at all. If an error or interruption occurs, all changes made up to that point are backed out.
- **Consistency**—All integrity conditions in the database are maintained with each transaction, taking the database from one consistent state into another consistent state.
- **Isolation**—Each transaction is isolated from other transactions, so each transaction accesses only data that are part of a consistent database state.
- **Durability**—If a transaction has been reported back to a user as complete, the resulting changes to the database survive subsequent hardware or software failures.

3.5.4 Application Systems Testing

Testing the effectiveness of application controls involves analyzing computer application programs, testing computer application program controls or selecting and monitoring data process transactions. Testing controls by applying appropriate audit procedures is important to ensure their functionality and effectiveness. Methods and techniques for each category are described in **figure 3.24**.

 ©ISACA. All Rights Reserved.

Figure 3.24—Testing Application Systems

Technique	Description	Advantages	Disadvantages
Snapshot	Records flow of designated transactions through logic paths within programs	Verifies program logic	Requires extensive knowledge of the information systems (IS) environment
Mapping	Identifies specific program logic that has not been tested and analyzes programs during execution to indicate whether program statements have been executed	• Increases efficiency by identifying unused code • Identifies potential exposures	Cost of software
Tracing and tagging	• Tracing shows the trail of instructions executed during an application. • Tagging involves placing an indicator on selected transactions at input and using tracing to track them.	Provides an exact picture of sequence of events, and is effective with live and simulated transactions	Requires extensive amounts of computer time, an intimate knowledge of the application program and additional programming to execute trace routines
Test data/deck	Simulates transactions through real programs	• Copies of the actual master files or dummy data may be used as test data • Source code review is unnecessary • Can be used on a surprise basis • Provides objective review and verification of program controls and edits • Initial use can be limited to specific program functions minimizing scope and complexity • Requires minimal knowledge of the IS environment	• Difficult to ensure that the proper program is checked • Risk of not including all transaction scenarios • Requires good knowledge of application systems • Does not test the actual master file and master file records
Base-case system evaluation	• Uses test data sets developed as part of a comprehensive testing of programs • Verifies correct system operations before acceptance and periodic revalidation	Comprehensive testing verification and compliance testing	• Extensive effort to maintain data sets • Close cooperation required among all parties
Parallel operation	Processes production data through existing and newly developed programs at the same time, compares results and verifies changed production prior to replacing existing procedures	Verifies new system before discontinuing the old one	Added processing costs
Integrated testing facility	Creates a fictitious file in the database with test transactions processed simultaneously with live data	Periodic testing does not require separate test process.	• Needs careful planning • Test data must be isolated from production data

©ISACA. All Rights Reserved.

Figure 3.24—Testing Application Systems (cont.)

Technique	Description	Advantages	Disadvantages
Parallel simulation	Processes production data using computer programs that simulate application program logic	Eliminates need to prepare test data	Programs must be developed
Transaction selection programs	Use audit software to screen and select transactions input to the regular production cycle	• Independent of production system • Controlled by the auditor • Requires no modification to production systems	Cost of development and maintenance
Embedded audit data collection	Software embedded in host computer applications screens. It selects input transactions and generates transactions during production. Usually, it is developed as part of system development. Types include: • **Systems control audit review file (SCARF)** – Auditor determines reasonableness of tests incorporated into normal processing. It provides information for further review. • **Sample audit review file (SARF)** – Randomly selects transactions to provide representative file for analysis	Provides sampling and productions statistics	• High cost of development and maintenance • Auditor independence issues
Extended records	Gathers all data that have been affected by a particular program	Records are put into one convenient file.	Adds to data storage costs and overhead, and to system development costs

To facilitate the evaluation of application system tests, an IS auditor may want to use generalized audit software (GAS). This is particularly useful when specific application control weaknesses are discovered (e.g., ones that affect updates to master file records and certain error conditions on specific transaction records). Additionally, GAS can be used to perform certain application control tests, such as parallel simulation, in comparing expected outcomes to live data.

Automated Application Testing

Test data generators can be used to systematically generate random data that can be used to test programs. The generators work by using the field characteristics, layout and values of the data. In addition to test data generators, there are interactive debugging aids and code logic analyzers available to assist in the testing activities.

IS Auditor's Role in Information Systems Testing

Testing is crucial in determining that user requirements have been validated, the system is performing as anticipated and internal controls work as intended. Therefore, it is essential that an IS auditor be involved in reviewing this phase and perform the following:

- Review the test plan for completeness; indicate evidence of user participation, such as user development of test scenarios and/or user sign-off of results; and consider rerunning critical tests.
- Reconcile control totals and converted data.
- Review error reports for their precision in recognizing erroneous data and resolution of errors.
- Verify cyclical processing for correctness (month-end, year-end processing, etc.).
- Verify accuracy of critical reports and output used by management and other stakeholders.

 ©ISACA. All Rights Reserved.

- Interview end users of the system for their understanding of new methods, procedures and operating instructions.
- Review system and end-user documentation to determine its completeness and verify its accuracy during the test phase.
- Review parallel testing results for accuracy.
- Verify that system security is functioning as designed by developing and executing access tests.
- Review unit and system test plans to determine whether tests for internal controls are planned and performed.
- Review the UAT and ensure that the accepted software has been delivered to the implementation team. The vendor should not be able to replace this version.
- Review procedures used for recording and following through on error reports.

3.5.5 System Implementation

Implementation is initiated only after a successful testing phase. The system should be installed according to the enterprise's change control procedures.

An IS auditor should verify that appropriate signoffs have been obtained prior to implementation and perform the following:

- Review the programmed procedures used for scheduling and running the system and system parameters used in executing the production schedule.
- Review all system documentation to ensure its completeness and confirm that all recent updates from the testing phase have been incorporated.
- Verify all data conversions to ensure that they are correct and complete before implementing the system in production.

Implementation Planning

After it is developed and ready for operation, the new system delivered by the project will need an efficient support structure. It is not enough to set up roles for a support structure and name people to fulfill these roles. Support personnel will need to acquire new skills. The workload has to be distributed such that the right people support the right issues; thus, new processes have to be developed while respecting the specificities of IT department requirements. Additionally, an infrastructure dedicated to support staff has to be made available. For these and other reasons, setting up a support structure normally is a project in itself and requires planning, a methodology and good practices adaptation from past experiences.

The objective of such a project is to develop and establish the support structure that will exist for the new technical infrastructure. The main goals are to accomplish the following:

- Provide appropriate support structures for first-, second- and third-line support teams.
- Provide a single point of contact.
- Provide roles and skills definitions with applicable training plans.

Often the project sponsor's organization operates and supports a legacy solution and will implement a new system environment based on new system architecture. The existing support procedures and the organizational units will have to maintain the future system to provide the appropriate level of support for the new platform and for the old one.

To achieve significant success in updating staff on changes to the business process and introducing new software, it is necessary to address some important questions, such as:

- How can the existing support staff be involved in the setup of the new project without neglecting the currently running system?
- What is the gap of knowledge/skills that must be addressed in the training plan?
- How large is the difference between the current legacy environment operation and the operation of the new platform?

Generally, a transition project should conform to the following guidelines:

- There should be a smooth transition from the existing platform to the new platform, without any negative effect on users of the system.
- There should be maximum employment of the existing support staff to operate the new system environment and keep the effort of new hires at a minimum level.

A primary challenge is to manage the phases from build to integrate, to migrate and for the phasing-out of the existing system and the phasing-in of the new one. The migration cannot be accomplished via a single event. Instead, a step-by-step transition of the affected services must take place. Further, the implemented processes for a legacy environment might be different from what may be implemented with the new platform and any changes must be communicated to users and system support staff.

©ISACA. All Rights Reserved.

Implementation Plan/Knowledge Transfer Plan

In accordance with good practices, the transfer should follow the shadowing and relay-baton method. Shadowing gives staff the opportunity to become accustomed to the system by observation. The relay-baton approach is the most suitable concept to transfer knowledge and responsibility in a transparent way. The metaphor of the relay-baton expresses exactly what must be achieved (i.e., knowledge is transferred in small portions).

Training Plan

After the roles and responsibilities are defined, they will be documented in the form of a chart to allow for a clear and easy-to-read overview.

For example, a staff training plan should show all of the required training in terms of:

- Content
- Scheduling information
- Duration
- Delivery mechanism (classroom and/or web-based)
- Train-the-trainer concept

The plan should consider the role definitions and skill profiles for the new to-be structure and the results of the gap analysis. The plan considers that the staff who need to be trained must still run the current system, so that detailed coordination with the daily business tasks is maintained.

The following list gives an example of work tasks defined to fulfill the overall project goal:

- Collate existing support structure documentation.
- Review the existing IT organization model.
- Define the new support organization structure.
- Define the new support processes.
- Map the new process to the organization model.
- Execute the new organization model.
- Establish support functions.
- Develop communications material for support staff.
- Conduct briefing and training sessions.
- Review mobilization progress.
- Transfer to the new organization structure.
- Review the preceding items.

3.6 Implementation Configuration and Release Management

The effective and efficient development and maintenance of complicated IT systems requires that rigorous configuration, change and release management processes be implemented and adhered to within an enterprise.

These processes provide systematic, consistent and unambiguous control on attributes of IT components comprising the system (hardware, software, firmware and network connectivity, including physical connecting media wire, fiber and radio frequency). Knowledge of the configuration status of computing environments is critical to system reliability, availability and security and achieving timely maintenance of these systems. Changes to IT systems must be carefully assessed, planned, tested, approved, documented and communicated to minimize any undesirable consequences to the business processes.

An IS auditor should be aware of the tools available for managing configuration, change and release management and of the controls in place to ensure SoD between development staff and the production environment. Tools for managing configuration, change and release management include ManageEngine Service Desk, SysAid and ServiceNow.

3.6.1 Configuration Management Systems

Because of the difficulties associated with exercising control over system and programming maintenance activities, more enterprises are implementing configuration management systems. In many cases, regulatory requirements mandate these levels of control to provide a high degree of reliability and repeatability in all associated system processes. In a configuration management system, maintenance requests must be formally documented and approved by a change control group (e.g., configuration control boards). In addition, careful control is exercised over each stage of the maintenance process via checkpoints, reviews and sign-off procedures.

Configuration management involves procedures throughout the system hardware and software life cycle (from requirements analysis to maintenance) to identify, define and baseline software items in the system and provide a basis for problem management, change management and release management. This process is usually facilitated with a configuration management database (CMDB), which documents information on the hardware and software assets within the organization.

The process of checking out prevents or manages simultaneous code edits, with hardware, network and system architects reviewing and approving the changes or updates to the hardware asset and inventory tracking systems.

Checking in is the process of moving an item to the controlled environment. When a change is required (and

 ©ISACA. All Rights Reserved.

supported by a change control form), the configuration manager checks out the item. After the change is made, it can be checked using a different version number. The process of checking out also prevents or manages simultaneous code edits. With hardware, network and system architects review and approve the changes or updates to both the hardware asset and the inventory tracking systems.

For configuration management to work, management support is critical. The configuration management process is implemented by developing and following a configuration management plan and operating procedures. This plan should not be limited to just the software developed but should also include all system documentation, test plans and procedures.

Commercial software products are often used to automate some processes. Such tools should allow control to be maintained for applications software from the outset of system analysis and design to running live. Configuration management tools support change management and release management through the:

1. Identification of items affected by a proposed change to assist with impact assessment (functional, operational and security)
2. Recording of configuration items affected by authorized changes
3. Implementation of changes in accordance with authorization records
4. Registering of configuration item changes when authorized changes and releases are implemented
5. Recording of baselines that are related to releases (with known consequences) to which an enterprise would revert if an implemented change fails
6. Preparing a release to avoid human errors and resource costs

A new version of the system (or builds) should be built only from the baselined items. The baseline becomes the trusted recovery source for these systems and applications. These baselines should be built or based on industry recognized sources or benchmarks. For example, the Center for Internet Security (CIS) provides benchmarks that are configuration baselines and practices to configure a system securely. It is important to use baselines not only for recovery but also to ensure that systems are implemented with the least amount of functionality necessary so as not to introduce unnecessary vulnerabilities into the environment.

From an IS audit perspective, effective use of configuration management software provides important evidence of management's commitment to careful control over the maintenance process.

3.7 System Migration, Infrastructure Deployment and Data Conversion

New software applications tend to be more comprehensive and integrated than older applications. Furthermore, enterprises rely increasingly on data warehouses, models and simulation for decision making; thus, importing data from old (and legacy) systems into the new application is crucial. Data format, coding, structure and integrity are to be preserved or properly translated. A migration scenario must be set up and a rollback plan needs to be in place. There are many direct (old to new application) and indirect (using interim repositories) strategies and tools. Data conversion is a one-time task in many development projects. The importance of correct results is critical, and success depends on the use of good practices by the development team because the programmed input checks under development will not be available for the conversion. Source data must be correctly characterized, and the destination database must accommodate all existing data values. Resulting data should be carefully tested. Steps for the conversion that are developed in the test environment must be recorded so they can be repeated on the production system.

An IS auditor should ensure that any tools and techniques selected for the process are adequate and appropriate, data conversion achieves the necessary objectives without data loss or corruption and any loss of data is minimal and formally accepted by user management.

3.7.1 Data Migration

A data conversion (also known as data porting) is required if the source and target systems use different field formats or sizes, file/database structures or coding schemes. For example, a number may be stored as text, floating point or binary-coded decimal.

Conversions are often necessary when the source and target systems are on different hardware and/or OS platforms, and different file or database structures (e.g., relational database, flat files, or virtual storage access method) are used.

The objective of data conversion is to convert existing data into the new required format, coding and structure while preserving the meaning and integrity of the data. The data conversion process must provide some means, such as audit trails and logs, to allow for the verification

©ISACA. All Rights Reserved.

of the accuracy and completeness of the converted data. This verification of accuracy and completeness may be performed through a combination of manual processes, system utilities, vendor tools and one-time-use special applications.

A large-scale data conversion can potentially become a project within a project because considerable analysis, design and planning will be required. Among the steps necessary for a successful data conversion are:

- Determining which data should be converted using programs and which data, if any, should be converted manually
- Performing any necessary data cleansing ahead of conversion
- Identifying the methods to be used to verify the conversion, such as automated file comparisons, comparing record counts and control totals, accounting balances and individual data items on a sample basis
- Establishing the parameters for a successful conversion (e.g., Is 100-percent consistency between the old and new systems necessary, or will some differences within defined ranges be acceptable?)
- Scheduling the sequence of conversion tasks
- Designing audit trail reports to document the conversion, including data mappings and transformations
- Designing exception reports to record any items that cannot be converted automatically
- Establishing responsibility for verifying and signing off on individual conversion steps and accepting the overall conversion
- Developing and testing conversion programs, including functionality and performance
- Performing one or more conversion dress rehearsals to familiarize personnel with the sequence of events and their roles, and testing the conversion process end to end with real data
- Controlling the outsourcing of the conversion process with a proper agreement covering nondisclosure, data privacy, data destruction and other warranties
- Running the actual conversion with all necessary personnel onsite or able to be contacted

A successful data migration delivers the new system on time, on budget and with the required quality. The data migration project should be carefully planned and use appropriate methodologies and tools to minimize the risk of:

- Disruption of routine operations
- Violation of the security and confidentiality of data
- Conflicts and contention between legacy and migrated operations
- Data inconsistencies and loss of data integrity during the migration process

The data model and the new application model should be stored in an enterprise repository. Using a repository allows a simulation of the migration scenario and traceability during the project. An enterprise repository enables an overview of the reengineering and data migration process (e.g., which modules and entities are in which stage, such as in service or already migrated). These models will be modified in the course of the processes described in the following sections.

Refining the Migration Scenario

To determine the scope of the implementation project, module analysis should be undertaken to identify the affected functional modules and data entities. The plan for the implementation project should be refined based on this information and an analysis of business requirements.

The next step is to develop a migration plan. This is a detailed listing of tasks for the production deployment of a new system. Within this plan, decision points are defined to make go or no-go decisions. The following processes require decision points:

- **Support migration process**—A support process to administer the enterprise repository must be implemented. Because this repository should be used after completion of the project to manage the software components of the new architecture, this process should be capable of supporting future development processes. The enterprise repository administration and report generation support the migration by supporting the reverse engineering of changes in the legacy architecture and facilitating the creation of impact analysis reports.
- **Migration infrastructure**—The project develops specifications for the infrastructure of the migration project. This approach ensures consistency and increases confidence in the functionality of the fallback scenario. The migration project team completes a high-level analysis of the legacy and new data models to establish links between them that will be refined later. The migration infrastructure is the basis for specifying the following components:
  - **Data redirector (temporary adapters)**—Good practices suggest the staged deployment of applications to minimize the end-user impact of their implementation and limit the risk by having a fallback scenario with minimum impact.

 ©ISACA. All Rights Reserved.

For this reason, an infrastructure component is needed to handle distributed data on different platforms within distributed applications. The design of a data redirector on the new architecture corresponds to service-oriented architectures and should cover features such as access to the not-yet-migrated legacy data during run time, data consistency due to the usage of standards such as Open Group for Unix Systems eXtended Architecture (X/Open XA) interface and a homogeneous new architecture.

- **Data conversion components**—The need to create an enterprise data model to eliminate data redundancies and inconsistencies often is identified. For this reason, infrastructure components to transform the legacy data model to the new data model must be provided. These components can be described as follows:
  - Unload components to copy the data (either as is or suitably modified to align with the data format of the target system) in legacy databases that have been identified for migration
  - Transfer components to execute the data transfer from the legacy system to the new system
  - Load components to execute the load of the data into the new database

Software packages that support data migration, such as ERP and document management software, should be acquired as soon as the software evaluation is done. The data conversion plan should be based on the available databases and migration tools provided by the selected vendor(s).

The decision on which method to use for data conversion has to be made as part of the implementation project and should be based on transaction volume and change degree of the data model.

Fallback (Rollback) Scenario

Not all new system deployments go as planned. To mitigate the risk of downtime for mission-critical systems, good practices dictate that the tools and applications required to reverse the migration are available prior to attempting the production cutover. Some or all of these tools and applications may need to be developed as part of the project.

Components have to be delivered that can back out all changes and restore data to the original applications in case of nonfunctioning new applications. Two types of components should be considered as part of a fallback contingency plan.

The first component consists of:

- Unload components to execute the unloading of the data from the new data structures
- Transfer components for the data conversion
- Load components to execute the loading of the data into the legacy data structures

The second component consists of:

- A log component to log the data modifications within the new data model during runtime within the service layer
- Transfer components for the data conversion
- Load components to execute the load of the data into the legacy data structures

Another important consideration is the new system's data structure. This can be determined by reading the software user guides, analyzing the ERDs, understanding the relationships between data elements and reviewing definitions of key terms (e.g., entity and record) in the new system.

Next, it is important to review the decisions on how business processes should be conducted in the new system. Changes are identified, and the output of this exercise is a table of new data terminology against current definitions of data elements. In this step, the project team identifies how current data are defined in the new system. Following this step, a data cleanup is completed to eliminate inconsistencies in the current database, if possible, and duplications of data sets are discovered and resolved. The rules of conversion are defined and documented, with the objective of ensuring that the business processes executed in the new system yield results that maintain data integrity and relationships.

Data conversion rules are programmed by the software development team. Data conversion scripts are created to convert the data from the old database to the new database. These are tested on a discrete selection of data that are carefully selected to include all cases. This process is referred to as program or unit testing. Following the sign-off of data conversion scripts by programmers, the scripts are run on a test copy of the production database. The values of data are verified by executing assessments including business process tests. Users and developers complete cycles of testing until conversion scripts are fine tuned. After testing has been completed, the next step is to promote the converted database to production.

The key points to be taken into consideration in a data conversion project are to ensure:

- Completeness of data conversion

©ISACA. All Rights Reserved.

- Integrity of data
- Storage and security of data under conversion
- Consistency of data
- Continuity of data access

The last copy of the data before conversion from the old platform and the first copy of the data after conversion to the new platform should be maintained separately in the archive for any future reference.

3.7.2 Changeover (Go-Live or Cutover) Techniques

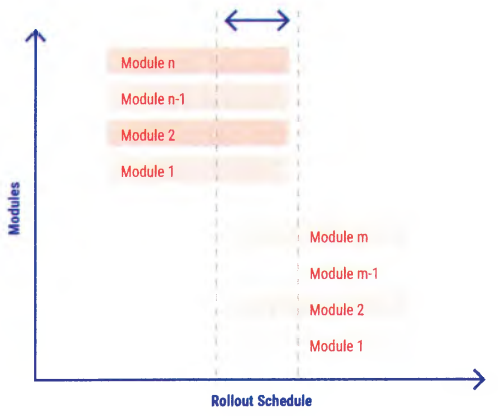
Changeover refers to an approach to shift users from using the application from the existing (old) system to the replacement (new) system. This is appropriate only after testing the new system with respect to its program and relevant data. Changeover is sometimes called the go-live technique because it enables the start of the new system. This approach is also called the cutover technique because it helps in cutting out from the older system and moving over to the newer system.

This technique can be achieved in three different ways.

Parallel Changeover

This technique includes running the old system, then running both the old and new systems in parallel and, finally, fully changing over to the new system after gaining confidence in the working of the new system. With this approach, the users must use both systems during the period of overlap. This minimizes the risk of using the newer system and, at the same time, helps in identifying problems, issues or concerns that the user comes across in the newer system in the beginning. After a period of overlap, the user gains confidence and assurance in relying on the newer system. At this point, the use of the older system is discontinued and the new system becomes totally operational. Note in **figure 3.25** that the number (m and n, respectively) of modules in the new and old systems may be different.

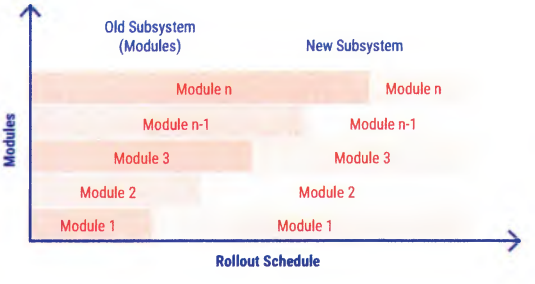
Figure 3.25—Parallel Changeover



Phased Changeover

In this approach, the older system is broken into deliverable modules. Initially, the first module of the older system is phased out using the first module of the newer system. Then, the second module of the older system is phased out using the second module of the newer system, and so forth until reaching the last module. Thus, the changeover from the older system to the newer system takes place in a preplanned, phased manner. See **figure 3.26**.

Figure 3.26—Phased Changeover



Some of the risk that may exist in the phased changeover includes:

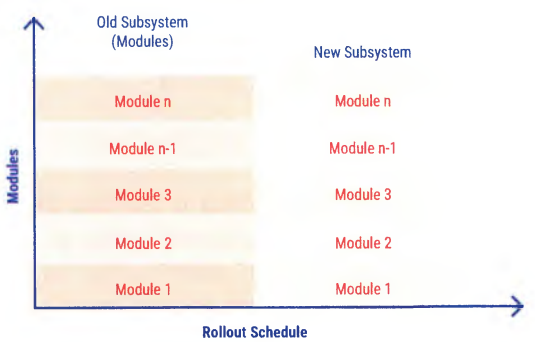
- Resource challenges (both on the IT side—to be able to maintain two unique environments, such as hardware, OSs, databases and code; and on the operations side—to be able to maintain user guides, procedures and policies, definitions of system terms, etc.)

- Extension of the project life cycle to cover two systems
- Change management for requirements and customizations to maintain ongoing support of the older system

Abrupt Changeover

In this approach, the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued after changeover to the new system takes place. See **figure 3.27**.

Figure 3.27—Abrupt Changeover



Changeover to the newer system involves four major steps or activities:

1. Conversion of files and programs; test running on test bed
2. Installation of new hardware, OS, application system and the migrated data
3. Training employees or users in groups
4. Scheduling operations and test running for go-live or changeover

Some of the risk items related to changeover include:

- Asset safeguarding
- Data integrity
- System effectiveness
- System efficiency
- Change management challenges (depending on the configuration items considered)
- Duplicate or missing records (possible existence of duplicate or erroneous records if data cleansing is not done correctly)

3.7.3 System Change Procedures and the Program Migration Process

Following implementation and stabilization, a system enters the ongoing development, or maintenance, stage. This phase continues until the system is retired. The phase involves those activities required to either correct errors in the system or enhance the capabilities of the system.

In this regard, an IS auditor should consider the following:

- The existence and use of a methodology for authorizing, prioritizing and tracking system change requests from the user
- Whether emergency change procedures are addressed in the operations manuals
- Whether change control is a formal procedure for the user and the development groups
- Whether the change control log ensures all changes shown were resolved
- The user's satisfaction with the turnaround—timeliness and cost—of change requests
- The adequacy of the security access restrictions over production source and executable modules
- The adequacy of the enterprise's procedures for dealing with emergency program changes
- The adequacy of the security access restrictions over the use of the emergency logon IDs

The IS auditor should examine a selection of changes on the change control log to:

- Determine whether changes to requirements resulted in appropriate change-development documents, such as program and operations documents.
- Determine whether changes were made as documented.
- Determine whether current documentation reflects the changed environment.
- Evaluate the adequacy of the procedures in place for testing system changes.
- Review evidence (test plans and test results) to ensure that procedures are carried out as prescribed by organizational standards.
- Review the procedures established for ensuring executable and source code integrity.
- Review production executable modules and verify that there is only one corresponding version of the program source code.
- Check the technical controls of the change management tool.

Additionally, an IS auditor should review the overall change management process for possible

©ISACA. All Rights Reserved.

improvements in acknowledgment, response time, response effectiveness and user satisfaction with the process.

Critical Success Factors

Critical success factors of planning the implementation include the following:

- To avoid delays, the appropriate skilled staff must attend workshops and participate for the entire project duration.
- The documentation needed for carrying out the work needs to be ready at project initiation.
- Decision-makers must be involved in all steps to ensure that all necessary decisions can be made.

End-User Training

The goal of a training plan is to ensure that the end user can become self-sufficient in the operation of the system. One of the most important keys in end-user training is to ensure that training is considered and a training project plan is created early in the development process. A strategy can be developed that takes into consideration the timing, extent and delivery mechanisms.

The training should be piloted using a cross-section of users to determine how best to customize the training to the different user groups. Following the pilot, the training approach can be adjusted as necessary, based on the feedback received from the pilot group.

Separate classes should be developed for individuals who will assist in the training process. These train-the-trainer classes also provide useful feedback for improving the content of the training program.

The timing of the delivery of training is very important. If training is delivered too early, users will forget much of the training by the time the system goes into production. If training is delivered too late, there will not be enough time to obtain feedback from the pilot group and implement the necessary changes into the main training program. Training classes should be customized to address skill level and needs of users based on their roles within the enterprise.

To develop the training strategy, an enterprise must name a training administrator. The training administrator will identify users who need to be trained with respect to their specific job functions. Consideration should be given to the following format and delivery mechanisms:

- Case studies
- Role-based training
- Lecture and breakout sessions
- Modules at different experience levels
- Practical sessions on how to use the system
- Remedial computer training (if needed)
- Online sessions on the web or on physical media

It is important to have a library of cases or tests, including user errors and the system response to those errors. The training administrator should record student information in a database or spreadsheet, including student feedback for improving the training course.

3.7.4 System Software Implementation

System software implementation involves identifying features, configuration options and controls for standard configurations to apply across the enterprise. Additionally, implementation involves testing the software in a nonproduction environment and obtaining some form of certification and accreditation to place the approved OS software into production.

3.7.5 Certification/Accreditation

Certification is a process by which an assessor enterprise performs a comprehensive assessment against a standard of management and operational and technical controls in an IS. The assessor examines the level of compliance in meeting certain requirements, such as standards, policies, processes, procedures, work instructions and guidelines —requirements made in support of accreditation. The goal is to determine the extent to which controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the system's security requirements. The results of a certification are used to reassess the risk and update the system security plan, thus providing the factual basis for an authorizing official to render an accreditation decision.

Accreditation is the official management decision (given by a senior official) to authorize operation of an IS and to explicitly accept the risk to the enterprise's operations, assets or individuals, based on the implementation of an agreed-on set of requirements and security controls. Security accreditation provides a form of QC and challenges managers and technical staff at all levels to implement the most effective security controls possible in an IS, given mission requirements, and technical, operational and cost/schedule constraints.

By accrediting an IS, a senior official accepts responsibility for the security of the system and is fully accountable for any adverse impact to the enterprise if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize accreditation.

 ©ISACA. All Rights Reserved.

3.8 Postimplementation Review

Projects should be formally closed to provide accurate information on project results, improve future projects and allow an orderly release of project resources. The closure process should determine whether project objectives were met or excused and should identify lessons learned to avoid mistakes and encourage repetition of good practices. In contrast to project closure, a postimplementation review typically is carried out several weeks or months after project completion, when the major benefits and shortcomings of the solution implemented will be realized. The review is part of a benefits realization process and includes an estimate of the project's overall success and impact on the business.

A postimplementation review is also used to determine whether appropriate controls were built into the system. It should consider the technical details and the process that was followed in the course of the project, including the following:

- Adequacy of the system:
  - Does the system meet user requirements and business objectives?
  - Have controls been adequately defined and implemented?
- Projected cost versus benefits or ROI measurements
- Recommendations that address any system inadequacies and deficiencies
- Plan for implementing any recommendations
- Assessment of the development project process:
  - Were the chosen methodologies, standards and techniques followed?
  - Were appropriate project management techniques used?
  - Is the risk of operating the system within acceptable risk levels?

Not all lessons associated with a given project may be immediately evident on completion. It is good practice for the project development team and a selection of end users to perform a second, joint review after the project has been completed and the system has been in production for a sufficient time period, to assess its effectiveness and value to the enterprise.

Closing a project is a formal process that focuses on capturing lessons learned for future use. **Figure 3.28** summarizes five steps that should be included in the closing of a project.

Figure 3.28—Project Closeout Steps

Step	Action
1	Assign responsibility for any outstanding issues to specific individuals and identify the related budget for addressing these issues (if applicable).
2	Assign custody of contracts, and either archive documentation or pass it on to those who need it.

3	Conduct a postimplementation review with the project team, development team, users and other stakeholders to identify lessons learned that can be applied to future projects. Include the following information:
	• Content-related criteria, such as:
	  ▪ Fulfillment of deliverable targets and any additional objectives
	  ▪ Attainment of project-related incentives
	  ▪ Adherence to the schedule and costs
	• Process-related criteria, such as:
	  ▪ Team dynamics and internal communication
	  ▪ Relationships between the project team and external stakeholders

4	Document any risk that was identified in the course of the project, including risk that may be associated with proper use of the deliverables, and update the risk register.
5	Complete a second postimplementation review after the project deliverables have been completed for long enough to realize the true business benefits and costs, and use the results of this review to measure the project's overall success and impact on the business.

It is important to note that, for a postimplementation review to be effective, the information to be reviewed should be identified during the project feasibility and design phase and collected during each stage of the project. For example, the project manager might establish certain checkpoints to measure effectiveness

©ISACA. All Rights Reserved.

of software development processes and accuracy of software estimates during the project execution. Business measurements should also be established up front and collected before the project begins and after the project is implemented (**figure 3.29**).

Figure 3.29—Measurements of Critical Success Factors

Productivity	• Dollars spent per user • Number of transactions per month • Number of transactions per user
Quality	• Number of discrepancies • Number of disputes • Number of occurrences of fraud/misuse detection
Economic value	• Total processing time reduction • Monetary value of administration costs
Customer service	• Turnaround time for customer question handling • Frequency of useful communication to users

It is also important to allow enough business cycles to be executed in the new system to realize the new system's actual ROI.

A postimplementation project review should be performed jointly by the project development team and appropriate end users. Typically, the focus of this type of internal review is to assess and critique the project process, whereas a postimplementation review has the objective of assessing and measuring the value that the project has on the business. Alternatively, an independent group that is not associated with the project implementation (internal or external audit) can perform a postimplementation review.

3.8.1 IS Auditor's Role in Postimplementation Review

An IS auditor performing a postimplementation review should be independent of the system development process. Therefore, an IS auditor involved in consulting with the project team on the development of the system should not perform this review. Unlike internal project team reviews, postimplementation reviews performed by an IS auditor tend to concentrate on the control aspects of the system development and implementation processes.

It is important that all audit involvement in the development project be thoroughly documented in the audit work papers to support an IS auditor's findings and recommendations. This audit report and documentation should be reused during maintenance and changes to validate, verify and test the impact of any changes made to the system. The system should periodically undergo a review to ensure that the system is continuing to meet business objectives in a cost-effective manner and control integrity still exists.

An IS auditor should perform the following functions:

- Determine if the system objectives and requirements were achieved. During the postimplementation review, careful attention should be paid to the end users' use, trouble tickets, work orders and overall satisfaction with the system. This review indicates whether the system's objectives and requirements were achieved.
- Determine if the cost benefits identified in the feasibility study are being measured, analyzed and accurately reported to management.
- Review program change requests performed to assess the type of changes required of the system. The type of changes requested may indicate problems in the design, programming or interpretation of user requirements.
- Review controls built into the system to ensure that they are operating according to design. If enterprise asset management (EAM) was included in the system, this module should be used to test key operations.
- Review operators' error logs to determine if there are any resource or operating problems inherent within the system. The logs may indicate inappropriate planning or testing of the system prior to implementation.
- Review input and output control balances and reports to verify that the system is processing data accurately.

 ©ISACA. All Rights Reserved.

Case Study

Wonderwheels is a major national retailer specializing in outdoor sports, hunting, fishing and camping, including a wide variety of all-terrain vehicles (ATVs), which inspired its name. The enterprise has operations currently based in the United States and has a long-term business plan to expand its retail centers to selected parts of the

As part of ongoing current operations, management has asked an internal IS auditor to review the enterprise readiness for complying with requirements for protecting cardholder information. This is meant to be a high-level overview of where the firm stands and not a point-by-point review of its compliance with the specific standard (which would be undertaken as a separate engagement later in the year).

During the initial assessment, the IS auditor learned the following information:

- **POS register encryption**—The retailer uses wireless POS registers that connect to application servers located at each store. These registers use wired equivalent protection (WEP) encryption.
- **POS local application server locations**—The POS application server, usually located in the middle of the customer service area at each store, forwards all sales data over a frame relay network to database servers at the Wonderwheels corporate headquarters, with strong encryption applied to the data. The data are then sent over a virtual private network (VPN) to the credit card processor for approval of the sale.
- **Enterprise database locations**—Enterprise databases are located on a protected, screened subset of the enterprise local area network.
- **Sales data distribution**—Weekly aggregated sales data, by product line, are copied as-is from the enterprise databases to magnetic media and mailed to a third party for analysis of buying patterns.
- **Current ERP system compliance**—The current state of the enterprise ERP system is such that it may be out of compliance with newer laws and regulations. During the initial assessment, the IS auditor determined that the ERP system does not adhere to the EU General Data Protection Regulation (GDPR).

Additionally, Wonderwheels database software has not been patched in over two years, due to a few factors:

- Vendor support for the database package was dropped because it was acquired by a competitor and its remaining business was refocused to other software services.
- Wonderwheels management implemented plans to upgrade to a new database package. The upgrade is underway; however, it is taking longer than anticipated.

Regarding the database upgrade, sizeable customizations were anticipated and are being carried out with a phased approach of partial deliverables. These deliverables are released to users for pilot usage on real data and actual projects. Concurrently, design and programming of the next phase are ongoing. In spite of positive initial test results, the internal audit group has voiced that it has not been included in key compliance decisions regarding the configuration and testing of the new system. In addition, operational transactions are often queued, or hang during execution, and, with increasing frequency, data are corrupted in the database. Additional problems have shown up—errors already corrected have started occurring again, and functional modifications already tested tend to present other errors. The project, already late, is now in a critical situation.

1. Which of the following presents the **MOST** significant risk to the retailer?

   A. Database patches are severely out of date.
   B. Wireless POS registers use WEP encryption.
   C. Credit cardholder information is sent over the Internet.
   D. Aggregate sales data are mailed to a third party.

2. Based on the case study, which of the following controls is the **MOST** important to implement?

   A. POS registers should use two-factor authentication, with enforced complex passwords.
   B. Wireless access points should use Media Access Control (MAC) address filtering.
   C. The current ERP system should be patched for compliance with the GDPR.
   D. Aggregate sales data should be anonymized and encrypted prior to distribution.

©ISACA. All Rights Reserved.

3. In the preliminary report to management, regarding the state of the database upgrade, which of the following is **MOST** important for the IS auditor to include?

   A. Internal audit should be included among the steering committee approvals.
   B. There is a possibility that the new database may not be compatible with the existing ERP solution.
   C. An ERP upgrade and/or patch is required to ensure updated database compatibility.
   D. Internal audit should be able to review the upgraded database to ensure compliance with Payment Card Industry Data Security Standard (PCI DSS).

4. To contribute more directly to help address the problems around the database upgrade, the IS auditor should:

   A. Review the validity of the functional project specifications as the basis for an improved software baselining definition.
   B. Propose to be included in the project team as a consultant for QC of deliverables.
   C. Research the problems further to identify root causes and define appropriate countermeasures.
   D. Contact the project leader, discuss the project plans and recommend redefining the delivery schedule using the PERT methodology.

Answers on page 244

Page intentionally left blank

Chapter 3 Answer Key

Case Study

1. A. Unpatched database servers are located on a screened subnet; this mitigates the risk to the enterprise.
   B. Use of WEP encryption presents the most significant risk because WEP uses a fixed secret key that is easy to break. Transmission of credit cardholder information by wireless registers is susceptible to interception and presents a very serious risk.
   C. Sending credit cardholder data over the Internet is less of a risk because strong encryption is being used.
   D. Because the sales data being sent to the third party are aggregate data, no cardholder information should be included.

2. A. According to the case study, it is unclear whether the POS registers already use two-factor authentication. It is known that aggregate sales data are copied onto other media as-is, without any controls, for external distribution.
   B. According to the case study, it is unclear whether the wireless access points use MAC address filtering. It is known that aggregate sales data are copied onto other media as-is, without any controls, for external distribution.
   C. Compliance with the GDPR, although important, is not the most important due to the current operations being only in the United States, and the potential for expansion into the EU is a long-term vision for the enterprise.
   D. It is unclear whether sales data are secure and free of personally identifiable information, such as credit card information and Social Security numbers. This presents the most significant risk and should be addressed.

3. **A. If internal audit is part of the steering committee, then it will have a say in the compliance and security-related controls to be included in production releases.**
   B. Ensuring database compliance is an operational responsibility and not an audit responsibility.
   C. Compatibility with existing architecture must be a function of the database implementation project team as a whole, which can include internal audit and also includes operations. Therefore, it is not the best answer choice.
   D. Although it is important that the upgraded database solution be compliant with all regulations affecting the enterprise, such a review should not be limited to one regulation. Therefore, it is not the best choice of those answers provided.

4. A. Functional project specifications should be executed by users and systems analysts, and not by the auditor.
   B. To propose to be project consultant for quality would not bring about an essential contribution, because quality is a formal characteristic; whereas, in the current case, the problem is substantial system instability.
   C. The only appropriate action is additional research, even if the apparently technical nature of the problem renders it unlikely that the auditor may find it alone.
   D. To contact the project leader and redesign the schedule of deliveries would not solve the problem. Furthermore, the definition of real causes may sensibly alter the project environment.

 ©ISACA. All Rights Reserved.

Chapter 4

Information Systems Operations and Business Resilience

Overview

Domain 4 Exam Content Outline 246
Learning Objectives/Task Statements 246
Suggested Resources For Further Study 246
Self-Assessment Questions 247
Chapter 4 Answer Key 250

Part A: Information Systems Operations

4.1 IT Components 253
4.2 IT Asset Management 274
4.3 Job Scheduling and Production Process Automation 274
4.4 System Interfaces 276
4.5 End-User Computing and Shadow IT 277
4.6 Systems Availability and Capacity Management 279
4.7 Problem and Incident Management 286
4.8 IT Change, Configuration and Patch Management 290
4.9 Operational Log Management 294
4.10 IT Service Level Management 298
4.11 Database Management 300

Part B: Business Resilience

4.12 Business Impact Analysis 309
4.13 System and Operational Resilience 311
4.14 Data Backup, Storage and Restoration 313
4.15 Business Continuity Plan 320
4.16 Disaster Recovery Plans 335

Case Study

Case Study 345
Chapter 4 Answer Key 348

©ISACA. All Rights Reserved.

Overview

Information systems (IS) operations and business resilience are important to provide assurance to users and management that the expected level of service will be delivered. Service level expectations are derived from the organization's business objectives. IT service delivery includes IS operations, IT services and management of IS and the groups responsible for supporting them. Disruptions are also an often-unavoidable factor of doing business.

Preparation is key to being able to continue business operations while protecting people, assets and reputation. Employing business resiliency tactics helps organizations address these issues and limit the impact.

This domain represents 26 percent of the CISA examination (approximately 39 questions).

Domain 4 Exam Content Outline

Part A: Information Systems Operations

1. IT Components
2. IT Asset Management
3. Job Scheduling and Production Process Automation
4. System Interfaces
5. End-user Computing and Shadow IT
6. Systems Availability and Capacity Management
7. Problem and Incident Management
8. IT Change, Configuration and Patch Management
9. Operational Log Management
10. IT Service Level Management
11. Database Management

Part B: Business Resilience

1. Business Impact Analysis
2. System and Operational Resilience
3. Data Backup, Storage and Restoration
4. Business Continuity Plan
5. Disaster Recovery Plans

Learning Objectives/Task Statements

Within this domain, the IS auditor should be able to:

- Conduct audits in accordance with IS audit standards and a risk based IS audit strategy.
- Evaluate the role and/or impact of automatization and/or decision-making systems for an organization.
- Evaluate the IT strategy for alignment with the organization's strategies and objectives.
- Evaluate the organization's management of IT policies and practices, including compliance with legal and regulatory requirements.
- Determine whether the organization has defined ownership of IT risk, controls and standards.
- Evaluate the organization's ability to continue business operations.
- Evaluate the organization's storage, backup and restoration policies and processes.
- Evaluate whether IT vendor selection and contract management processes meet business, legal and regulatory requirements.
- Evaluate supply chains for IT risk factors and integrity issues.
- Evaluate whether effective processes are in place to support end users.
- Evaluate whether IT service management practices align with organizational requirements.
- Evaluate whether IT operations and maintenance practices support the organization's objectives.
- Evaluate the organization's database management practices.
- Evaluate the organization's data governance program.
- Evaluate the organization's problem and incident management program.
- Evaluate the organization's change, configuration, release and patch management programs.
- Evaluate the organization's log management program.
- Evaluate the organization's policies and practices related to asset life cycle management.
- Evaluate risk associated with shadow IT and end-user computing (EUC) to determine effectiveness of compensating controls.
- Evaluate the organization's threat and vulnerability management program.
- Evaluate logical, physical and environmental controls to verify the confidentiality, integrity and availability of information assets.

Suggested Resources For Further Study

CM, S.; *Architecting Cloud-Native Serverless Solutions*, Packt Publishing, UK, 2023

Crask, J.; *Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301*, KoganPage, USA, 2021

Cuel, R.; D. Ponte; F. Virili; eds; *Exploring Digital Resilience: Challenges for People and Organizations*, Springer International Publishing, Switzerland, 2022

Eryurek, E.; U. Gilad; V. Lakshmanan; A. Kibunguchy-Grant; J. Ashdown; *Data Governance: The Definitive*

 ©ISACA. All Rights Reserved.

Guide: People, Processes, and tools to Operationalize Data Trustworthiness, O'Reilly Media, USA, 2021

International Organization for Standardization/ International Electrotechnical Commission, *ISO/IEC 20000-1:2018, Information technology—Service management—Part 1: Service management system requirements*, Switzerland, 2018, *www.iso.org/standard/70636.html*

ISACA, *COBIT®*, *www.isaca.org/cobit*

Kegerreis, M.; M. Schiller; C. Davis; *IT Auditing Using Controls to Protect Information Assets*, McGraw Hill, USA, 2020

Mannino, M.; *Database: Design, Application Development & Administration*, Chicago Business Press, USA, 2019

Pal, S.; D. Le; P. Pattnaik; C*loud Computing Solutions: Architecture, Data Storage, Implementation and Security*, Wiley, USA, 2022

Philips, B.D.; *Business Continuity Planning: Increasing Workplace Resilience to Disasters*, Elsevier, USA, 2021

Scholl, H.; E. Holdeman; F. Boersma; *Disaster Management and Information Technology: Professional Response and Recovery Management in the Age of Disasters*, Springer, Switzerland, 2023

Sikdar, P.; *Practitioner's Guide to Business Impact Analysis*, Auerbach Publications, USA, 2017

Snedaker, S.; *Business Continuity & Disaster Recovery for IT Professionals*, Syngress Publishing Inc., USA, 2014

Wallace, M.; L. Webber; *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*, Amacom, USA, 2018

Watters, J.; *Disaster Recovery, Crisis Response & Business Continuity*, Apress, USA, 2014

Self-Assessment Questions

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see section About This Manual for more guidance regarding practice questions.

1. Which one of the following provides the **BEST** method for determining the level of performance provided by similar information processing facility (IPF) environments?

   A. User satisfaction
   B. Goal accomplishment
   C. Benchmarking
   D. Capacity and growth planning

2. For mission critical systems with a low tolerance to interruption and a high cost of recovery, the information systems (IS) auditor, in principle, recommends the use of which of the following recovery options?

   A. Mobile site
   B. Warm site
   C. Cold site
   D. Hot site

3. Which of the following is the **MOST** effective method for an IS auditor to use in testing the program change management process?

   A. Trace from system-generated information to the change management documentation
   B. Examine change management documentation for evidence of accuracy
   C. Trace from the change management documentation to a system-generated audit trail
   D. Examine change management documentation for evidence of completeness

4. Which of the following would allow an enterprise to extend its intranet across the internet to its business partners?

   A. Virtual private network (VPN)
   B. Client-server
   C. Dial-up access
   D. Network service provider (NSP)

©ISACA. All Rights Reserved.

5. The classification based on criticality of a software application as part of an IS business continuity plan is determined by the:

   A. nature of the business and the value of the application to the business.
   B. replacement cost of the application.
   C. vendor support available for the application.
   D. associated threats and vulnerabilities of the application.

6. When conducting an audit of client-server database security, the IS auditor should be **MOST** concerned about the availability of:

   A. system utilities.
   B. application program generators.
   C. systems security documentation.
   D. access to stored procedures.

7. When reviewing a network used for internet communications, an IS auditor will **FIRST** examine the:

   A. validity of password change occurrences.
   B. architecture of the client-server application.
   C. network architecture and design.
   D. firewall protection and proxy servers.

8. An IS auditor should be involved in:

   A. observing tests of the disaster recovery plan (DRP).
   B. developing the DRP.
   C. maintaining the DRP.
   D. reviewing the disaster recovery requirements of supplier contracts.

9. Data mirroring should be implemented as a recovery strategy when:

   A. recovery point objective (RPO) is low.
   B. RPO is high.
   C. recovery time objective (RTO) is high.
   D. disaster tolerance is high.

10. Which of the following components of a business continuity plan (BCP) is **PRIMARILY** the responsibility of an organization's IT department?

    A. Developing the BCP
    B. Selecting and approving the recovery strategies used in the BCP
    C. Declaring a disaster
    D. Restoring the IT systems and data after a disaster

Answers on page 250

Page intentionally left blank

Chapter 4 Answer Key

Self-Assessment Questions

1. A. User satisfaction is the measure to ensure that an effective information processing operation meets user requirements.
   B. Goal accomplishment evaluates the effectiveness involved in comparing performance with predefined goals.
   C. Benchmarking provides a means of determining the level of performance offered by similar information processing facility (IPF) environments.
   D. Capacity and growth planning are essential due to the importance of IT in organizations and the constant technological change.

2. A. Mobile sites are specially designed trailers that can be quickly transported to a business location or to an alternate site to provide a ready-conditioned information processing facility (IPF).
   B. Warm sites are partially configured, usually with network connections and selected peripheral equipment—such as disk drives and controllers—but without the main computer.
   C. Cold sites have only the basic environment to operate an IPF. Cold sites are ready to receive equipment but do not offer any components at the site before the need.
   D. Hot sites are fully configured and ready to operate within several hours or, in some cases, even minutes.

3. **A. When testing change management, the information systems (IS) auditor should start with system-generated information, containing the date and time a module was last updated, and trace from there to the documentation authorizing the change.**
   B. Focusing exclusively on the accuracy of the documentation examined does not ensure that all changes were, in fact, documented.
   C. To trace in the opposite direction would run the risk of not detecting undocumented changes.
   D. Focusing exclusively on the completeness of the documentation examined does not ensure that all changes were, in fact, documented.

4. **A. Virtual private network (VPN) technology allows external partners to securely participate in the extranet using public networks as a transport or shared private network. Because of low cost, using public networks (Internet) as a transport is the principal method. VPNs rely on tunneling/encapsulation techniques, which allow the Internet Protocol (IP) to carry a variety of different protocols (e.g., systems network architecture [SNA] and internetwork packet exchange [IPX]).**
   B. Client-server does not address extending the network to business partners (i.e., client-server refers to a group of computers within an organization connected by a communications network where the client is the requesting machine and the server is the supplying machine).
   C. Although it may be technically possible for an enterprise to extend its intranet using dial-up access, it would not be practical or cost effective to do so.
   D. A network service provider may provide services to a shared private network by providing Internet services, but it does not extend an organization's intranet.

5. **A. The criticality classification is determined by the role of the application system in supporting the strategy of the organization.**
   B. The replacement cost of the application does not reflect the relative value of the application to the business.
   C. Vendor support is not a relevant factor for determining the criticality classification.
   D. The associated threats and vulnerabilities will be evaluated only if the application is critical to the business.

6. **A. System utilities may enable unauthorized changes to be made to data on the client-server database. In an audit of database security, the controls over such utilities would be the primary concern of the information systems (IS) auditor.**
   B. Application program generators are an intrinsic part of client-server technology, and the IS auditor would evaluate the controls over the generator's access rights to the database rather than their availability.
   C. Security documentation should be restricted to authorized security staff, but this is not a primary concern.
   D. Access to stored procedures is not a primary concern.

 ©ISACA. All Rights Reserved.

7. A. Reviewing the validity of password changes would be performed as part of substantive testing.
   B. Understanding the network architecture and design is the starting point for identifying the various layers of information and the access architecture across the various layers, such as client-server applications.
   C. The first step in auditing a network is to understand the network architecture and design. Understanding the network architecture and design provides an overall picture of the network and its connectivity.
   D. Understanding the network architecture and design is the starting point for identifying the various layers of information and the access architecture across the various layers, such as proxy servers and firewalls.

8. **A. The information systems (IS) auditor should always be present when disaster recovery plans (DRP) are tested to ensure that the tested recovery procedures meet the required targets for restoration, that recovery procedures are effective and efficient, and to report on the results as appropriate.**
   B. IS auditors may be involved in overseeing plan development, but they are unlikely to be involved in the actual development process.
   C. Similarly, an audit of plan maintenance procedures may be conducted, but the IS auditor normally would not have any responsibility for the actual maintenance.
   D. An IS auditor may be asked to comment upon various elements of a supplier contract, but this is not always the case.

9. **A. Recovery point objective (RPO) is the earliest point in time at which it is acceptable to recover the data. In other words, RPO indicates the age of the recovered data (i.e., how long ago the data was backed up or otherwise replicated). If RPO is very low, such as minutes, it means that the organization cannot afford to lose even a few minutes of data. In such cases, data mirroring (synchronous data replication) should be used as a recovery strategy.**
   B. If RPO is high, such as hours, then other backup procedures could be used.
   C. A high recovery time objective (RTO) means that the IT system may not be needed immediately after the disruption/declaration of disaster (i.e., it can be recovered later).
   D. RTO is the time from the disruption/declaration of disaster during which the business can tolerate the nonavailability of IT facilities. If RTO is high, slower recovery strategies that bring up IT systems and facilities can be used.

10. A. Members of the organization's senior management are primarily responsible for overseeing the development of the business continuity plan (BCP) and are accountable for the results.
    B. Management is also accountable for selecting and approving the strategies used for disaster recovery.
    C. IT may be involved in declaring a disaster but is not primarily responsible.
    D. The IT department of an organization is primarily responsible for restoring the IT systems and data after a disaster within the designated timeframes.

©ISACA. All Rights Reserved.

Page intentionally left blank

 ©ISACA. All Rights Reserved.

Part A: Information Systems Operations

IS operations are vital to modern organizations for effectively managing and maintaining systems and networks. IS operations include hardware and software installation, system configuration, network management, data backup and recovery, security monitoring and user support. IT operations involve coordinating resources, personnel and processes to ensure the reliable and uninterrupted operation of IS, enabling organizations to achieve their objectives.

Efficient IT operations contribute to increased productivity, streamlined processes, enhanced data integrity and improved decision-making capabilities. Organizations can improve competitiveness and avoid disruption by optimizing system performance, minimizing downtime and resolving technical issues promptly.

IT operations professionals play a crucial role in this domain. They have a deep understanding of computer systems, networks and software applications, which enables them to effectively diagnose and troubleshoot technical problems. They ensure that systems adhere to industry standards and regulatory requirements, safeguarding sensitive data from breaches and unauthorized access.

IT operations practices are important to reassure users and management that the expected level of service will be delivered. Service level expectations are derived from the organization's business objectives. IT service delivery includes IS operations, IT services, and management of IS and the groups responsible for their support.

4.1 IT Components

The components of IT operations vary depending on the specific organization and its IT infrastructure. IT operations can be complex and require a highly customized approach based on the enterprise's specific needs, industry and scale of operations. An IS auditor should be familiar with relevant regulations (e.g., the EU General Data Protection Regulation (GDPR), US Health Insurance Portability and Accountability Act (HIPPA) and industry-specific requirements) and should assess whether IT operations comply with all applicable regulations and standards. Because the technology landscape changes constantly, IS auditors should stay updated on emerging technologies and industry trends, such as cloud computing, virtualization, artificial intelligence (AI) and cybersecurity threats. This knowledge allows them to assess the risk and controls associated with these technologies during IT operations.

The most common elements in IT operations are:

- **Infrastructure**—The network infrastructure is vital for connectivity and data transfer within the organization. Hardware within the infrastructure includes workstations, storage devices and peripherals such as printers and scanners. It includes routers, switches, firewalls and other networking equipment. As part of their infrastructure, large organizations often have data centers that house servers, storage systems and networking equipment. Data centers are designed to provide a controlled environment with features like climate control, power supply, fire suppression, physical security and redundancy measures to ensure the availability and reliability of IT systems. Data centers serve as centralized locations for hosting critical infrastructure components, applications and data. An IS auditor should comprehensively understand the organization's IT infrastructure, including hardware, software, networks, data centers and cloud services. This knowledge enables auditors to assess infrastructure components' effectiveness, efficiency and security.
- **Network**—Networking components are critical for connecting devices, enabling communication and facilitating data transfer. Typical networking components are routers, switches, firewalls, load balancers, virtual private network (VPN) concentrators, network cables and satellite communication equipment. Companies have the need to access resources on the Internet—especially when they implement multiple, distributed locations—and the requirement to connect them through a wide area network (WAN) to ensure availability of IT services. To meet these needs, physical networks are generally organized into logical circuits that separate traffic, and then special equipment is used to forward it or provide protocol switching when the traffic must be transmitted through a WAN or an Internet service provider. Often, encryption is applied by network equipment before the network traffic is forwarded to ensure its confidentiality. Legacy telecommunication and network services are often replaced with less expensive virtual services like software-defined WAN (SD-WAN). An IS auditor should possess in-depth knowledge of network security controls, including access controls, network security, data protection, encryption, vulnerability management and incident response. Auditors should assess the adequacy and

©ISACA. All Rights Reserved.

effectiveness of these controls to mitigate security risk.

- **Applications and software**—Applications and software solutions support various business functions and processes. IT operations often lead the selection, development, implementation and maintenance of reliable, secure and up-to-date software that optimizes productivity, streamlines operations and meets business requirements. IT operations manage various software components, including operating systems (OSs), applications, databases and middleware. An IS auditor should understand change management processes, assess the effectiveness of change controls and evaluate whether proper testing, documentation and authorization procedures are followed as software is updated and upgraded. Application controls should include user access reviews, interface controls, separation of duties, backup and encryption.
- **System monitoring and management**—IT operations continuously monitor IT infrastructure, network performance and application health through monitoring tools, log analysis, event management and proactive issue detection and resolution. Monitoring relies on implementing monitoring tools and performance management practices to identify bottlenecks, detect issues and optimize system performance. An IS auditor should understand the monitoring systems in place, assess their effectiveness in detecting and responding to performance issues, and evaluate the organization's capacity planning and optimization practices.
- **Backup and disaster recovery**—The integrity and availability of an organization's data are crucial. Organizations need efficient data management practices, including reliable backup systems, disaster recovery plans (DRPs) and data replication mechanisms to protect against data loss and minimize downtime during system failures, natural disasters or other disruptive incidents to ensure data can be restored in case of loss or corruption. An IS auditor should be familiar with incident management processes and evaluate their effectiveness in detecting, reporting and responding to incidents. Auditors should assess the organization's business continuity and DRP to ensure that critical IT operations can be restored promptly.
- **Virtualization and cloud computing**—With the increasing adoption of virtualization and cloud technologies, IT operations often involve managing virtual machines, hypervisors and cloud infrastructure. This includes provisioning, scaling and optimizing resources in virtual and cloud environments. Within cloud services, IT operations may include managing the adoption of cloud platforms, such as infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS), and virtualization technologies to enhance flexibility, scalability and cost efficiency in technology. IS auditors should ensure controls are in place through direct testing or reliance on third-party reviews such as system and organization controls (SOC) reports.
- **Documentation and knowledge management**—Both comprehensive documentation of IT systems, configurations and processes and effective knowledge management practices are essential for effective IT operations. Knowledge management systems facilitate storing and sharing procedures, troubleshooting guides, process narratives and end-to-end process flowcharts to ensure efficient operations, smooth transitions and effective collaboration within the IT team. An IS auditor should review all IT documentation to ensure it is complete, up-to-date and accessible for future reference.

Note

Vendor-specific terminology is used within this manual for illustrative purposes only. Candidates will not be examined on the components of vendor-specific hardware offerings or on vendor-specific terminology unless this terminology has become generalized and is used globally.

4.1.1 Networking

A discussion of IT operations and components benefits from an overview of networking concepts. The purpose of network architecture standards is to facilitate this process by providing a reference model that organizations can use for building intercomputer and network communication processes.

The benchmark standard for this process is the open systems interconnection (OSI) reference model. OSI is a proof-of-concept model composed of seven layers, each specifying specialized tasks or functions. Each layer is self-contained and relatively independent of the other layers in terms of its function. This enables solutions offered by one layer to be updated without adversely affecting the other layers.

The purpose of the OSI model is to conceptually describe the movement of information (data). The OSI program was derived from a need for international networking standards and was designed to facilitate

 ©ISACA. All Rights Reserved.

communication between hardware and software systems despite differences in underlying architectures.

It is important to note that in the OSI model each layer communicates not only with the layers above and below it in the local stack, but also with the same layer on the remote system. For example, the application layer on the local system appears to be communicating with the application layer on the remote system. All the details of how the data is processed further down the stack are hidden from the application layer. This is true at every level of the model. Each layer appears to have a direct (virtual) connection to the same layer on the remote system.

The application layer provides a standard interface for applications that must communicate with devices on the network (e.g., print files on a network-connected printer, send an email or store data on a file server). Thus, the application layer provides an interface to the network. In addition, the application layer may communicate the computer's available resources to the rest of the network. The application layer should not be confused with application software. Application software uses the application layer interface to access network-connected resources.

The presentation layer transforms data to provide a standard interface for the application layer and provides common communication services, such as encryption, text compression and reformatting. The presentation layer converts the outgoing data into a format acceptable by the network standard and then passes the data to the session layer. Similarly, the presentation layer converts data received from the session layer into a format acceptable to the application layer.

The session layer controls the dialogs (sessions) between computers. It establishes, manages and terminates the connections between the local and remote application layers. All conversations, data exchanges and dialogs between the application layers are managed by the session layer.

The transport layer provides reliable and transparent transfer of data between end points, end-to-end error recovery and flow control. The transport layer ensures that all the data sent to it by the session layer is successfully received by the remote system's transport layer. The transport layer is responsible for acknowledging every data packet received from the remote transport layer, ensuring that an acknowledgement is received from the remote transport layer for every packet sent. If an acknowledgement is not received for a packet, then that packet will be resent.

The network layer creates a virtual circuit between the transport layer on the local device and the transport layer on the remote device. This is the layer of the stack that understands IP addresses and is responsible for routing and forwarding. This layer prepares the packets for the data link layer.

The data link layer enables the reliable transfer of data across a physical link. It receives packets of data from the network layer, encapsulates them into frames and sends them as a bit stream to the physical layer. These frames consist of the original data and control fields necessary to provide synchronization, error detection and flow control. Error detection is accomplished calculating a cyclic redundancy check (CRC) value and then adding it to each frame of data. The receiving data link layer calculates the CRC value for the data portion of the received frame and discards the frame if the calculated and received values do not match. A CRC calculation will detect all single-bit and most multiple-bit errors.

A bit stream received from the physical layer is similarly converted to data packets that are sent to the network layer. The data link layer logically connects to another device on the same network segment using a media access control (MAC) address. Each device on the network has a unique MAC hardware address that is assigned to it at the time of manufacture. The MAC address can be overridden, but this practice is not recommended. The data link layer normally listens only to data intended for its MAC address. An important exception to this rule is that a network interface may be configured as a promiscuous interface that will listen to all data the physical layer sends.

The physical layer provides the hardware that transmits and receives the bit stream as electrical, optical or radio signals over an appropriate medium or carrier. This layer defines the cables, connectors, cards and physical aspects of the hardware required to physically connect a device to the network. Error correction and detection is not usually implemented in the physical layer, with a few notable exceptions.

The intent of the OSI model is to provide a standard interface at each layer and to ensure that each layer does not have to be concerned with the details of how the other layers are implemented.

This approach supports system-to-system communication (peer-to-peer relationships) in which each layer on the sender side provides information to its peer layer on the receiving side. The process is characterized as a data traversal process with the following actions occurring:

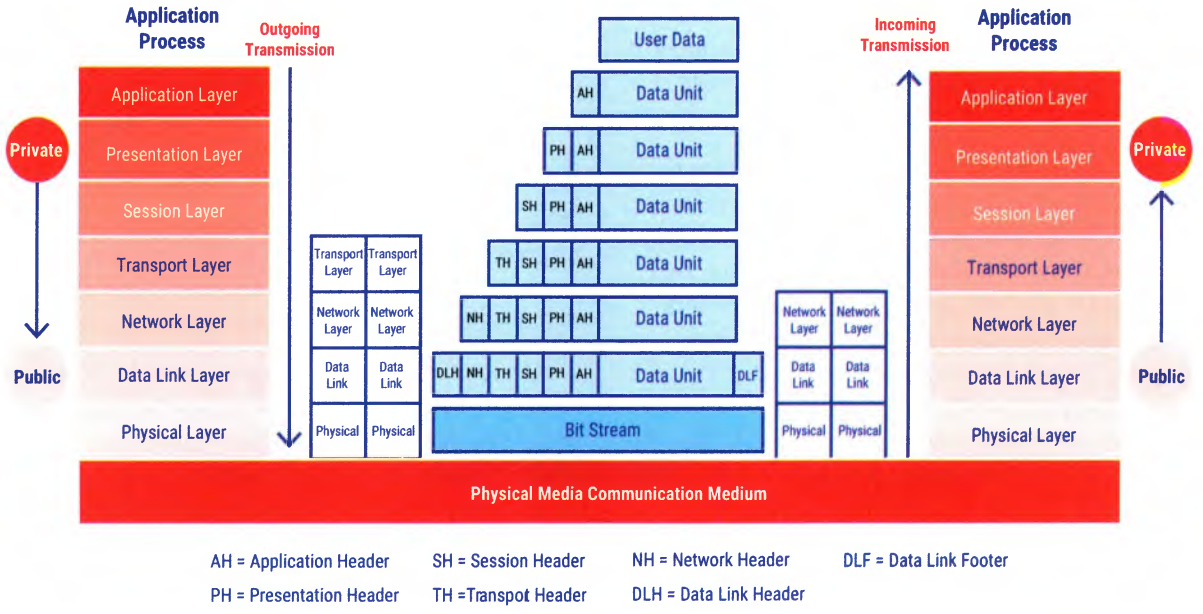
- Data travels down through layers at the local end.

©ISACA. All Rights Reserved.

- Protocol-control information (headers/trailers) is used as an envelope at each layer to pick up control information.
- Data travels up through the layers at the receiving/destination end.
- Protocol-control information (headers/trailers) is removed as the information is passed up.

A traditional OSI model showing this process is depicted in **figure 4.1**.

Figure 4.1—Traditional OSI Model



The concepts of the OSI model are used in the design and development of organizations' network architectures, including local area networks (LANs), WANs and metropolitan area networks (MANs), and in the use of the public Transmission Control Protocol/Internet Protocol (TCP/IP)-based global Internet.

Local Area Network

A LAN covers a small, local area—from a few devices in a single room to a network across a few buildings. The increase in reasonably priced bandwidth has reduced the design effort required to provide cost-effective LAN solutions for organizations of any size.

As LANs get larger and traffic increases, the requirement to carefully plan the logical configuration of the network becomes increasingly important. Network planners need to be highly skilled and very knowledgeable. Their tools include traffic monitors that allow them to monitor traffic volumes on critical links. Tracking traffic volumes, error rates and response times is every bit as important on larger LANs as it is on distributed servers and mainframes.

To set up a LAN, an organization must assess cost, speed, flexibility and reliability. The issues include:

- Assessing media for physically transmitting data
- Assessing methods for the physical network medium
- Understanding from a performance and security standpoint how data will be transmitted across the network and how the LAN network is organized and structured in terms of optimizing the performance of the devices connected to it

Network Physical Media Specifications

The type and characteristics of physical media (e.g., speed, sensitivity to external disturbances, signal loss and propagation, security) not only affect the cost of implementation and support but also impact the capacity, flexibility and reliability of the network.

 ©ISACA. All Rights Reserved.

LANs can be implemented using various types of media, including:

- **Copper (twisted-pair) circuits**—Two insulated wires are twisted around each other, with current flowing through them in opposite directions. This reduces the opportunity for cross talk between pairs in the same bundle and allows for lower sensitivity to electromagnetic disturbances (shielded twisted-pair circuits) within each pair. Twisted-pair circuits can also be used for some dedicated data networks. A disadvantage of unshielded twisted-pair cabling is that it is not immune to the effects of electromagnetic interference (EMI) and should be run in dedicated conduits, away from sources of potential interference, such as fluorescent lights. Parallel runs of cable over long distances should also be avoided since the signals on one cable can interfere with signals on adjacent cables, an EMI condition known as cross talk.
- **Fiber-optic systems**—Glass fibers are used to carry binary signals as flashes of light. Compared to twisted-pair circuits, fiber-optic systems have a low transmission loss. Optical fibers do not radiate energy or conduct electricity. In addition, they are not affected by EMI and present a significantly lower risk of security problems, such as wiretaps. Optical fiber is a more fragile medium and is more attractive for applications in which changes are infrequent. Optical fiber is smaller and lighter than metallic cables of the same capacity. Fiber is the preferred choice for high-volume, long-distance runs. One example is using fiber to connect floor switches to enterprise data switches. In addition, fiber-optic cable is often used to connect servers to storage area networks (SANs).
- **Radio systems (wireless)**—Data is communicated between devices using low-powered systems that broadcast (or radiate) and receive electromagnetic signals representing data.

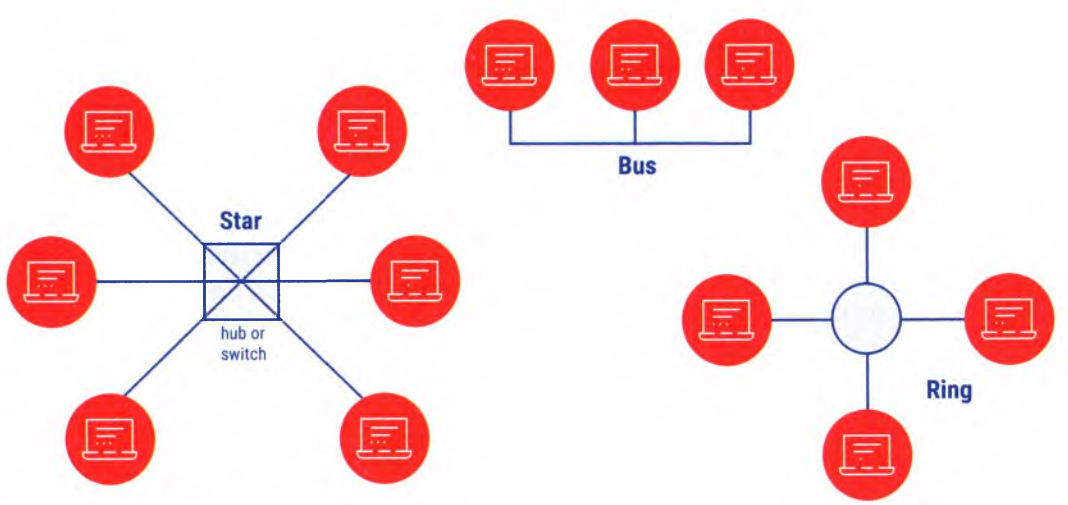
LAN Topologies and Protocols

LAN topologies define how networks are organized from a physical standpoint, whereas protocols define how information transmitted over a network is interpreted by systems.

LAN physical topology was previously tied tightly to the protocols that were used to transfer information across the wire. This is no longer true. For current technology, the physical topology is driven by ease of construction, reliability and practicality. Of the physical topologies that have been commonly used—bus, ring and star—only the star is used to any great extent in new construction. **Figure 4.2** illustrates commonly used physical topologies.

LAN media access technologies for accessing physical transmission media give devices shared access to the network, while also preventing a single device from monopolizing the network.

Figure 4.2—Physical Topologies in Common Use



©ISACA. All Rights Reserved.

LAN Components

LAN components consist of hardware and software technologies designed to work together to enable digital communication within a LAN. They include repeaters, hubs, bridges, switches and routers.

- **Repeaters**—Repeaters are physical layer devices that extend the range of a network or connect two separate network segments together. Repeaters receive signals from one network segment and amplify (regenerate) them to compensate for signals (analog or digital) that are distorted due to a reduction of signal strength during transmission (i.e., attenuation).
- **Bridges**—Bridges are data link layer devices that were developed to connect LANs or create two separate LAN or WAN network segments from a single segment to reduce collision domains. The two segments work as different LANs below the data link level of the OSI reference model, but from that level and above, they behave as a single logical network. Bridges act as store-and-forward devices in moving frames toward their destination. This is achieved by analyzing the MAC header of a data packet, which represents the hardware address of a network interface card (NIC). Bridges can also filter frames based on Layer 2 information. For example, they can prevent frames sent from predefined MAC addresses from entering a particular network. Bridges are software-based, and they are less efficient than similar hardware-based devices, such as switches. Therefore, bridges are not major components in today's enterprise network designs.
- **Layer 2 switches**—Layer 2 switches are data link level devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks. Furthermore, switches store and forward frames, filtering and forwarding packets among network segments, based on Layer 2 MAC source and destination addresses, just as bridges and hubs do at the data link layer. Switches, however, provide more robust functionality than bridges through use of more sophisticated data link layer protocols that are implemented via specialized hardware called application-specific integrated circuits (ASICs). The benefits of this technology are performance efficiencies gained through reduced costs, low latency or idle time, and a greater number of ports on a switch with dedicated high-speed bandwidth capabilities (e.g., many ports on a switch are available with 10/100 Ethernet and/or Gigabit Ethernet speeds). Switches are also applicable in WAN technology specifications.
- **Routers**—Routers are similar to bridges and switches in that they link two or more physically separate network segments. The network segments linked by a router, however, remain logically separate and can function as independent networks. Routers operate at the OSI network layer by examining network addresses (i.e., routing information encoded in an IP packet). By examining the IP address, the router can make intelligent decisions to direct the packet to its destination. Routers differ from switches operating at the data link layer in that they use logically based network addresses, use different network addresses/segments of all ports, block broadcast information, block traffic to unknown addresses, and filter traffic based on network or host information.

Routers are often not as efficient as switches because they are generally software-based devices and they examine every packet coming through, which can create significant bottlenecks within a network. Therefore, careful consideration should be given to where routers are placed within a network. This should include leveraging switches in network design as well as applying load balancing principles with other routers for performance efficiency considerations.

LAN Risk

Risk associated with use of LANs includes:

- Loss of data and program integrity through unauthorized changes
- Lack of current data protection through inability to maintain version control
- Exposure to external activity through poor user verification and potential public network access from remote connections
- Virus and worm infection
- Improper disclosure of data because of general access rather than need-to-know access provisions
- Illegal access by impersonating or masquerading as a legitimate LAN user
- Internal user sniffing (obtaining seemingly unimportant information from the network, such as network addresses, that can be used to launch an attack)
- Internal user spoofing (reconfiguring a network address to pretend to be a different address)
- Lack of enabled detailed automated logs of activity (audit trails)
- Destruction of the logging and auditing data

 ©ISACA. All Rights Reserved.

LAN Security

The LAN security provisions available depend on the software product, product version and implementation. Commonly available network security administrative capabilities include:

- Declaring ownership of programs, files and storage
- Limiting access under the principle of least privilege (POLP), which restricts users' access to what they need to perform their role
- Implementing record and file locking to prevent simultaneous updates
- Enforcing user ID/password sign-on procedures, including the rules relating to password length, format and change frequency
- Implementing port security policies by using switches rather than hubs or non-manageable routers. This will prevent unauthorized hosts with unknown MAC addresses from connecting to the LAN.
- Encrypting local traffic using Internet Protocol Security (IPSec) protocol

To gain a full understanding of the LAN, the IS auditor should identify and document:

- Users or groups with privileged access rights
- LAN topology and network design
- LAN administrator/LAN owner
- Functions performed by the LAN administrator/owner
- Distinct groups of LAN users
- Computer applications used on the LAN
- Procedures and standards relating to network design, support, naming conventions and data security

Wide Area Network

A WAN is a data communications network that transmits information across geographically dispersed LANs, such as among plant sites, cities and nations.

Key WAN characteristics include:

- They are applicable to the physical and data link layers of the OSI reference model.
- Data flow can be simplex (one-way flow), half duplex (one way at a time) or full duplex (both ways at one time without turnaround delay).
- Communication lines can be either switched or dedicated.

Implementation of WANs

Fiber-optic cables are commonly used for most high-capacity network connections. Other systems that may be used include:

- **Microwave radio systems**—Microwave radio provides line-of-sight transmission of voice and data through the air. Historically, analog microwave circuits supplied the majority of long-haul low-speed data and voice transmissions. This technology was used because it provided a lower-cost alternative to the low-capacity cable carrier systems of the time. Most heavy route microwave systems have since been replaced by fiber-optic cable systems providing greatly increased capacity and greatly improved reliability at a cost per channel mile that is a tiny fraction of the cost for microwave circuits of similar capacity. All new microwave construction uses digital signals, providing greatly increased data rates and reduced error rates when compared to analog circuitry. Microwave radio circuits are still in common use on "light routes" where the economics do not favor installation of fiber. Most electrical utility companies will use microwave systems to connect their Supervisory Control and Data Acquisition (SCADA) systems. The design of microwave circuits must consider the physical topology of the area and the climate. Microwave antennae must be able to "see" each other. Climate conditions, such as rainfall, can adversely affect microwave links.
- **Satellite radio link systems**—These contain several receiver/amplifier/transmitter sections called transponders. Each transponder has a bandwidth of 36 MHz, operates at a slightly different frequency, has individual transmitter sites and sends narrow beams of microwave signals to the satellite. Like microwaves, satellite signals can be affected by weather. Although satellite signals can carry large amounts of information at a time, the disadvantage is a bigger delay compared to other media, due to the "jump" from the earth to the satellite and back (traditionally estimated at about 300 ms). However, expanded deployment of low-earth orbit satellite networks, such as Starlink, is reducing latency to under 100 ms (sometimes as little as 20-30 ms), changing expectations and possibilities related to satellite-based Internet service.

Figure 4.3 identifies the advantages and disadvantages of each physical layer medium available to networks. These physical specifications are applicable to WAN technologies.

©ISACA. All Rights Reserved.

Figure 4.3—Transmission Media

Media	Use and Distance	Advantages	Disadvantages
Twisted pair	• Used for short distances fewer than 200 feet (60.96 meters) • Supports voice and data	• Cheap • Simple to install • Readily available • Simple to modify	• Easy to tap • Easy to splice • Cross talk • Interference • Noise
Coaxial cable	• Supports data and video	• Ease of installation • Straightforward • Readily available	• Thick • Expensive • Does not support many local area networks (LANs) • Distance sensitive • Difficult to modify
Fiber optics	• Used for long distances • Supports voice, data, image and video	• High bandwidth capabilities • Secure • Difficult to tap • No cross talk • Smaller and lighter than copper	• Expensive • Hard to splice • Difficult to modify
Radio systems	• Used for short distances	• Cheap	• Easy to tap • Interference • Noise
Microwave radio systems	• Line-of-sight carrier for voice and data signals	• Cheap • Simple to install • Available	• Easy to tap • Interference • Noise
Satellite radio link systems	• Uses transponders to send information	• High bandwidth and different frequencies	• Interference • Noise • Easy to tap

WAN Message Transmission Techniques

WAN message transmission techniques include:

- **Message switching**—Sends a complete message to the concentration point for storage and routing to the destination point as soon as a communications path becomes available. Transmission cost is based on message length.
- **Virtual circuits**—A logical circuit between two network devices that enables reliable data communications. Two types are available—switched virtual circuits (SVCs) and permanent virtual circuits (PVCs). SVCs dynamically establish on-demand connectivity and PVCs establish an always-on connection.

TCP/IP and Its Relation to the OSI Reference Model

The protocol suite used as the de facto standard for the Internet is known as TCP/IP. The TCP/IP suite includes both network-oriented protocols and application support protocols. **Figure 4.4** shows some of the standards associated with the TCP/IP suite and where they fit within the OSI model. The TCP/IP set of protocols was developed before the ISO/OSI framework; therefore, there is no direct match between the TCP/IP standards and the layers of the framework.

 ©ISACA. All Rights Reserved.

Figure 4.4—OSI Association With the TCP/IP Suite

	OSI Model	TCP/IP Conceptual Layers	Protocol Data Unit (PDU)	TCP/IP Protocols	Equipment	Layer Functions	Layer Functions
7	Application	Application	Data	Hypertext Transfer Protocol (HTTP) File Transport Protocol (FTP) Simple Mail Transport Protocol (SMTP) Trivial File Transfer Protocol (TFTP) Network File System (NFS) Name Server Protocol (NSP) Simple Network Management Protocol (SNMP) Remote Terminal Control Protocol (Telnet) Line Printer Daemon (LPD) X Windows Domain Name System (DNS) Dynamic Host Configuration Protocol (DHCP)/ Boot	Gateway	Provides user interface	File, print, message, database and application services
6	Presentation					Presents data Handles processing such as encryption	Data encryption, compression and translation services
5	Session					Maintains separation of the data of different applications	Dialog control
4	Transport	Transport	Segment	Transmission Control Protocol (TCP) User Datagram Protocol (UDP)	Layer 4 switch	Provides reliable or unreliable delivery	End-to-end connection
3	Network	Network interface	Packet	Internet Control Message Protocol (ICMP) Address Resolution Protocol (ARP) Reverse Address Resolution Protocol (RARP) Internet Protocol (IP)	Route Layer 3 switch	Provides logical addressing that routers use to determine paths	Routing

©ISACA. All Rights Reserved.

Figure 4.4—OSI Association With the TCP/IP Suite (cont.)

	OSI Model	TCP/IP Conceptual Layers	Protocol Data Unit (PDU)	TCP/IP Protocols	Equipment	Layer Functions	Layer Functions
2	Data link	LAN or WAN interface	Frame	Ethernet Fast Ethernet Fiber Distributed Data Interface (FDDI) Token Ring Point-to-Point Protocol (PPP)	Layer 2 switch Bridges Wireless AP Network Interface Card (NIC)	Combines packets into bytes and bytes into frames Provides access to media using MAC address Performs error detection, not error correction	Framing
1	Physical		Bits		Hub Repeater NIC	Moves bits between devices Specifies voltage, wire speed and pin-out of cables	Physical topology

Network Administration and Control

Network administration ensures that the network is functioning properly from a performance and security perspective. Duties include monitoring usage and throughput, load balancing, reacting to security violations and failure conditions, saving and restoring data and making changes for scalability as the network use grows. Therefore, appropriate knowledge of network structure and topology, the protocols used and the available administration tools is required.

The software used to monitor the network and enact changes should be accessible only to the network administrator. This software is the network OS software associated with specific network devices, principally switches and routers.

The network OSs provide many functions aimed at shaping the network as a unified, controlled and uniform computing environment, including:

- Support local and remote terminal access to hosts and servers
- Support sharing of common network resources, such as file and print services
- Establish links to hosts and servers

Network OSs provide many user-oriented features, including:

- Allow transparent access to the various resources of the network hosts
- Check the user authorization to particular resources
- Mediate and simplify access to make remote resources as easily accessible as local resources
- Establish uniform logon and logging procedures throughout the network
- Provide up-to-the-minute online network documentation
- Permit more reliable operation than possible on a single host or server, particularly when groups of equivalent hosts are used

Network Performance Metrics

The major network performance metrics are latency, jitter, throughput and Quality of service (QoS):

- **Latency**—The delay that a message or packet experiences on its way from source to destination. Latency occurs because the information needs to cross through different devices (switching and routing times) and, to a lesser extent, because signals must travel some distance (propagation delay). When a

 ©ISACA. All Rights Reserved.

network device is busy, the packets either must wait, be queued in a buffer or be dropped. A very easy way to measure latency in a TCP/IP network is to use the ping command.

- **Jitter**—Jitter is the difference in latency between packet flow from origination to destination measured in milliseconds. The main difference between latency and jitter is that latency is the delay through the network, whereas jitter is the change in the amount of latency. A significant variance in delays is referred to as "high jitter," while a minor change is referred to as "low jitter."
- **Throughput**—The quantity of useful work made by the system per unit of time. In telecommunications, it is the number of bytes per second that pass through a channel.
- **Quality of service (QoS)**—The measurement of the overall performance of the network, especially from the network users' point of view. It is a measure of the capability of the network to provide quality services to users. It takes into consideration latency and jitter, as well as other measures such as transmission delay, availability and packet loss.

Network error counts and number of retransmissions are also measured to assess network performance.

Network Management Issues

It is common today to see WANs communicating with a mix of LAN and host systems network architecture (SNA) traffic or pure LAN-oriented traffic. Almost all organizations have standardized their telecommunications infrastructure on TCP/IP and modern routers.

This trend toward a different technical design approach is made evident by the specific name (i.e., WAN) that designates telecommunication networks in a TCP/IP environment. A WAN needs to be monitored and managed similarly to a LAN. ISO, as part of its communications modeling effort (ISO/IEC 10040), has defined five basic tasks related to network management:

- **Fault management**—Detects the devices that present some kind of technical fault
- **Configuration management**—Allows users to know, define and change the configuration of any device remotely
- **Accounting management**—Holds the records of the resource usage in the WAN (who uses what)
- **Performance management**—Monitors usage levels and sets alarms when a threshold has been surpassed
- **Security management**—Detects suspicious traffic or users, and generates alarms accordingly

Network Management Tools

In an organization's modern internetworking environment, tasks are typically accomplished using a set of tools generically called network management tools.

Response time reports identify the time necessary for a command entered by a user at a terminal to be answered by the host system. Response time is important because end users experiencing slow response time will be reluctant to use IS resources to their fullest extent. These reports typically identify average, worst and best response times over a given time interval for individual telecommunication lines or systems. These reports should be reviewed by IS management and system support personnel to track potential problems. If response time is slow, all possible causes, such as input/output (I/O) channel bottlenecks, bandwidth utilization and central processing unit (CPU) capacity, should be investigated; various solutions should be analyzed; and appropriate and cost-justified corrective actions should be taken.

Downtime reports track the availability of telecommunication lines and circuits. Interruptions due to power/line failure, traffic overload, operator error or other anomalous conditions are identified in a downtime report. If downtime is excessive, IS management should consider the following remedies:

- Add or replace telecommunications lines
- Switch to a more dependable transmission link (such as dedicated lines versus shared lines)
- Install backup power supplies
- Improve access controls
- Closely monitor line utilization to better forecast user needs, both in the near and long term

Online monitors check data transmission accuracy and errors. Monitoring can be performed by echo checking (received data is bounced back to sender for verification) and status checking all transmissions, ensuring that messages are not lost or transmitted more than once.

Network monitors provide a real-time display of network nodes and status.

Network (protocol) analyzers are diagnostic tools attached to a network link that use network protocols' intelligence for monitoring the packets flowing along the link and produce network use reports. Network analyzers are typically hardware-based and operate at the data link and/or network level. Output includes:

- Protocol(s) in use
- The type of packets flowing along the monitored link
- Traffic volume analysis
- Hardware errors, noise and software problems

©ISACA. All Rights Reserved.

- Performance statistics (e.g., percentage of used bandwidth)
- Problems and possible solutions

Simple Network Management Protocol (SNMP) is a TCP/IP-based protocol that monitors and controls different variables throughout the network, manages configurations, and collects statistics on performance and security. A master console polls all the network devices on a regular basis and displays global status. SNMP software can accept specific operator requests in real time. Based on the operator instructions, SNMP software sends specific commands to an SNMP-enabled device and retrieves the required information. To perform these tasks, all devices (i.e., routers, switches, hubs, PCs, servers) need to have SNMP agents running. The actual SNMP communications occur between all the agents and the console.

Converged Protocols

Converged protocols are those that enable communication over different mediums through the merging of proprietary protocols with standard protocols. This is a benefit in information security architecture as it simplifies security, with the same infrastructure typically used for multiple scenarios. Converged protocols typically use the existing TCP/IP supporting network infrastructure to host special or proprietary services without the need for further deployments of alternate underlying networking hardware, which results in significant cost savings for the organization. However, the architectures can also add complexity by introducing more protocols and devices that need to be managed on the same infrastructure. Some common examples of converged protocols whose architectures are of interest to the IS auditor include:

- **Fiber channel (FC)**—FC is a form of network data storage that allows for high-speed, loss-less delivery of file transfers at upward of 16 Gbps over up to 10 km distance. It was designed to be operated over fiber-optic cables and typically requires its own dedicated infrastructure separated from the regular client-based applications. FC primarily supports point-to-point networks that are often deployed for block storage, low latency applications such as databases that support high-speed online transactional processing (OLTP), online ticketing and virtual environments. FC is generally more secure than IP-based storage networks.
- **Fiber channel over ethernet (FCoE)**—FCoE is a technological solution that encapsulates FC frames over Ethernet networks. It typically requires 10 Gbps (or higher speeds of up to 40gbps) Ethernet in order to support the FC protocol. It means that FCoE can operate as a network layer or OSI Layer 3 protocol, replacing IP as the payload of standard Ethernet networks. The IS auditor providing assurance over FCoE should note that even though the technology is reliable and fault tolerant, it is very expensive to implement due to the high cost of required infrastructure such as switches and storage arrays.
- **Multi-protocol label switching (MPLS)**—MPLS is a high-throughput and high-performance network technology that directs data across a network based on short path labels rather than longer network addresses. It saves significant time and is less complex compared to traditional IP-based routing processes as it provides a mechanism for engineering network traffic patterns that is independent of routing tables. In an MPLS environment, the analysis of the packet header is performed just once, and the packet is then assigned to a stream that is identified by a label. A label is a short (20-bit), fixed-length value at the front of the packet that serves as a lookup index for the label forwarding table. The forwarding table stores forwarding information for each label as well as other information, such as class-of-service values used to prioritize packet forwarding. A key benefit of MPLS is that it is designed to handle a wide range of protocols through encapsulation, thus avoiding reliance on TCP/IP. This permits the use of several other networking technologies.
- **Voice over IP (VoIP)**—VoIP is a tunneling mechanism used to transport voice and/or data over a TCP/IP network. It is less expensive than other methods and offers a wider variety of options and features, including acting as a direct telephone replacement on computer networks and mobile devices. VoIP can support video and data transmission to allow videoconferencing and remote collaboration on projects. VoIP is available in both commercial and open-source options. Some VoIP solutions require specialized hardware to allow traditional telephone handsets/base stations to connect to the VoIP system by plugging into a USB adapter. Others are software-based only. VoIP calls are generally cheaper than landline and cellphone calls.
- **Internet Small Computer Systems Interface (iSCSI)** —iSCSI is a SAN protocol that supports location-independent file storage, transmission and retrieval over networks. It is typically viewed as a low-cost alternative to FC. It is an IP-based networking standard for transferring data carrying SCSI commands over a TCP/IP network. It links data storage facilities and provides block-level access to a

 ©ISACA. All Rights Reserved.

storage device. It allows two hosts to interpose and exchange SCSI commands by using IP networks that take a high-performance local storage bus, emulate it over a network, and create a SAN. Its components are:

- **iSCSI initiator**—The initiator is the host-based software or hardware that is installed in the server and allows the sending of data to and from the storage array. The source array typically acts as an initiator for data migration between the storage arrays.
- **iSCSI target**—The target is the system placed on a storage device, essentially a server for hosting the storage resources. It also has access to storage. It typically represents hard disk storage and is often accessed by Ethernet-based networks.

The IS auditor should understand the benefits of using iSCSI technology. iSCSI is reusable, and the organization's existing servers can configure iSCSI several times. The technology is also easy to understand and configure; thus, it can be implemented by employees with limited knowledge. This makes it ideally suited for supporting disaster recovery processes. Benefits include:

- **Reducing costs**—iSCSI provides a low-cost network at the block level. It helps to reduce the requirement for additional network devices as it does not always need to use host bus adaptors, separate cabling or other specific devices in its implementation.
- **Enhancing flexibility**—It runs on an IP that makes it more flexible and does not limit the distance between the initiator and the target. It also leverages the interoperability advantages of TCP/IP and Ethernet.
- **Providing efficient data transmission**—iSCSI is fast and efficient and can be used for massive data transmission systems. It is usually configured for 10 GbE infrastructure and can transfer massive amounts of data at any given time.
- **Enhancing security**—The iSCSI protocol ensures network security resilience by enabling authentication identity, network isolation, integrity and confidentiality. Network isolation ensures that valid initiators connect to storage arrays, protecting data from unauthorized access.

Internet Protocol Networking

IP networking enables devices to communicate by providing the foundation for other protocols to communicate. IP itself is a connectionless protocol. There are two common types of IP networking:

- **Internet Protocol Version 4 (IPv4)**—IPv4 is used on packet-switched link layer networks (e.g., Ethernet). It provides an addressing capability of approximately 4.3 billion addresses and is the most-used IP address. It consists of a 32-bit address written in numbers that are separated by a dotted decimal notation.
- **Internet Protocol Version 6 (IPv6)**—IPv6 is more advanced and has better features compared to IPv4. It represents the next generation of IP addressing and has the capability to provide an infinite number of addresses. It is gradually replacing IPv4 to accommodate the growing number of networks worldwide and help solve the IP address exhaustion problems that affect Internet communications. Compared to IPv4, IPv6 provides a larger address space and simplifies header information and router tasks. It is also more compatible with mobile networks and allows bigger payloads in its communications.

Figure 4.5 summarizes the major differences between IPv4 and IPv6 from a security perspective.

Figure 4.5—Comparison of IPv4 and IPv6

	IPv4	IPv6
Checksum fields	Checksum fields are used.	Checksum fields are not available in Internet Protocol Version 6 (IPv6).
Transmission method	Broadcasting	Multicasting
Data security	Encryption and authentication are not supported.	Encryption and authentication are provided.
Address configuration	Manual and Dynamic Host Configuration Protocol (DHCP) configuration are supported.	Manual, DHCP, autoconfiguration and renumbering functionalities are supported.

©ISACA. All Rights Reserved.

Figure 4.5—Comparison of IPv4 and IPv6 (cont.)

	IPv4	IPv6
End-to-end connection integrity	End-to-end integrity of connections cannot be achieved.	End-to-end connection integrity is highly achievable.
Security features	The version is not developed for security purposes and security depends on the application.	The version is enhanced for security purposes.
Packet flow identification	There is no mechanism for identifying packet flows.	Flow label field in the header is used to identify packet flows.

There are a few transition strategies for converting IPv4 into IPv6, including:

- **Dual stacking**—Dual stacking allows an organization to implement both versions on the same device. All the communicating devices must support the IPv4/IPv6 dual stack while the interfaces connected to the dual stack network must also be configured with both IPv4 and IPv6 addresses.
- **Tunneling**—This approach uses the current routing system provided by IPv4 to accommodate IPv6 traffic if it requires passage. The advantage of this approach is that it maintains consistency of the IPv4 routers and hosts as configured.

Network Address Translation

Network address translation (NAT) is a mechanism for converting internal IP address packet headers into public IP addresses for transmission over the Internet. It was developed to allow private networks to use any IP address without causing collisions or conflicts with public Internet hosts with the same IP addresses.

The major types of NAT are:

- **Static NAT**—A static NAT maps a specific internal IP address permanently to an external IP address. In addition, the external address is always the same IP address. Simply, each node has a static internal/external address pair allowing an internal host, such as a web server, to have a private IP address and be reachable over the Internet. It also enables external entities to communicate with outside systems.
- **Dynamic NAT**—A dynamic NAT is a NAT architecture in which mappings between external and internal addresses change in sessions. The internal IP address is dynamically mapped to an external IP address that is derived from a large pool of IP addresses, which allows internal network access to the Internet without requiring the lease of more public IP addresses. This is a less costly approach as it lowers abuse of public IP addresses.
- **NAT with port address translation (NPAT)**—NPAT permits several private network devices to share the same public IP address in the network. A dynamic unique port number is dynamically assigned to each device over a private network. The NAT router then translates the port number and the private IP address into a single external address, allowing easy and fast communication between multiple devices over the Internet through the use of a single public IP address.

NAT offers important benefits including:

- **Cost reduction**—An organization can connect an entire network to the Internet using only a single leased public IP and conserve IP address space. It is also possible to use or reuse the private IP addresses and still be able to communicate with the Internet.
- **Improved privacy**—NAT hides the device's IP address and addressing scheme and network topography from the Internet. Attackers can only see a single IP address or IP addresses are frequently changed, making it difficult to launch an attack.
- **Increased security**—NAT restricts connections so that only traffic stemming from connections originating from the internal protected network are allowed back into the network from the Internet. Thus, most intrusion attacks are automatically repelled. NAT also enhances security for private networks by keeping internal addressing private from the external network.
- **Increased flexibility and scalability**—NAT eliminates address renumbering when a network evolves, thereby making the networking system flexible. It also improves IPv4 scalability.
- **Boundary enforcement**—As the private IP addresses used inside the organizational LAN are not routable from outside, network boundaries are easier to enforce. This makes it possible to force traffic to flow through the network firewall for inspection before being routed.

 ©ISACA. All Rights Reserved.

Despite its many advantages, NAT has limitations. For example, the implementation is time consuming and requires huge storage capacities to maintain data records such as connection tables in the processor. It can also interfere with the proper functioning of other protocols such as IPSec. Some applications may stop functioning when NAT is enabled, especially when other network systems are not compatible. There may also be switching paths delays when NAT is enabled causing unexpected delays in the overall organizational communication system.

4.1.2 Computer Hardware Components and Architectures

Computer-system hardware components are interdependent components that perform specific functions and can be classified as either processing or I/O.

Processing Components

The central component of a computer is the CPU. Computers may:

- Have the CPU on a single chip (microprocessor)
- Have more than one CPU (multi-processor)
- Contain multiple CPUs on a single chip (multi-core processor)

The CPU comprises an arithmetic logic unit (ALU), a control unit and an internal memory. The control unit contains electrical circuits that control/direct all operations in the computer system. The ALU performs mathematical and logical operations. The internal memory (i.e., CPU registers) is used for processing transactions.

Other key components of a computer include:

- Motherboard
- Random access memory (RAM)
- Read-only memory (ROM)
- Permanent storage devices (hard disk drive [HDD] or solid-state drive [SSD])
- Power supply unit
- Cooling system
- OS (see section 4.10.2 Operating Systems)
- Wi-Fi
- Cellular radio (e.g., LTE, 5G, etc.)
- Bluetooth

HDDs and SSDs are both storage devices, but they use different technologies to store and access data. HDDs use mechanical spinning disks and a moving read/write head to access data, whereas SSDs use flash memory to store data. SSDs have no moving parts, which makes them faster, more durable and less susceptible to mechanical failure than HDDs.

Many devices contain a graphics processing unit (GPU). GPUs were originally developed to relieve CPUs from graphics-intensive tasks. On servers and cloud virtual systems, GPUs execute intensive calculations involving a high amount of data and free the CPU from such tasks. This has made them popular for running complex calculations in applications for machine learning, artificial intelligence and other high-performance computing.

Input/Output Components

Input/Output (I/O) components are used to pass instructions/information to the computer and to display or record the output generated by the computer. Some components, such as the keyboard and mouse, are input-only devices, while others, such as the touchscreen, are both input and output devices. A printer is an example of an output-only device.

Types of Computers

Computers can be categorized according to several criteria—mainly their processing power, size and architecture. These categories are shown in **figure 4.6**.

©ISACA. All Rights Reserved.

Figure 4.6—Common Types of Computers

Supercomputers	Very large and expensive computers with the highest processing speeds are designed for specialized purposes or fields that require extensive processing power (e.g., complex mathematical or logical calculations). They are typically dedicated to a few specific specialized systems or application programs.
Mainframes	Large, general-purpose computers are made to share their processing power and facilities with thousands of internal or external users. Mainframes accomplish this by executing a large variety of tasks almost simultaneously. The range of capabilities of these computers is extensive. A mainframe computer often has a proprietary operating system (OS) that can support background (batch) and real-time (online) programs operating parallel applications. Mainframes have traditionally been the main data processing and data warehousing resource of large organizations and have long been protected by several early security and control tools.
High-end and midrange servers	Multiprocessing systems capable of supporting thousands of simultaneous users can be comparable to a mainframe in size and power. High-end/midrange servers have many control features of mainframes, such as online memory and central processing unit (CPU) management and physical and logical partitioning. Their capabilities are comparable to mainframes in terms of speed, both for processing data and execution of client programs, but they cost much less than mainframes. Their OSs and system software base components are often commercial products. The higher-end devices generally use UNIX and, in many cases, function as database servers. In contrast, smaller devices are more likely to use the Windows OS and function as application and file/print servers.
Personal computers (PCs)	Small computer systems called PCs or workstations are designed for individual users. PCs are inexpensively priced and based on microprocessor technology. They are used for managing office automation functions such as word processing, spreadsheets and email; for managing small databases; and for interacting with web-based applications and personal graphics, voice, imaging, design, web access and entertainment tools. Although designed as single-user systems, these computers are commonly linked together to form a network.
Thin-client computers	Thin-client PCs are generally configured with minimal hardware (e.g., diskless workstation), with the intent being that most processing occurs at the server level using software, such as Microsoft Terminal Services or Citrix Presentation Server, to access a suite of applications.
Laptop computers	Lightweight (under 10 pounds/five kilograms) personal computers are easily transportable and powered by a normal AC connection or a rechargeable battery pack. Similar to the desktop variety of personal computers in capability, laptop computers also have similar CPUs, memory capacity and disk storage capacity. Their battery packs make them less vulnerable to power failures. Being portable, laptop computers are vulnerable to theft. Devices may be stolen to obtain stored information or to hijack connectivity within an internal local area network (LAN) or remotely.
Next unit of computing (NUC)	The NUC is a small-form device or computer element that delivers a full desktop PC experience, gaming experience or edge device experience.
Single-board computer (SBC)	A SBC is a complete functioning computer with the microprocessor, input/output (I/O) functions, memory and other features all built on a single circuit board (e.g., Raspberry Pi, Arbor, Forlinx, Gateworks, WinSystems). A predetermined amount of RAM is built-in and there are no expansion slots for peripherals.
Smartphones, tablets and other handheld devices	Handheld devices enable users to substitute a small computing device for a laptop computer. Some of their features include a scheduler, a telephone and address book, to-do lists, an expense manager, an e-reader and a web browser. Such devices can combine computing, telephone and networking features that are available for use anytime and anywhere. Handheld devices can also interface with PCs to back up or transfer important information. Likewise, information from PCs can be downloaded to handheld devices.

 ©ISACA. All Rights Reserved.

4.1.3 Common Enterprise Back-End Devices

In a distributed environment, many devices are used to deliver application services. One factor that has significantly changed in recent years is the rapid growth of the Internet of Things (IoT). Organizations need to embrace many connected items—including cars, thermostats, video cameras, mattresses and medical equipment—and understand how they affect operations. Although increased innovation, productivity and services offer benefits, IoT use risks data leakage and privacy issues. See chapter 5 Protection of Information Assets for more information.

Some of the devices most commonly encountered include:

- **Print servers**—Businesses of all sizes require that printing capability be available to users across multiple sites and domains. Generally, a network printer is configured based on where the printer is physically located and who within the organization needs to use it. Print servers allow businesses to consolidate printing resources for cost savings.
- **File servers**—File servers provide organization-wide access to files and programs. Document repositories can be centralized in a few organizational locations and controlled with an access-control matrix. Group collaboration and document management are easier with a document repository than with dispersed storage across multiple workstations.
- **Application (program) servers**—Application servers typically host software programs that provide client computers with application access, including processing the application business logic and communicating with the application database. Consolidating applications and licenses in servers enables centralized management and a more secure environment.
- **Web servers**—Web servers provide information and services to external customers and internal employees through web pages. Web servers are normally accessed via URLs.
- **Proxy servers**—Proxy servers provide an intermediate link between users and resources. Unlike servers that allow direct access, proxy servers access services on a user's behalf. A proxy server may render a more secure and faster response than a direct access server, depending on the proxied services.
- **Database servers**—Database servers store data and act as a repository. The servers concentrate on storing information rather than presenting it in a usable form. Application servers and web servers process the data stored in database servers into usable information.
- **Data loss prevention (DLP) gateway**—A DLP gateway is a network security device used to prevent data loss and exfiltration. It typically sits between the internal network and the Internet, and it inspects all traffic flowing in and out of the organization. DLP gateways can help prevent data breaches by identifying sensitive data and blocking attempts to send it outside the organization.
- **Appliances (specialized devices)**—Appliances provide a specific service and normally cannot run other services. They are significantly smaller, faster and more efficient than less specialized devices. Capacity and performance demands require that certain services be run on appliances instead of generic servers. Examples of appliances are:
  - Firewalls
  - Intrusion detection systems (IDSs)
  - Intrusion prevention systems (IPSs)
  - Switches
  - Routers
  - VPNs
  - Load balancers

Note

See chapter 5 Protection of Information Assets for more information on these appliances.

Proxy Servers

A proxy server is a server that acts on behalf of a user. There are two main types of proxy servers: forward proxies and reverse proxies.

Forward proxies sit between a client and the Internet. They intercept all traffic from the client and forward it to the Internet on the client's behalf. Forward proxies can be used for a variety of purposes, such as:

- **Improving performance**—Forward proxies can cache frequently accessed websites and content, which can improve page load times for users.
- **Filtering traffic**—Forward proxies can be used to filter traffic and block access to certain websites or types of content.
- **Anonymizing data**—Forward proxies can be used to hide clients' IP addresses from the websites they visit.

Reverse proxies sit between the Internet and a web server. They intercept all traffic from the Internet and forward it to the web server on the Internet's behalf.

©ISACA. All Rights Reserved.

Reverse proxies can be used for a variety of purposes, such as:

- **Load balancing**—Reverse proxies can distribute traffic across multiple web servers, which can improve performance and reliability.
- **Security**—Reverse proxies can be used to protect web servers from attack by filtering traffic and hiding the web servers' IP addresses.
- **Caching**—Reverse proxies can cache frequently accessed content, which can improve performance for users.

Open proxies are proxy servers that are accessible to anyone on the Internet. Professional organizations generally avoid open proxies, as they can be used for malicious purposes such as phishing and spam.

4.1.4 USB Mass Storage Devices

Removable storage devices—such as universal serial bus (USB) flash drives, external hard drives and secure digital (SD) cards that connect through a USB port—are generically known as USB mass storage class devices. These devices provide convenient and portable ways to store and transfer data. They were designed to connect many peripherals through a single standardized interface socket and improve plug-and-play capabilities by allowing hot swapping or allowing devices to be connected and disconnected without rebooting the computer or turning off the device.

Other convenient features include providing power to low-consumption devices without requiring an external power supply and allowing many devices to be used without requiring the installation of manufacturer-specific individual device drivers. USB flash drives, external hard drives and SD cards are typically readable through a USB port. SD cards may be read through a dedicated SD port or through a card reader inserted into a USB port.

USB ports can connect computer peripherals such as mice, keyboards, tablets, gamepads, joysticks, scanners, digital cameras, printers, personal media players, flash drives and external hard drives. Most OSs recognize the connection of a USB device and load the necessary device drivers.

SD/xD cards and flash drives are solid-state electronic data storage devices used with digital cameras, handheld and mobile computers, telephones, music players, video game consoles and other electronics. They offer high recordability, power-free storage, a small form factor and rugged environmental specifications.

Risk Related to USB Mass Storage Devices

USB mass storage devices are extremely common and used extensively by individuals. Due to their pervasiveness, IS auditors should be familiar with related risk. Risk factors related to the use of USB mass storage class devices include:

- **Viruses and other malicious software**—USB mass storage class devices present a computer virus vector that is very difficult to defend against. Whenever files are transferred between two machines, and USB mass storage class devices are no exception, there is a risk that malware (e.g., viruses, spyware and keyloggers) will be transmitted. Some USB mass storage class devices include a physical switch that can put the drive in read-only mode. When transferring files to an untrusted machine, setting a mass storage class device in read-only mode will prevent any data (including viruses) from being written to the device.
- **Data theft**—Hackers, corporate spies and disgruntled employees steal data, and these are crimes of opportunity in many cases. Any unattended and unlocked PC with a USB port provides an opportunity for criminal activity using a USB mass storage class device. A hacker with physical access to a corporate PC can steal data or plant spyware.
- **Data and media loss**—The portability of USB mass storage class devices presents an increased risk for lost data and media. If an unencrypted mass storage class device is lost, any individual who finds the device can access the data on the drive.
- **Corruption of data**—If the drive is improperly unplugged, then data loss can occur due to corruption. USB mass storage class devices differ from other types of removable media because the computer is not automatically alerted when USB mass storage class devices are removed. Users of USB mass storage class devices must alert the computer when they intend to remove the device; otherwise, the computer will be unable to perform the cleanup functions necessary for safe disconnection, especially if files from the device are currently open.
- **Compatibility issues**—Different versions of USB ports might have compatibility issues with various devices, leading to potential data transfer failure or corruption.
- **Physical damage risk**—USB mass storage class devices are susceptible to physical damage due to their small size and portability, potentially leading to data loss.
- **Loss of confidentiality**—Because of its convenient small physical size and large capacity, a USB mass storage class device can store a significant amount of

 ©ISACA. All Rights Reserved.

data, some that may be confidential. When a drive is lost, the risk of data falling into the hands of a competitor is increased. Legal issues can also arise due to loss of confidentiality. For example, in the United States, lost or compromised patient data can indicate a breach of patient privacy in violation of HIPAA.

Security Controls Related to USB Mass Storage Devices

Some of the controls that can help reduce the risk associated with the use of USB mass storage class devices are:

- **Encryption**—An ideal encryption strategy allows data to be stored on the USB mass storage class device but renders the data useless without the required encryption key, such as a strong password or biometric data. Products are available to implement strong encryption and comply with the latest encryption standards. Encryption is a good method to protect information written to a device from loss or theft. But sensitive data are still exposed to theft unless the information is also encrypted on the network or local workstation hard drive.
- **Granular control**—Solutions are available to provide granular management of USB ports in a centralized manner. This type of specialized software allows an organization to block USB mass storage class devices yet still allow peripherals like USB mice and keyboards to connect. The software can be configured to allow USB mass storage class devices from a particular manufacturer or allow certain computers to allow particular USB mass storage class devices. As with all security issues, a technological solution in isolation is insufficient. Strong policies, procedures, standards and guidelines must be implemented to ensure memory card and USB port security. Further, an aggressive user awareness program is necessary to effect changes in employee behavior.
- **Security personnel education**—Flash drives are so small and unobtrusive that they are easily concealed and removed from an enterprise. Physical security personnel should understand USB mass storage class devices and the risk they present.
- **The lock desktop policy enforcement**—In higher-risk environments, desktop computers should be configured to automatically lock after short intervals. This can prevent someone from inserting a USB mass storage class device while the computer operator is away.
- **Antivirus policy**—Antivirus software should be configured to scan all attached drives and removable media. Users should be trained to scan files before opening them.
- **Use of secure devices only**—Enforce the use of encryption. Centralized software can manage devices inserted through a USB port, enforce encryption or only accept encrypted devices.
- **Inclusion of return information**—The inclusion of a small, readable text file containing return information may help with device retrieval if a USB mass storage class device is lost or misplaced. It would be prudent to omit company details, providing a phone number or post office box instead. It also would be prudent to include a legal disclaimer that clearly identifies the information on the drive as confidential and protected by law.

4.1.5 Wireless Communication Technologies

Wireless communication technologies are an essential part of any organization. These technologies enable users to connect to the Internet, communicate with each other and track goods and inventory. While not an exhaustive list, the most common wireless communication technologies include Wi-Fi, Bluetooth and radio frequency identification (RFID).

Wi-Fi is a wireless networking technology that uses radio waves to provide wireless high-speed Internet access. Wi-Fi is the most common wireless communication technology in use today, and it is used in a wide variety of devices, such as computers, smartphones and tablets.

Bluetooth is a wireless communication technology that allows devices to communicate with each other over short distances. Bluetooth is commonly used to connect devices such as smartphones, headphones, wireless speakers and certain tracking devices.

See section 5.9 Mobile, Wireless and Internet of Things Devices for more information on Wi-Fi and Bluetooth technologies, as these are often used in networking scenarios.

RFID is a wireless communication technology that uses radio waves to identify and track objects. RFID tags are small electronic devices that can be attached to objects. RFID readers can then be used to read the tags and identify the objects. RFID is commonly used in applications such as asset tracking, inventory management and access control.

©ISACA. All Rights Reserved.

Wireless communication technologies have a number of advantages over traditional wired communication technologies, such as:

- **Convenience**—Wireless communication technologies are more convenient to use than wired technologies because they do not require cables. This makes them ideal for use in a variety of environments, such as homes, offices and factories.
- **Mobility**—Wireless communication technologies allow devices to communicate with each other even if they are not physically connected. This makes them ideal for use in mobile applications, such as cellphones and laptops.
- **Scalability**—Wireless communication technologies can be easily scaled to support a large number of devices. This makes them ideal for use in large networks, such as enterprise networks and public Wi-Fi networks.

See section 5.11 Information System Attack Methods and Techniques for more information on data-related risk.

4.1.6 Hardware Maintenance Program

To ensure proper operation, hardware must be routinely cleaned and serviced. Maintenance requirements vary based on complexity and performance workloads (e.g., processing requirements, terminal access and number of applications running). Maintenance should be scheduled to closely coincide with vendor-provided specifications. Maintenance is also important for environmental hardware that controls temperature and humidity, fire protection and electrical power. The hardware maintenance program is designed to document maintenance performance.

Information typically maintained includes:

- Reputable service company information for each hardware resource requiring routine maintenance
- Maintenance schedule information
- Maintenance cost information
- Maintenance performance history information, such as planned versus unplanned, executed and exceptional

IS management should monitor, identify and document any deviations from vendor maintenance specifications and provide supporting arguments for those deviations.

When performing an audit of this area, the IS auditor should:

- Verify that the program covers the scope and objectives in alignment with business requirements, and indicate gaps where present. For instance, it could be difficult to meet scopes and objectives in certain remote locations, where hardware vendors may not offer the same coverage as in more centrally located offices. Based on the identified gaps, the auditor should assess the risk to the organization.
- Ensure that a formal maintenance plan has been developed and approved by management and is being followed.
- Identify maintenance costs that exceed the budget or are excessive. These overages may indicate a lack of adherence to maintenance procedures or upcoming changes to the hardware. Proper inquiry and follow-up procedures should be performed.

Hardware Monitoring Reports and Procedures

The following are typical reports and procedures for monitoring the effective and efficient use of hardware:

- **Availability reports**—indicate the time periods during which the computer is in operation and available for use by users or other processes. A key concern this report addresses is excessive IS unavailability, referred to as downtime. Unavailability may indicate inadequate hardware facilities, excessive OS maintenance, the need for preventive maintenance, inadequate environmental facilities (e.g., power supply or air conditioning) or inadequate operator training.
- **Hardware error reports**—identify CPU, I/O, power and storage failures. These reports should be reviewed by IS operations management to ensure that equipment is functioning properly, to detect failures and to initiate corrective action. The IS auditor should know that attributing an error in hardware or software is not necessarily easy and immediate. Reports should be checked for intermittent or recurring problems, which might indicate difficulties in properly diagnosing the errors.
- **Asset management reports**—provide an inventory of network-connected equipment, such as PCs, servers, routers and other devices.
- **Utilization reports**—document the use of the machine and peripherals. Software monitors capture utilization measurements for processors, channels and secondary storage media, such as disk drives. Depending on the OS, resource utilization for multiuser computing environments found in mainframe/large-scale computers should average in the 85- to 95-percent range, with allowances for utilization occasionally reaching 100 percent and falling below 70 percent. Trends from utilization reports can be used by IS management to predict whether more or fewer processing resources are required.

 ©ISACA. All Rights Reserved.

4.1.7 Hardware Reviews

During audits of infrastructure and operations, hardware reviews should include the areas shown in **figure 4.7**.

Figure 4.7—Hardware Reviews

Areas to Review	Questions to Consider
Hardware acquisition plan	• Is the plan aligned with business requirements? • Is the plan aligned with the enterprise architecture (EA)? • Is the plan compared regularly to business plans to ensure continued synchronization with business requirements? • Is the plan synchronized with information systems (IS) plans? • Have criteria for the acquisition of hardware been developed? • Is the environment adequate to accommodate the currently installed hardware and new hardware to be added under the approved hardware acquisition plan? • Are the hardware and software specifications, installation requirements and the likely lead time associated with planned acquisitions adequately documented?
Acquisition of hardware	• Is the acquisition in line with the hardware acquisition plan? • Have the IS management staff issued written policy statements regarding the acquisition and use of hardware, and have those statements been communicated to the users? • Have procedures and forms been established to facilitate the acquisition approval process? • Are requests accompanied by a cost-benefit analysis? • Are purchases routed through the purchasing department to streamline the process, avoid duplications, ensure compliance with tendering requirements and legislation, and to take advantage of quantity and quality benefits such as volume discounts?
IT asset management	• Has the hardware been tagged? • Has an owner been designated? • Where will the hardware be located? • Have copies of the contracts/service level agreements (SLAs) been retained?
Capacity management and monitoring	• Are criteria used in the hardware performance monitoring plan based on historical data and analysis obtained from the IS trouble logs, processing schedules, job accounting system reports, preventive maintenance schedules and reports? • Is continuous review performed of hardware and system software performance and capacity? • Is monitoring adequate for equipment that has been programmed to contact its manufacturer (without manual or human intervention) in the case of equipment failure?
Preventive maintenance schedule	• Is the prescribed maintenance frequency recommended by the respective hardware vendors being observed? • Is maintenance performed during off-peak workload periods? • Is preventive maintenance performed at times other than when the system is processing critical or sensitive applications?
Hardware availability and utilization reports	• Is hardware availability adequate to meet workload schedules and user requirements? • Is backup hardware sufficiently flexible to accommodate required hardware preventive maintenance? • Are IS resources readily available for critical application programs?
Problem logs and job accounting system reports	• Have IS management staff reviewed hardware malfunctions, reruns, abnormal system terminations and operator actions?

©ISACA. All Rights Reserved.

4.2 IT Asset Management

An asset is something of tangible or intangible value worth protecting, including people, information, infrastructure, finances and reputation. To protect and manage an asset, there must be an inventory that identifies the asset, specifies its location and indicates whether it has been assigned an owner. The first steps in IT asset management are identifying all IT assets and creating an inventory of IT assets.

The inventory record of each information asset should include:

- **Owner**—the person or entity responsible for the asset
- **Designated custodian**—the individual or group responsible for the asset's maintenance and care
- **Specific identification**—the unique identifiers for the asset
- **Relative value**—the asset's value to the organization
- **Loss implications and recovery priority**—the potential impact if the information asset is lost and its priority in recovery efforts
- **Location**—where the asset is physically or virtually located
- **Security/risk classification**—the asset's classification in terms of security and risk
- **Asset group**—the extensive information system of which the asset is a part
- **Life cycle management**—the current stage in the asset's life cycle
- **Compliance requirements**—any legal or regulatory obligations related to the asset
- **Access controls**—details of authorized access to the asset
- **Disposal date**—date when the asset was returned or removed from circulation

Common methods for building the initial inventory include consulting the purchasing system, reviewing contracts and reviewing the installed software. Numerous tools exist to aid in identifying software on company-owned devices (e.g., laptops and mobile devices). Some tools are used in software audits to flag unapproved software use (see section 4.5 End-User Computing and Shadow IT). At the same time, other security solutions restrict software installation to IT administrators.

Once created, the inventory must be maintained. This includes adding new assets when they are acquired and distributed, periodically confirming an asset is still in the owner's possession and removing an asset once returned or destroyed. IT asset management should be employed for software and hardware assets. It is common to physically tag hardware assets. At the same time, the software is often tracked through network scanning and annual confirmation that the software license is still needed (see section 4.10.6 Software Licensing Issues). Depending on the nature of the asset and risk classification of the data accessed by the owner, it may be necessary to remotely wipe or disable assets when an individual states intent to leave the organization or when the asset is reported as lost or stolen (see section 5.5.1 Information Asset Security Policies, Procedures and Guidelines for more information on classifying and protecting information assets).

4.3 Job Scheduling and Production Process Automation

In complex IS environments, computer systems transfer thousands of data files daily. A job schedule is typically created that lists the jobs that must be run and the order in which they are run, including any dependencies. Due to the inherent complexity of this process, automated job scheduling software controls the scheduling process. In addition to scheduling batch jobs, job scheduling software can be used to schedule backups and other maintenance activities. Job scheduling is a major function within the IT department, and the controls related to job scheduling are taken very seriously. The schedule includes the jobs that must be run, the sequence of job execution and the conditions that cause program execution.

High-priority jobs should be given optimal resource availability, and maintenance functions (such as backup and system reorganization) should be performed during nonpeak times, if possible. Schedules keep customer demand manageable and permit unexpected or on-request jobs to be processed without unnecessary delay. Low-priority jobs are scheduled when time becomes available to alleviate the burden on IT staff and ensure accurate and consistent execution.

Job scheduling procedures are necessary to ensure that IS resources are used optimally based on processing requirements. Applications are increasingly required to be continually available; therefore, job scheduling (maintenance or long processing times) represents a greater challenge than before.

4.3.1 Job Scheduling Software

Job scheduling software is system software used by installations that process many batch routines. The scheduling software sets up daily work schedules. It automatically determines which jobs must be submitted to the system for processing. Automatic scheduling

 ©ISACA. All Rights Reserved.

software requires ongoing maintenance and optimization to ensure desired outcomes are achieved.

The advantages of using job scheduling software include:

- Job information is set up only once, reducing reliance on operators and error probability.
- Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.
- Logs are maintained of all job successes and failures.
- Security over access to production data is available.
- The burden on manual tasks is reduced or eliminated.

4.3.2 Scheduling Reviews

Figure 4.8 describes an audit approach to be considered when reviewing workload job scheduling and personnel scheduling.

Figure 4.8—Scheduling Reviews

Areas to Review	Questions to Consider
• Regularly scheduled applications • Input deadlines • Data preparation time • Estimated processing time • Output deadlines • Procedures for collecting, reporting and analyzing key performance indicators	• Are the items included in service level agreements (SLAs)? • Are the items functioning according to the SLAs?
Job schedule	• Have critical applications been identified, and is the highest priority assigned to them? • Have processing priorities been established for other applications, and are the assigned priorities justified? • Is scheduling of rush/rerun jobs consistent with their assigned priority? • Do scheduling procedures facilitate the optimal use of computer resources while meeting service requirements? • Do operators record jobs to be processed and required data files? • Do operators schedule jobs for processing on a predetermined basis and perform them using automated or manual scheduling software?
Daily job schedule	• Is the number of personnel assigned to each shift adequate to support the workload? • Does the daily job schedule serve as an audit trail? • Does the schedule provide each shift of computer operators with the work to be carried out, the sequence in which programs are to be run and an indication of when lower-priority work can be performed? • At the end of a shift, does each operator pass a statement of the work completed and the reasons any scheduled work was not finished to the work scheduler or the next shift of operators?
Console log	• Were jobs run and completed according to the schedule? • Were all job failures flagged and communicated for action to be taken? • Were job failure root causes investigated and determined? • Were the reasons for job failures valid? • Were job failures communicated to all appropriate end-user stakeholders?
Exception processing logs	• Do operators obtain written or electronic approval from owners when scheduling request-only jobs? • Do operators record all exception processing requests? • Do operators review the exception processing request log to determine the appropriateness of procedures performed?

©ISACA. All Rights Reserved.

Figure 4.8—Scheduling Reviews (cont.)

Areas to Review	Questions to Consider
Restarting jobs	• Are all restarted jobs properly authorized and logged for information systems (IS) management review? • Are procedures established for rerunning jobs to ensure that the correct input files are being used and subsequent jobs in the sequence rerun, if appropriate? • Are restarted jobs verified for completion?
Personnel	• Are personnel capable of assigning or changing job schedules and priorities authorized to do so?

4.4 System Interfaces

A system is a set of components, including hardware and software, that work together to run one or more computers. System interfaces allow data output from one application to be sent as input to another with little or no human interaction. Interfaces that involve humans are usually called user interfaces.

System interfaces provide the ability to transfer data even if the systems use different programming languages or were created by different developers. This gives organizations greater flexibility to choose the applications that best serve specific areas, even if those areas need to share data.

Generally, data transfers through system interfaces can be sorted into three categories:
1. System-to-system
2. Partner-to-partner
3. Person-to-person

System-to-system interfaces facilitate transfer of data between two systems, whether internal or external. System-to-system interfaces are common in large organizations for moving information between teams working with different tools and for moving financial data through various business cycles. Data may be transferred to specialized tools for analysis. These uses have increased in part because of the growing importance of business intelligence and analytics applications, which involve transferring data from a repository to an analytic tool to obtain intelligence and insights via data mining, reporting and visualization.

Partner-to-partner interfacing occurs when an organization needs two or more partner organizations to interface directly. For example, a large manufacturing company may need several suppliers to work together to deliver a complex part for the final product. The partner-to-partner interface facilitates the interaction between parties that do not have a direct connection. Data is continuously transferring back and forth across agreed-upon systems.

Person-to-person transfers are human interactions involving data exchange. These transfers are often the most unnoticed and unmanaged. Data exchange can be as easy as attaching a data file to an email and sending it or providing access to a shared drive. These transfer forms are more difficult to observe, manage, secure and control.

4.4.1 Risk Associated With System Interfaces

Recognizing the increased importance of providing accurate data in real time, organizations are focusing more on using a centralized methodology for tracking and managing system interfaces and ensuring that documented audit trails are available for relevant government regulations.

Some common risk concerns include:
- Problems with system-to-system interfaces can lead to pervasive errors if not corrected quickly.
- Partner-to-partner interfaces can expose confidential data to a third party or a cybersecurity vulnerability through a partner organization.
- Person-to-person interfaces are subject to human error, security exposure and repercussions from privacy issues that may not be caught in time.

Organizations must be able to rely on the accuracy and completeness of the data exchanged through system interfaces. If an interface fails to function correctly, incorrect management reports (e.g., research, financial, intelligence, performance and competitive) can have a significant negative impact on a business and decision-making. Beyond an effect on business value, even a small error can invoke compliance liability.

Another risk related to data security involves data during the transfer through system interfaces. The data extracted from the originating system must be the same as the data

 ©ISACA. All Rights Reserved.

downloaded and recorded in the recipient system. The data needs to be protected and secured throughout the transfer process.

Unauthorized access to the data via interception, malicious activity, error or other means can occur during data transfer through interfaces. Examples include granting elevated access to a shared drive to the wrong individual, being targeted by phishing attacks or allowing access through unsecure third parties.

System outages that render the data unavailable to a system interface can also affect data reliability (e.g., accuracy and completeness) because incomplete reports may be produced.

4.4.2 Controls Associated With System Interfaces

The IS auditor should ensure that the organization has a program that tracks and manages all internal and external system interfaces and data transfers in line with business needs and goals. This program should include the ability to see all the transfers made, including ad hoc ones, whether the organization uses a commercial- or custom-managed file transfer (MFT) system. IS auditors should ensure that the program can:

- Manage multiple file transfer mechanisms
- Use multiple protocols
- Handle encryption and decryption
- Compress/decompress data files
- Connect to common database servers
- Support email transfers
- Automate regular data transfers
- Analyze, track and report data attributes
- Ensure regulatory compliance
- Offer interruption handling
- Integrate with back-office applications
- Authenticate and authorize users
- Log required data/events

The IS auditor should ensure that the organization has a program that tracks and manages all internal and external system interfaces and data transfers in line with the business needs and goals. This program should include logging all transfers, including ad hoc ones, whether the organization uses a commercial or custom MFT system or implements application programming interface (API) calls. IS auditors should ensure that the program can:

- Manage multiple file transfer mechanisms and/or APIs
- Use multiple protocols
- Automatically encrypt, decrypt and electronically sign data files and API calls

Controls must be implemented to ensure that the data residing on the sending system is the same as the data recorded on the receiving system. For example, an organization may use a software package to generate controls during the extraction that automatically reconciles the data after it is recorded on the receiving system.

While automated controls are generally preferred, there should be a mechanism for reconciling the completeness and accuracy of any data transferred through interfaces. The reconciliation can be completed manually by running a report of the data sent and comparing it to a report on the data received, or it can be completed automatically through leverage of cryptographic hash checksums. Reconciliation monitoring should be done by a qualified person who can detect material differences in the data.

IS auditors should ascertain if the organization uses encryption, as appropriate for each use, to protect data during a transfer. Encryption is necessary when the risk of unauthorized access or interception is relatively high (e.g., industrial espionage, identity theft, credit card data theft). The transfer process may require strong access and authentication controls, and the data files might be password-protected.

There should be control over nonrepudiation, which ensures that the intended recipient is the actual recipient of the data.

To ensure that an audit trail is associated with the system interface, the organization needs to capture important information, including who sent the data, when it was sent, when it was received, what data structure (e.g., xls, csv, txt or xml) was used, how the data was sent and who received the data. Further, automated logs of servers should be assessed along the path, especially if the data is transmitted to an external system where it touches multiple Internet hosts and is more exposed to hackers and cybercriminals.

4.5 End-User Computing and Shadow IT

End-user computing (EUC) refers to the technologies and tools that enable individual users, typically non-IT professionals, to create, manage and utilize technical resources. EUC encompasses a broad range of applications, devices and platforms that empower end users to perform tasks without direct involvement from IT personnel. Typically, EUC is governed and managed by an organization's IT function. When end users go around the official EUC process to purchase, install and implement technical resources independently, the result is

©ISACA. All Rights Reserved.

referred to as Shadow IT because the IT department is unaware of the technology.

4.5.1 End-User Computing

End users are the people who access business applications that were programmed, serviced and installed by others. End-user computing (EUC) refers to the ability of end users (who typically are not programmers) to design and implement their own applications or information system using computer software products. An end-user support manager often is a liaison between an IT department and end users.

One of the benefits of EUC is that users can quickly build and deploy applications, taking pressure off the IT department. EUC enables organizations to be more flexible and rapidly address shifting marketplaces, regulations and consumer interests.

Lack of IT department involvement in EUC brings associated risk because the applications may not be subject to an independent review. Also, in many cases they are not created in the context of a formal development methodology.

The lack of IT department oversight of EUC can lead to security risk. Examples include:

- **Authorization**—There may be no security mechanism to authorize access to the system.
- **Authentication**—There may be no security mechanism to authenticate users to the system.
- **Audit logging**—Logging may not be available on standard EUC solutions (e.g., Microsoft Excel and Access).
- **Encryption**—The application may contain sensitive data that has not been encrypted or otherwise protected.
- **Data loss**—Applications may not be properly backed up.
- **Compliance risk**—Applications may store sensitive or private information.
- **Monitoring/auditing challenges**—Applications may not be captured within IT inventories, hindering any monitoring processes.
- **Maintenance/security patching**—Applications and databases may not be included in IT maintenance and security patching schedules.

In most instances, EUC applications do not pose significant risk to the enterprise. Nonetheless, management should define risk criteria to determine the criticality of an application. Organizations need to manage and control EUC, and the IS auditor should ensure that policies for the use of EUC exist. EUC applications also should be subject to data classification and an inventory of all such applications should exist (see section 4.2 IT Asset Management for more information). Applications deemed critical should be subject to the same controls as any other application.

4.5.2 Shadow IT

Shadow IT is the use of systems, services, hardware or software on an enterprise network or within an enterprise's infrastructure without proper vetting and approval from the IT or cybersecurity department. With the rise of low-cost, cloud-based software, and with users being accustomed to the diffusion and ease-of-use of smartphones with the computing power of desktop devices, more departments and individuals can procure IT resources within minutes without going through proper channels. This problem increases when individuals work from home networks and/or use personal hardware.

Shadow IT can include an application, tool, service or system that is used within an organization to collaborate, develop software, share content, store and manipulate data or serve any number of other purposes without being reviewed, tested, approved, implemented or secured by the organization's IT and/or information security functions' written policies and procedures. Shadow IT can drive disruption and innovation but potentially expose an enterprise to significant risk. To manage the benefits and risk of shadow IT, an organization must identify whether an IT upgrade or a digitalization and innovation program are necessary, determine the need for controls, employ appropriate controls and understand that applying controls is not a one-time activity. If controls are needed, regular assessments must follow their implementation to ensure they are still in place and operating effectively.

Many controls can address the threats related to shadow IT and a variety of approaches to their assessment. Many of these are unique to the type of enterprise and the organization's size and risk appetite. Typical controls include:

- **Shadow IT policy**—a shadow IT policy that aligns with business objectives and supports security requirements
- **IT department as a service-delivery organization**—a culture that encourages and rewards the achievement of a strong and supportive relationship between the IT department and business units, with IT functioning in a consultative way

 ©ISACA. All Rights Reserved.

- **IT budgeting and procurement**—a requirement that the IT department review and approve all IT-related purchases
- **IT system consolidation (if feasible)**—limiting the number of service providers, networks, platforms, devices and/or media used to store, process or transmit data, and consolidating applications to facilitate data management and consolidation of environments (e.g., data centers) to reduce overall technology footprint
- **User access and administrative rights**—user administration rights or data access rights that are explicitly assigned. Unassigned users cannot freely install or adopt new applications.
- **User education**—a formal IT user education program targeted at personnel in all business units
- **User activity monitoring**--recording and monitoring user activity
- **User data exchange**—establishing strong end-point controls

4.6 Systems Availability and Capacity Management

Systems performance refers to the study of an entire system, including physical hardware, components and software, and how it operates. Enterprises want to ensure that systems perform as expected and that issues are identified and addressed promptly. It is important to understand the features of the IS architecture and associated software to aid the systems performance management process.

4.6.1 IS Architecture and Software

The architecture of most computers can be viewed as several layers of circuitry and logic arranged in a hierarchical structure to interact with the computer's OS. The computer hardware, including some hard-coded instructions (firmware), is at the base of the hierarchy. The nucleus (kernel) functions are the next level up in the hierarchy. Functions of the nucleus relate to basic processes associated with the OS, which include:

- Handling interruption
- Process creation/destruction
- Process state switching
- Dispatching
- Process synchronization
- Interprocess communication
- Support of I/O processes
- Support of the allocation and reallocation/release of memory

The nucleus is a highly privileged area in which most user access is restricted. Above the nucleus are various OS processes that support users. These processes, or system software, are a collection of computer programs used to design, process and control all the computer applications that operate and maintain the computer system. Comprised of system utilities and programs, the system software ensures system integrity, controls the flow of computer programs and events and manages computer interfaces. Software developed for the computer must be compatible with its OS. Examples include:

- Access control software
- Data communications software
- Database management software
- Program library management systems
- Disk management systems
- Network management software
- Job scheduling software
- Utility programs

Some or all of the software may be built into the OS.

4.6.2 Operating Systems

Prior to considering the various forms of system software, the most significant system software related to a computer—its OS—needs to be understood. The OS contains programs that interface between the user, processor and application software. The OS runs the computer and acts as a scheduler and traffic controller. It provides the primary means of managing the sharing and use of computer resources, such as processors, real memory (e.g., RAM), auxiliary memory (e.g., disk storage) and I/O devices.

Most modern OSs have expanded the basic OS functionalities to include capabilities for more efficient operation of system and application software. For example, all modern OSs possess a virtual storage memory capability that allows programs to use and reference a range of addresses greater than the real memory. This technique of mapping parts of a large slower memory to a faster and smaller working memory is used between various levels of cached memory within modern systems.

OSs vary in terms of the resources managed, comprehensiveness of management and resource management techniques used. The type of computer, its intended use and the normal, expected attached devices and networks influence the OS requirements, characteristics and complexity. For example, a single-user microcomputer operating in stand-alone mode needs

©ISACA. All Rights Reserved.

an OS capable of cataloging files and loading programs to be effective. A mainframe computer handling large volumes of transactions for consolidation and distribution requires an OS capable of managing extensive resources and many concurrent operations, in terms of application input and output, with very high reliability. For example, z/OS has been engineered specifically to complement this environment.

A server with multiple users interacting with data and programs, from database servers and middleware connections to legacy mainframe applications, requires an OS that can accommodate multiprocessing, multitasking and multithreading. It must be able to share disk space (files) and CPU time among multiple users and system processes, and to manage connections to network devices. For example, UNIX is designed to specifically address this type of environment.

A microcomputer in a networked environment functioning as a server with specialized functions (e.g., applications, database management systems [DBMSs] and directory/file storage) can interact with data and programs of multiple users to provide services to client workstations throughout the network.

It is common for OSs to run on virtual servers. In a virtual environment, the software is used to partition one physical server into multiple independent virtual servers. Each environment then can run its own (and, if required, different) OS. To the operator, the OS behaves like it is running on a physical server.

Software Control Features or Parameters

Various OS software products provide parameters and options for tailoring the system and activating features such as activity logging. Parameters are important in determining how a system runs because they allow a standard piece of software to be customized for diverse environments.

Software control parameters deal with:

- Data management
- Resource management
- Job management
- Priority setting

Parameter selections should be appropriate to the organization's workload and control environment structure. The most effective means of determining how controls function within an OS is to review the software control features and/or parameters.

Improper implementation and/or monitoring of OSs can result in undetected errors and corruption of the data being processed, leading to unauthorized access and inaccurate logging of system usage.

Software Integrity Issues

OS integrity is a very important requirement and involves using specific hardware and software features to:

- Protect from deliberate and unintentional modification
- Ensure that user programs cannot interfere with privileged programs
- Provide effective process isolation to ensure that:
  - Multiple concurrently running processes are prevented from interfering with each other either by accident or by design and are protected from writing into each other's memory (e.g., changing instructions, sharing resources, etc.).
  - Least privilege is enforced so that processes have no more privilege than needed to perform functions and operate modules and call on more privileged routines only if and for as long as needed.

To maintain system and data integrity, it is necessary to correctly and consistently define, enforce and monitor the operating environment and the granted permissions. IS management is responsible for implementing appropriate authorization techniques to prevent nonprivileged users from gaining the ability to execute privileged instructions and thus take control of the entire machine.

For example, IBM mainframe z/OS systems are customized at system generation (SYSGEN) time. When these systems are started (initial program load), important options and parameters are read from information kept in a key system directory (the SYS1.PARMLIB partitioned data set). The directory specifies critical initialization parameters used to meet the data center's installation requirements (i.e., other system software activated for job scheduling, security, activity logging, etc.). If uncontrolled, these options provide a nonprivileged user with a way to access the OS's supervisory state. The IS auditor should review system configuration directories/files in all OSs for control options that protect the supervisory state.

PC-based client-server Windows, UNIX and Linux OSs have special system configuration files and directories. The existence of program flaws or errors in configuring, controlling and updating systems with the latest security patches makes them vulnerable to compromise. Important Windows system options and parameters are set in a set of special system configuration files, referred to as the registry. The registry is an important aspect of IS auditing. Noting any changes in the registry is crucial

 ©ISACA. All Rights Reserved.

for maintaining the system's integrity, confidentiality and availability. In UNIX-based OSs, the same issues are present. Critical system configuration files and directories related to the nucleus (kernel) operations, system start-up, network file sharing and other remote services should be appropriately secured and checked for correctness.

Operating System Reviews

When auditing operating software development, acquisition or maintenance, the details shown in **figure 4.9** should be considered.

Figure 4.9—Operating Systems Reviews

Areas to Review	Questions to Consider
System software selection procedures	• Do they align with the enterprise architecture (EA)? • Do they comply with short- and long-range information systems (IS) plans? • Do they meet the IS requirements? • Are they properly aligned with the objectives of the business? • Do they include IS processing and control requirements? • Do they include an overview of the capabilities of the software and control options?

Feasibility study and selection process	• Are the same selection criteria applied to all proposals?
	• Has the cost-benefit analysis of system software procedures addressed:
	  ▪ Direct financial costs associated with the product?
	  ▪ The cost of product maintenance?
	  ▪ Hardware requirements and capacity of the product?
	  ▪ Training and technical support requirements?
	  ▪ Impact of the product on processing reliability?
	  ▪ Impact on data security?
	  ▪ Financial stability of the vendor's operations?

System software security	• Have procedures been established to restrict the ability to circumvent logical security access controls? • Have procedures been implemented to limit access to the system interrupt capability? • Have procedures been implemented to manage software patches and keep the system software up to date? • Are physical and logical security provisions adequate to restrict access to the master consoles? • Were vendor-supplied installation passwords for the system software changed at the time of installation?
IT asset management	• Has an owner been designated? • Have copies of the contracts/service level agreements (SLAs) been retained? • What is the license agreement? • Has compliance with the license agreement been achieved?

System software implementation	• Are controls adequate in:
	  ▪ Change procedures?
	  ▪ Authorization procedures?
	  ▪ Access security features?
	  ▪ Documentation requirements?
	  ▪ Documentation of system testing?
	  ▪ Audit trails?
	  ▪ Access controls over the software in production?

©ISACA. All Rights Reserved.

Figure 4.9—Operating Systems Reviews (cont.)

Areas to Review	Questions to Consider
Authorization documentation	• Have additions, deletions or changes to access authorization been documented? • Does documentation exist of any attempted violations? If so, has there been follow-up?

System documentation	• Are the following areas adequately documented:
	  ▪ Installation control statements?
	  ▪ Parameter tables?
	  ▪ Exit definitions?
	• Activity logs/reports?

System software maintenance activities	• Is documentation available for changes made to the system software? • Are current versions of the software supported by the vendor? • Is there a defined patching process?
System software change controls	• Is access to the libraries containing the system software limited to individuals needing to have such access? • Are changes to the software adequately documented and tested before implementation? • Is software authorized properly before moving from the test environment to the production environment?
Controls over the installation of changed system software	• Have all appropriate levels of software been implemented? • Have predecessor updates taken place? • Are system software changes scheduled for times when the changes least impact IS processing? • Has a written plan been established for testing changes to system software? • Are test procedures adequate to provide reasonable assurance that changes applied to the system correct known problems and do not create new problems? • Are tests being completed as planned? • Have problems encountered during testing been resolved, and have the changes been retested? • Have fallback or restoration procedures been implemented in case of production failure?

4.6.3 Access Control Software

Access control software is designed to detect or prevent unauthorized access to data, unauthorized use of system functions and programs, unauthorized updates/changes to data and unauthorized attempts to access computer resources. (See chapter 5 Protection of Information Assets for more information on access control software.)

4.6.4 Data Communications Software

Data communications software is used to transmit messages or data from one point to another, either locally or remotely. For example, a database request from an end user is transmitted from that user's terminal to an online application, then to a DBMS in the form of messages handled by data communications software. Responses to the user are handled similarly (i.e., from the DBMS to the online application and back to the user's terminal).

A typical simple data communications system has three components:
1. The transmitter (source)
2. The transmission path (channel or line)
3. The receiver

One-way communication flows in one direction. In two-way communication, both ends may simultaneously operate as source and receiver, with data flowing over the same channel in both directions. The data communication system is concerned only with the correct transmission between two points. It does not operate on the content of the information.

A data communication system is divided into multiple functional layers. Software interfaces with hardware at

 ©ISACA. All Rights Reserved.

each layer to provide a specific set of functions. All data communication systems at a minimum have a physical layer and a data link layer. (See chapter 5 Protection of Information Assets for more information.)

Communication-based applications operate in local area network (LAN) and WAN environments to support:

- Electronic funds transfer (EFT) systems
- Database management systems
- Customer electronic services/electronic data interchange (EDI)
- Internet forums and email

The data communication system interfaces with the OS, application programs, database systems, telecommunication address method systems, network control systems, job scheduling systems and operator consoles.

4.6.5 Utility Programs

Utility programs are system software used to perform maintenance and routines that frequently are required during normal processing operations. Utility programs can be categorized by use into five functional areas:

1. Understanding application systems (flowcharting software, transaction profile analyzer, executive path analyzer and data dictionary)
2. Assessing or testing data quality (data manipulation utilities, database dump utilities, data comparison utility and query facility)
3. Testing a program's ability to function correctly and maintain data integrity (test data generator, online debugging facility, output analyzer and network simulator)
4. Assisting in faster program development (visual display utility, library copy, text editor, online coding facility, report generators and code generators)
5. Improving operational efficiency (CPU and memory utilization monitors and communication line analyzers)

Smaller computer systems (i.e., PC and server OSs) are often equipped with specific utilities to:

- Operate verification, cleaning and defragmenting of hard disk and removable memory units
- Initialize removable data volumes and volumes of disk/removable memory
- Save/restore system images
- Reconstruct and restore (logically) canceled files
- Test system units and peripherals

Many of these utility programs can perform outside the security system or function without producing an audit trail of activity. As a result, access to and use of sensitive and powerful utilities should be controlled and restricted.

4.6.6 Software Licensing Issues

Software copyright laws must be followed to protect against the imposition of penalties over copyright infringements and the added reputational risk of being identified as a company that illegally uses software. A software licensing agreement is a contract that establishes the terms and conditions under which a piece of software is licensed (i.e., made legally available for use) from the software developer (owner) to the user. There are two different software licensing types: free (**figure 4.10**) and paid (**figure 4.11**).

Figure 4.10—Free Software Licensing Types

Type	Description
Open source	The software may be used, copied, studied, modified and redistributed as required. Open source usually accompanies the program source and a copy of the software license (e.g., the GNU General Public License). A well-known example is Linux.
Freeware	The software is free, but the source code cannot be redistributed. A well-known example is Adobe Acrobat Reader. Freeware may also have restrictions limiting the software to personal use.
Trial	The software may initially be free, but it may only be trial-basis or have limited functionality compared to the full commercial version (and it may be known as the trial version, demo ware or an evaluation copy).

Figure 4.11—Paid Software Licensing Types

Type	Description
Per central processing unit (CPU)	Depends on the power of the server, specifically the number of the CPUs, and could include the number of CPU cores
Per seat	Depends on the number of unique users of the system

©ISACA. All Rights Reserved.

Figure 4.11—Paid Software Licensing Types (cont.)

Type	Description
Concurrent users	Depends on the total number of software users within a predefined period
Utilization	Depends on how busy the CPU is or the number of users that are active at any particular time
Per device	Depends on the number of individual devices (NOT users) that connect to the software
Enterprise	Usually allows unlimited use of the software throughout an organization without the need to apply any aforementioned rules, although there may be some restrictions
Mixed	A mix of the previous license types (e.g., a per seat license that allows only a certain number of devices for each user)

To detect software licensing violations, the IS auditor should:

- Review the listing of all standard, used and licensed application and system software.
- Obtain copies of all software contracts to determine the nature of the license agreements (e.g., an unlimited enterprise license, per-seat license or individual copies).
- Scan the network to produce a list of installed software by leveraging software inventory capabilities offered by asset and vulnerability management solutions to identify rogue equipment and to catalog installed software.
- Review a list of server specifications, including CPUs and cores, if required.
- Compare the license agreements with the installed software, noting any violations.

Options available to prevent software license violations include:

- Ensuring that a good software asset management process exists (see section 4.2 IT Asset Management)
- Centralizing control, distribution and installation of software (including disabling the ability of users to install software, if possible)
- Requiring all PCs to be restricted workstations with disabled or locked-down disk drives, USB ports, etc.
- Scanning user network endpoints regularly to ensure that unauthorized copies of software have not been loaded (achieved by comparing actual software loaded to the list of software assets)
- Enforcing documented policies and procedures that require users to sign an agreement not to install software without management authorization and a software license agreement.

Software licenses are primarily contractual compliance—that is, organizations agree to comply with the terms and conditions of the software publisher, with or without financial consideration. In certain circumstances, an IS auditor may need an expert legal opinion to confirm compliance.

Certain software publishers' licenses require the prescriptive capability of performing an audit of the license use by the licensee. An IS auditor must be prepared to support such audit requests by ensuring accurate collection of all licenses used upfront.

Related to licensing, some software contracts include pricing based on other factors or metrics, such as:

- **Transaction volume**—calculated based on the number of transactions, such as API call volume
- **Data volume**—based on gigabytes sent or minutes processed
- **Revenue share**—calculated as a percentage of revenue or transaction fees

Note

Some disaster recovery arrangements may require additional licenses and hosting of additional metering software. See section 4.16 Disaster Recovery Plans for more information.

4.6.7 Source Code Management

Source code is the text written in a programming language that is readable by humans and that must be converted to machine language before being executed as a program's instructions. It is translated into object code by assemblers and compilers and then tells the computer what to do. By its very nature, source code may contain intellectual property and should be protected, and access should be restricted.

Administrative access to source code may differ depending on the application and the nature of the agreement with the supplier. If no source code is supplied, it may be important to secure an escrow agreement. If the software is packaged, access to the source code may be granted under the license for customized modifications. If the software is bespoke or developed in-house, the organization will have full access to the source code. In all these instances, source code is subject to the software development life cycle

 ©ISACA. All Rights Reserved.

(see section 3.3 System Development Methodologies). Source code management is also tightly linked to change, release, quality assurance (QA) and information security management.

Source code should be managed using a version control system (VCS), often called revision control software (RCS). VCS maintain a central repository, which allows programmers to check out a program source to make changes to it. Checking in the source creates a new revision of the program. A VCS provides the ability to synchronize source changes with changes from other developers, including conflict resolution when changes have been made to the same source section. A VCS also allows branching, that is, making a copy of the trunk (original main code) that exists independently to allow customization for different customers, countries, locations, etc.

Examples of popular VCS are Apache® Subversion® and Git and its cloud implementations, such as GitLab and GitHub. Git is a distributed version control system (DVCS). While Subversion manages a single centralized repository, a DVCS has multiple repositories. In a DVCS, the entire repository may be replicated locally, with changes committed to the master repository when needed. This allows developers to work remotely without a connection.

The advantages of VCSs include:
- Controlling source code access
- Tracking source code changes
- Allowing concurrent development
- Allowing rollback to earlier versions
- Allowing branching

The IS auditor should always be aware of the following:
- Who has access to source code
- Who can commit the code (push the code to production)
- Alignment of program source code to program objects
- Alignment with change and release management
- Backups of source code, including offsite backups and escrow agreements

4.6.8 Capacity Management

Capacity management is the planning and monitoring of computing and network resources to ensure that the available resources are used efficiently and effectively. It requires that expansion or reduction of resources take place in parallel with overall business growth or reduction. The capacity plan should be developed based on input from users and IS management to ensure that business goals are achieved in the most efficient and effective way. The capacity plan should be reviewed and updated at least annually.

Capacity planning should include projections substantiated by experience, considering the growth of existing business and future expansions. The following information is key to the successful completion of this task:
- CPU/vCPU utilization
- Computer storage utilization
- Telecommunications
- LAN and WAN bandwidth utilization
- I/O channel utilization
- Number of users
- New technologies
- New applications
- Virtual machine density on physical hosts
- Service level agreements (SLAs)

The IS auditor must realize that the amount and distribution of these requirements have intrinsic flexibility. Specialized resources of a given class may impact the requirements for other classes. For example, when properly used, more intelligent terminals may consume less processor power and communications bandwidth than other terminals consume. Consequently, the information key to capacity planning is strictly related to the type and quality of used or planned system components.

One element of capacity management is deciding whether to host the organization's applications distributed across several small servers, consolidated onto a few large servers, in the cloud or in various combinations of the three. Consolidating applications on a few large servers (also known as application stacking) often allows the organization to better use its resources, but it increases the impact of a server outage. It affects more applications when the server has to be shut down for maintenance. Using the cloud allows extra capacity to be purchased on demand but brings the risk of relying on the supplier.

Larger organizations often have hundreds, if not thousands, of servers arrayed in groups referred to as server farms. If virtual servers are used, they may be organized as private (or internal or corporate) clouds.

If an organization has put data storage hardware in place, the IS auditor should review the capacity management plans that involve data storage and SAN utilization.

Capacity management must include network devices, such as switches and routers, that comprise physically and logically separated networks VLANs.

©ISACA. All Rights Reserved.

Capacity planning defines the business's requirements for IT capacity in business and technical terms. Further, it presents the consequences of delivering the required volume of activity through the IT infrastructure and applications at the right time and at an optimal cost. Capacity management ensures that the business's requirements for current and future capacity and performance aspects are provided cost-effectively.

Information system capacity is a key business requirement for IT systems. Business operations and processes can only be supported reliably when IT systems provide the required capacity. IT management should understand capacity requirements before designing information systems and should verify the final design against the capacity requirements. IT management must monitor capacity continuously and provide additional capacity as the business grows. For example, a file server may store all business files; when the storage reaches the 80 percent threshold, installation of an additional hard disk may be necessary to keep up with the storage requirements.

IT capacity—as measured by CPU power and memory, hard disk or server size—is expensive. Organizations do not want to acquire more than what they currently need. Capacity planning is the process of ensuring that the resource provision can always meet business requirements. Continuous monitoring of the capacity utilization threshold allows additional capacity to be acquired and deployed before the threshold no longer meets business requirements. With capacity management, expensive resources will be acquired only when they are needed, resulting in cost savings.

Capacity management monitors resource utilization and helps with resource planning. During procurement of the IT system, the capability management team will work with the architect to estimate resource requirements and to ensure that adequate, but not excessive, resources are provided to support the new solutions. The estimate is normally based on the number of transactions, size of data being stored, transaction processing time and response time, etc. Estimates help determine capability requirements for the new solutions.

Capacity management aims to consistently provide the required IT resources—at the right time and cost and in alignment with the current and future requirements of the business. Capacity management increases efficiency and cost savings by deferring the cost of new capacity to a later date and optimizing capacity to business needs. Capacity management reduces the risk of performance problems or failure by monitoring the resource utilization threshold and providing new resources before a shortage occurs. Capacity management also provides accurate capacity forecasting through application sizing and modeling for new services.

Capacity planning and monitoring include the elements listed in **figure 4.12**.

Figure 4.12—Capacity Planning and Monitoring Elements

Developing	Develop a capacity plan that describes current and future requirements for the capacity of IT resources.
Monitoring	Monitor IT components to ensure that agreed-upon service levels are achieved.
Analyzing	Analyze data collected from monitoring activities to identify trends for establishing normal utilization, service levels or baselines.
Tuning	Based on analyzed and interpreted monitoring data, optimize systems for the actual or expected workload.
Implementing	Introduce changes or new capacity to meet new capacity requirements.
Modeling	Model and forecast the behavior of IT resources to determine future capacity trends and requirements.
Application sizing	Take into consideration the predicted resources for new capacity. When designing an application, determine its size (number of concurrent users that can be handled, number of transactions and data storage requirements) and required server capability, memory size, processing power, etc.

4.7 Problem and Incident Management

Computer resources, like any other organizational asset, should benefit the entire organization. Among other uses, they should provide information to authorized personnel when and where it is needed and at an identifiable and auditable cost. Computer resources include hardware, software, telecommunications, networks, applications and data.

Controls over these resources are sometimes referred to as general controls. Effective control over computer resources is critical because of the reliance on computer processing for managing the business.

 ©ISACA. All Rights Reserved.

4.7.1 Problem Management

Problem management aims to resolve issues through the investigation and in-depth analysis of a major incident or several similar incidents to identify the root cause. Standard methodologies for root cause analysis include the development of fishbone/Ishikawa cause-and-effect diagrams, brainstorming, and the 5 Whys—an iterative question-asking technique used to explore the cause-and-effect relationships underlying a problem.

After a problem has been identified and analysis has determined a root cause, the condition becomes a known error. A workaround can then be developed to address the error state and prevent future occurrences of related incidents. The problem is then added to the known error database (KEDB). The goal is to proactively prevent the recurrence of the error elsewhere or, at a minimum, have a workaround that can be provided immediately should the incident recur.

Problem management and incident management are related but have different methods and objectives. Problem management's objective is to reduce the number and/or severity of incidents, while incident management's objective is to return the affected business process to its normal state as quickly as possible, minimizing the impact on the business. Effective problem management can show a significant improvement in the quality of service of an IS organization.

4.7.2 Process of Incident Handling

Incident management is one of the critical processes in IT service management (ITSM). See section 4.10 IT Service Level Management for more information. IT needs to be addressed continuously to better serve the customer. Incident management focuses on providing increased continuity of service by reducing or removing the adverse effect of disturbances to IT services. It covers almost all nonstandard operations of IT services —thereby defining the scope to include any nonstandard event. In addition to the initiation, other steps in the incident life cycle include classification, assignment to specialists, resolution and closure.

Any incident handling process must prioritize items after determining their impact and urgency. For example, there could be a situation in which a service request from the chief information officer (CIO) for a printer problem arrives at the same time as a request from the technology team to attend to a server crash. IS management should have parameters for assigning priorities to these incidents in light of their urgency and impact.

Unresolved incidents are escalated based on the criteria set by IS management. Incident management is reactive, and its objective is to respond to and resolve issues restoring normal service (as defined by the SLA) as quickly as possible. Formal SLAs are sometimes in place to define acceptable ranges for various incident management statistics.

4.7.3 Detection, Documentation, Control, Resolution and Reporting of Abnormal Conditions

Because of the highly complex nature of software and hardware and their interrelationships, a mechanism should exist to detect and document any abnormal conditions that could indicate an error. This documentation generally takes the form of an automated or manual log. See **figures 4.13** and **4.14**.

Figure 4.13—Typical Errors Logged

• Application errors • System errors • Operator errors	• Network errors • Telecommunication errors • Hardware errors

Figure 4.14—Items to Appear in an Error Log Entry

• Error date • Error resolution description • Error code • Error description • Source of error • Escalation date and time • Initials of the individual responsible for maintaining the log	• Initials of the individual responsible for closing the log entry • Department/center responsible for error resolution • Status code of problem resolution (e.g., problem open, problem closed pending some future specified date or problem irresolvable in the current environment) • Narrative of the error resolution status

The ability to add to the error log should not be restricted for control purposes. However, the ability to update the error log should be restricted to authorized individuals, and the updates should be traceable. Proper separation

©ISACA. All Rights Reserved.

of duties requires that the ability to close an error log entry be assigned to a different individual than the one responsible for maintaining or initiating the error log entry.

IS management should ensure that the incident and problem management mechanisms are properly maintained and monitored and that outstanding errors are addressed and resolved promptly.

IS management should develop operations documentation to ensure that procedures exist to escalate unresolved problems to a higher IS management level. While there are many reasons why a problem may remain outstanding for a long period of time, it is not acceptable for a problem to remain unresolved indefinitely. The primary risk resulting from a lack of attention to unresolved problems is the interruption of business operations. An unresolved hardware or software problem could potentially corrupt production data. Problem escalation procedures should be well documented. IS management should ensure that the problem escalation procedures are being adhered to properly. Problem escalation procedures generally include:

- Names/contact details of individuals who can deal with specific types of problems
- Types of problems that require urgent resolution
- Problems that can wait until normal working hours

Problem resolution should be communicated to appropriate systems, programming, operations and user personnel to ensure that problems are resolved in a timely manner. The IS auditor should examine problem reports and logs to ensure problems are assigned to the individuals or groups most capable of resolving them and are resolved on time.

The departments and positions responsible for problem resolution should be part of problem management documentation. This documentation must be maintained properly to be useful.

4.7.4 Support/Help Desk

The responsibility of the technical support function is to provide specialist knowledge of production systems to identify and assist in system change/development and problem resolution. In addition, technical support is responsible for apprising management of current technologies that may benefit overall operations.

Procedures covering the tasks to be performed by the technical support personnel that follow an organization's overall strategies and policies must be established. **Figure 4.15** illustrates common support functions.

Support is generally triaged when a help desk ticket/call is initiated and then escalated based on the complexity of the issue and the level of expertise required to resolve the problem.

The primary purpose of the help desk is to serve the user. The help desk personnel must ensure that all hardware and software incidents that arise are fully documented and escalated based on the priorities established by management. In many organizations, the help desk means different things. However, the basic function of the help desk is to be the first, single and central point of contact for users and follow the incident management process.

Figure 4.15—Typical Support Functions

- Determine the source of computer incidents and take appropriate corrective actions.
- Initiate problem reports, as required, and promptly resolve incidents.
- Obtain detailed knowledge of the network, system and applications.
- Answer inquiries regarding specific systems.
- Provide second- and third-tier support to business users and customers.
- Provide technical support for computerized telecommunications processing.
- Maintain documentation of vendor software, including issuing new releases, problem fixes and documentation of utilities and systems developed in-house.
- Communicate with information systems (IS) operations to signal abnormal patterns in calls or application behavior.

4.7.5 Network Management Tools

In an organization's modern inter-networking environment, all the tasks in **figure 4.15** can be accomplished by a set of network management tools.

Response time reports identify the time necessary for a command entered by a user at a terminal to be answered by the host system. Response time is important because end users experiencing slow response time will be reluctant to utilize IS resources to their fullest extent. These reports typically identify average, worst and best response times over a given time interval for individual telecommunication lines or systems. These reports should be reviewed by IS management and system support personnel to track potential problems. If response time is slow, all possible causes—such as I/O channel bottlenecks, bandwidth utilization and

CPU capacity—should be investigated. Various solutions should be analyzed, and appropriate and cost-justified corrective actions should be taken.

Downtime reports track the availability of telecommunication lines and circuits. Interruptions due to power/line failure, traffic overload, operator error or abnormal conditions are identified in a downtime report. If downtime is excessive, IS management should consider the following remedies:

- Add or replace telecommunications lines.
- Switch to a more dependable transmission link (such as dedicated lines versus shared lines).
- Install backup power supplies.
- Improve access controls.
- Closely monitor line utilization to better forecast user needs in the near and long term.
- Consider implementation of software-defined networking (SDN) to bundle connectivity.

Help desk reports are prepared by a team that is staffed or supported by IT technicians trained to handle problems occurring during normal IS use. An end user who encounters a problem can contact the help desk. Help desk facilities are critical to the telecommunications environment since they provide end users with an easy means of identifying and resolving problems before they significantly impact IS performance and end-user resource utilization. Reports prepared by the help desk provide a history of problems and their resolutions.

Online monitors check data transmission accuracy and errors. Monitoring can be performed by echo checking (received data are bounced back to the sender for verification) and status checking all transmissions, ensuring that messages are not lost or transmitted more than once.

Network monitors provide a real-time display of network nodes and statuses.

Network (protocol) analyzers are diagnostic tools attached to a network link that use network protocols' intelligence to monitor the packets flowing along the link and produce network use reports. Network analyzers are typically hardware-based and operate at the data link and/or network level. Output includes the following information:

- Protocol(s) in use
- Type of packets flowing along the monitored link
- Traffic volume analysis
- Hardware errors, noise and software problems
- Other performance statistics (e.g., percentage of used bandwidth)
- Problems and possible solutions

SNMP is a TCP/IP-based protocol that monitors and controls variables throughout the network, manages configurations and collects statistics on performance and security. A master console regularly polls all network devices and displays the global status. SNMP software is capable of accepting specific operator requests in real time. Based on the operator's instructions, SNMP software sends specific commands to an SNMP-enabled device and retrieves the required information. To perform all these tasks, each device (e.g., all routers, switches, hubs, PCs and servers) must have an SNMP agent running. SNMP communication occurs between all the agents and the console. To send and receive data for managing infrastructure equipment, SNMP is often used. Because sensitive information is frequently included in these messages, using SNMP version 2 or 3 (abbreviated SNMPV2 or SNMPV3) to incorporate encryption and additional security features is advised.

Internet Control Message Protocol (ICMP) is a network monitoring protocol specially designed for error reporting. Network devices such as routers make use of ICMP to send error messages for situations in which a host/client cannot be reached or requested information is not available. Unlike SNMP, ICMP does not exchange data within or between systems. It is a component of the TCP/IP stack, acting as a support to Internet protocol. ICMP forms a base for a quick understanding of the source and cause of errors while carrying out most of the common utilities used in completing a day-to-day task on the Internet.

4.7.6 Problem Management Reporting Reviews

The audit approach shown in **figure 4.16** should be considered when reviewing problem management reporting.

©ISACA. All Rights Reserved.

Figure 4.16—Problem Management Reporting Reviews

Areas to Review	Questions to Consider
• Interviews with information systems (IS) operations personnel	• Have procedures been developed and documented to guide IS operations personnel in promptly logging, analyzing, resolving and escalating problems to follow management's intent and authorization?
• Performance records • Outstanding error log entries • Help desk call logs	• Do problems exist during processing? • Are the reasons for delays in application program processing valid? • Are significant and recurring problems identified, and are actions taken to prevent their recurrence? • Were processing problems resolved promptly, and were the resolutions complete and reasonable? • Are there any reoccurring problems that are not being reported to IS management?
• Procedures used by the IT department • Operations documentation	• Are procedures for recording, evaluating and resolving or escalating any operating or processing problems adequate? • Are procedures used by the IT department to collect statistics regarding online processing performance adequate, and is the analysis accurate and complete? • Are all problems identified by IS operations being recorded for verification and resolution?

4.8 IT Change, Configuration and Patch Management

Change control procedures are among the more encompassing functions of change management. They are established by IS management to control the movement of application changes (programs, jobs, configurations, parameters, etc.) from the test environment, where development and maintenance occur, to the QA environment, where thorough testing occurs, to the production environment. Typically, IS operations staff is responsible for ensuring the integrity of the production environment and often serve as the final approvers of any changes to production.

Change management serves various IT purposes, including hardware modifications, installation or upgrades of new off-the-shelf application releases, application patching, and configuration adjustments for network devices such as firewalls, routers and switches.

The procedures associated with this process ensure that:

- All relevant personnel are informed of the change and when it is happening.
- The system, operations and program documentation are complete, up-to-date and compliant with the established standards.
- Job preparation, scheduling and operating instructions have been established.
- User and project management teams have reviewed and approved system and program test results.
- Data file conversion, if necessary, has occurred accurately and completely, as evidenced by user management review and approval.
- System conversion has occurred accurately and completely, as evidenced by user management review and approval.
- All aspects of jobs turned over have been tested, reviewed and approved by control/operations personnel.
- Legal or compliance aspects have been considered.
- If necessary, the risk of adversely affecting the business operation is reviewed and a rollback plan is developed to back out of the changes.

Apart from change control, standardized methods and procedures for change management are needed to ensure and maintain agreed-on quality service levels. These methods are aimed at minimizing the adverse impact of any probable incidents triggered by a change that may arise.

This objective is achieved through change request process formalization and documentation, authorization, testing, implementation and user communication. Change requests are often categorized into emergency, major and minor changes. There may be different change management procedures for each type of change.

4.8.1 Patch Management

Patch management involves acquiring, testing and installing multiple patches (code changes) to an administered computer system to maintain up-to-date

 ©ISACA. All Rights Reserved.

software and address security risk. Patch management tasks include:

- Maintain current knowledge of available patches.
- Decide which patches are appropriate for particular systems.
- Ensure that patches are installed properly; test systems after installation.
- Document all associated procedures, such as specific configurations required.

Several products are available to automate patch management tasks. However, patches can be ineffective and cause more problems than they fix. To avoid problems, system administrators should perform backups and test patches on non-critical systems before installation. Patch management can be viewed as part of change management.

See chapter 3 Information Systems Acquisition, Development and Implementation for details on program change controls.

4.8.2 Release Management

Software release management is the process of making software available to users. The term release is used to describe a collection of authorized changes. The release will typically consist of several problem fixes and enhancements to the service.

Each release, whether major or minor, is assigned a unique identity. In certain cases, minor fixes can inadvertently lead to new issues. Major releases that have undergone comprehensive testing are less likely to have such problems. Due to limitations in time, space and resource testing, a partial release, referred to as a delta release, might be deployed. The delta release only includes items that have been modified since the last release.

Releases are controlled, and if any problems arise in a new release, it should be possible to back out completely and restore the system to its previous state. Suitable contingency plans may be developed for taking appropriate action if a system is not completely restorable. These plans must be developed before any new release is implemented. **Figure 4.17** shows some of the principal types of releases.

Figure 4.17—Types of Releases

Major releases	Normally contain a significant change or addition of new functionality. A major upgrade or release usually supersedes all previous minor upgrades. Grouping together several changes facilitates comprehensive testing and planned user training. Large organizations typically have a predefined timetable for implementing major releases throughout the year (e.g., quarterly). Smaller organizations may have only one release during the year or numerous releases if an organization is quickly growing.
Minor software releases	Upgrades; normally contain small enhancements and fixes. A minor upgrade or release usually supersedes all preceding emergency fixes. Minor releases generally fix small reliability or functionality problems that cannot wait until the next major release. The entire release process should be followed to prepare and implement minor releases. These tasks will likely take less time because the development, testing and implementation activities are less demanding than with major releases.
Emergency software releases	Emergency releases are fixes that require implementation as quickly as possible to prevent significant user downtime to business-critical functions. Depending upon the required urgency of the release, limited testing and release management activities are executed before implementation. Such changes should be avoided whenever possible because they increase the risk of introducing errors.

Many new system implementations will involve phased delivery of functionality and thus require multiple releases. In addition, planned releases will offer an ongoing process for system enhancement.

The main roles and responsibilities in release management should be defined to ensure that everyone understands their role and level of authority and those of others involved in the process. The organization should choose the most appropriate approach, depending on the size and nature of the systems, the number and frequency of releases required and any special needs of the users (e.g., if a phased rollout is required over an extended

©ISACA. All Rights Reserved.

period). All releases should have a unique identifier that can be used by configuration management.

Planning a release involves:
- Gaining consensus on the release's contents
- Agreeing to the release strategy (e.g., the phasing over time and by geographical location, business unit and customers)
- Producing a high-level release schedule
- Planning resource levels (including staff overtime)
- Agreeing on roles and responsibilities
- Producing rollback plans
- Developing a quality plan for the release
- Planning acceptance of support groups and the customer

While the change management process requires that all changes go through robust testing and approval, release management puts the software changes into production.

4.8.3 IS Operations

IS operations consists of processes and activities that support and manage the entire IS infrastructure, systems, applications and data, focusing on day-to-day activities.

IS operations staff is responsible for the accurate and efficient operation of the network, systems and applications and for delivering high-quality IS services to business users and customers.

Tasks of the IS operations staff include:
- Execute and monitor scheduled jobs.
- Facilitate timely backup.
- Monitor unauthorized access and use of sensitive data.
- Monitor and review the extent of adherence to IS operations procedures as established by IS and business management.
- Participate in tests of DRPs.
- Monitor the performance, capacity, availability and failure of information resources.
- Facilitate troubleshooting and incident handling.

Procedures detailing instructions for operational tasks and procedures coupled with appropriate IS management oversight are necessary parts of the IS control environment.

The documentation should include:
- Operations procedures that are based on operating instructions and job flows for computer and peripheral equipment
- Procedures for monitoring systems and applications
- Procedures for detecting systems and applications errors and problems
- Procedures for handling IS problems and escalation of unresolved issues
- Procedures for backup and recovery

IS Operations Reviews

Because processing environments vary among installations, a tour of the information processing facility (IPF) gives the IS auditor a better understanding of operations tasks and procedures and the control environment. Audit procedures should include those shown in **figure 4.18**.

Figure 4.18—IS Operations Reviews

Areas to Review	Questions to Consider
Observation of information systems (IS) personnel	• Have controls been put in place to ensure the efficiency of operations and adherence to established standards and policies? • Is adequate supervision present? • Have controls been implemented regarding IS management review, data integrity and security?
Operator access	• Is access to files and documentation libraries restricted to operators? • Are responsibilities for the operation of computers and related peripheral equipment limited? • Is access to correcting program and data problems restricted? • Should access to utilities that allow system fixes to software and/or data be restricted? • Is access to production source code and data libraries (including run procedures) limited?

 ©ISACA. All Rights Reserved.

Figure 4.18—IS Operations Reviews (cont.)

Areas to Review	Questions to Consider

Operator manuals	• Are instructions adequate to address:
	  ▪ The operation of the computer and its peripheral equipment?
	  ▪ Startup and shutdown procedures?
	  ▪ The event of machine/program failure?
	  ▪ Records to be retained?
	  ▪ Routine job duties and restricted activities?

Access to the library	• Is the librarian prevented from accessing computer hardware? • Does the librarian have access only to the data management system? • Is access to library facilities provided to authorized staff only? • Is the removal of files restricted by production scheduling software? • Does the librarian handle the receipt and return of foreign media entering the library? • Are logs of the sign-in and sign-out of data files and media maintained?

Contents and location of offline storage	• Are the contents of offline file storage media containing production system programs and data clearly labeled?
	• Are offline library facilities located away from the computer room?
	• Are policies and procedures adequate for:
	  ▪ Administering the offline library?
	  ▪ Checking out/in media, including requirements for signature authorizations?
	  ▪ Identifying, labeling, delivering and retrieving offsite backup files?
	  ▪ Encrypting offsite backup files (especially those that physically move between locations)?
	  ▪ Inventorying the system for onsite and offsite media, including the specific storage locations of all media?
	  ▪ Secure disposal/destruction of media, including requirements for signature authorizations?

File-handling procedures	• Have procedures been established to control the receipt and release of files and secondary storage media to/from other locations? • Are internal labels used to help ensure that the correct media are mounted for processing? • Are established procedures adequate and in alignment with management's intent and authorization? • Are the procedures being followed?
Data entry	• Are input documents authorized, and do the documents contain appropriate signatures? • Are batch totals reconciled? • Does separation of duties exist between the person who keys the data and the person who reviews the keyed data for accuracy and errors? • Are control reports being produced? Are the reports accurate? Are the reports maintained and reviewed?
Lights-out operations	• Remote access to the master console is often granted to standby operators for contingency purposes such as automated software failure. Is security access sufficient to guard against unauthorized use? • Do contingency plans allow for properly identifying a disaster in an unattended facility? • Are the automated operation software and manual contingency procedures documented and tested adequately at the recovery site? • Are proper program change controls and access controls present? • Are software tests performed periodically, especially after changes or updates are applied? • Do assurances exist that errors are not hidden by the software and that all errors result in operator notification?

©ISACA. All Rights Reserved.

4.9 Operational Log Management

Operational logs, or audit trails, track and log activities within an application, providing a historical record of actions performed, system events and user interactions. Logs help with monitoring and investigating security incidents and ensure accountability. In some cases, log monitoring is used as a compensating control when establishing a primary control is impossible—when small organizations cannot completely separate duties due to limited staff, for example. Logs may be monitored to ensure against any individuals abusing their elevated access.

Operational log management involves collecting, monitoring, analyzing and storing logs generated by various systems, applications and devices within an organization's IT infrastructure. Logs are records that capture events, activities and errors within the IT environment. Within any IT environment, there can be many different types of logs.

Log records contain information that establishes:

- The type of event that occurred
- The time the event occurred
- The location where the event occurred
- Source of the event
- Outcome of the event
- Identity of any individuals, subjects, or objects/ entities associated with the event

4.9.1 Types of Logs

Nearly every component in a network has the potential to generate a log with the type of information it creates, gathers or interacts with. The most common types of logs include:

- **Event log**—Records information such as network traffic and use, login attempts, failed password attempts and application events. Event logs are very common and are often used as detective controls after breaches occur.
- **Server log**—Contains a text document record of activities related to a specific server during a specific period.
- **System log**—Records OS events such as startup messages, system changes, unexpected shutdowns, errors and warnings and other important processes.
- **Access log**—Lists the people or bots accessing certain applications or files. Access logs are often used as a compensating control when establishing a general or application control, like separation of duties, is not feasible.
- **Change log**—Includes a chronological list of changes to an application or file. Change logs are included in change management controls to ensure that authorized individuals perform all system modifications appropriately.
- **Availability log**—Tracks system performance, uptime and availability. These logs are used to determine if SLAs were met.
- **Resource log**—Provides information about connectivity issues and capacity limits. Network administrators often monitor these logs to ensure the environment is sized appropriately. They also can serve as an early indicator of a network breach.
- **Threat log**—Contains information about system, file or application traffic that matches a predefined security profile within a firewall. Threat logs are designed to trigger alerts as an early warning system for potential breaches.
- **Database log**—Tracks changes made to a database, including insertions, updates and deletions of records. Database logs help maintain data integrity, troubleshoot issues, evaluate the efficacy of the database structure and assess database security.
- **Error log**—Various applications produce error logs when a system experiences a problem. Error logs often include details about the nature of the event that are helpful in resolving it.
- **Firewall log**—Records incoming and outgoing network traffic that traverses through the firewall to identify potential threats.
- **Operating system log**—Identifies data file versions used for production processing, evaluates the programs scheduled and run, and discovers utilities or service ID usage. OS logs are used to evaluate OS activities to ensure that the integrity of the OS has not been compromised due to improper changes to system parameters and libraries.
- **Application log**—Evaluates overall efficiency of applications and verifies that changes to the application or its data were made following the proper authorization processes. Application logs can also be used to assess unauthorized access and use, and to identify suspicious user behavior.
- **Access control log**—Evaluates access controls for critical data files/databases and programs and for the security facilities that are active in communications systems, DBMSs and applications.

Many intruders will attempt to alter logs to hide their activities. Secure logging is needed to preserve evidence authenticity if logs are required for legal/court use. It is important that logs are protected from alteration. A common way to achieve this is to capture, centralize

 ©ISACA. All Rights Reserved.

and analyze the logs on a secure server using security information and event management (SIEM) software.

4.9.2 Log Management

The purpose of operational log management is to ensure the availability, integrity and confidentiality of log data, which play a crucial role in IT operations, security and compliance. Once the logs are created, the organization must actively monitor the data as part of a control process targeting specific risk. Log management follows a six-step cycle (**figure 4.19**).

Figure 4.19—Log Management Cycle



A log management infrastructure typically comprises the following three tiers:

1. **Log generation**—The log generation tier consists of the hosts that generate the log data. These hosts typically log client applications or services and send their data through networks to log servers in the second tier. However, other hosts send their logs through other means. For instance, they can permit servers to authenticate them and retrieve copies of the log files.
2. **Log analysis and storage**—Log servers receive logs or copies of log data from the hosts found in the log generation tier. This data is transferred to the servers either in real time or in occasional batches, depending on specific schedules or the amount of log data awaiting transfer. Servers that receive log data from multiple log generators are referred to as collectors or aggregators. In terms of storage requirements, the log data may be stored on the log servers or on separate database servers.
3. **Log monitoring**—The log monitoring tier contains consoles for monitoring and reviewing the log data and the results of automated log analysis. The consoles can be used in the generation of reports and to provide management for the log servers and clients. In terms of good security practices, console user privileges should be provided using the POLP.

In determining what event types require logging, organizations should consider monitoring and auditing each of the controls to be implemented. After detecting an attack, log analysis can help enterprises understand its extent. Complete logging records can show when and how the attack occurred, what information was accessed, and if data was exfiltrated. Retention of logs is also critical in case a follow-up investigation is required or if an attack remains undetected for a long period of time.

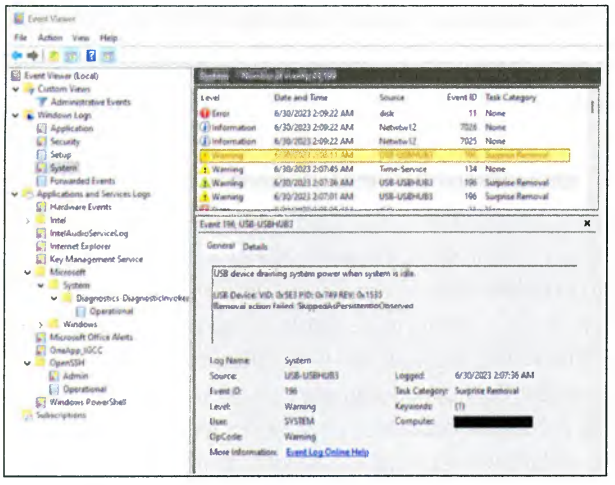
Data Collection

Operational log management involves systematically collecting logs from different sources, such as servers, network devices, databases, OSs and applications. Many systems have a built-in logging function. However, logging may involve deploying log collection agents or configuring centralized solutions for systems without this built-in feature for organizations that want to centralize data collection. At a minimum, logging should capture a timestamp for when an action occurred, user information for who took the action and event information for what action was taken. Depending on the type of log, other information should also be captured.

Figure 4.20 shows an example of a common Windows System Log. The log indicates that the user inappropriately removed a USB without ejecting the drive. The event is captured with a timestamp and description.

©ISACA. All Rights Reserved.

Figure 4.20—Windows System Log Example



Generating Alerts

After the data is collected, the next step is to alert the appropriate individuals when there is a potential problem or threat. Since logs capture different types of information, each log may need to alert a different person or team. For example, a Syslog event may only require alerting the end user. In contrast, a threat log will likely require alerting the IT security team of an attempted network breach. Alerts are designed to inform people so they can take immediate action. The IS auditor ensures that alerts are being generated based on appropriate parameters, that alerts are actually being received and that action is taken promptly based on the criticality of the alert.

Storing and Protecting Logs

Operational log management protects log data from unauthorized access, modification or deletion. As a best practice, many organizations implement a centralized log management system that collects and stores logs from various sources. Centralization facilitates easier log analysis, correlation and monitoring. Logs should adhere to a defined retention policy based on regulatory requirements and business needs. Log data is stored in secure locations to prevent unauthorized access and tampering. The use of encrypted file systems or databases with offsite backups should be considered to protect the confidentiality and integrity of log information. Access controls should be implemented to restrict log data access to authorized personnel only, using role-based access controls to ensure that individuals have appropriate permissions based on their roles and responsibilities. Finally, a regular, automated backup schedule should be established to prevent log data loss in case of hardware failures, system crashes or other incidents. Offsite backups or cloud storage options also should be considered for increased redundancy and disaster recovery.

Analyzing Log Data

Log monitoring includes two analyses. The first is an immediate threat assessment with an alert sent to individuals for action. Setting up real-time alerting mechanisms based on specific log events or patterns is crucial for timely response to critical incidents. When specific conditions or thresholds are met, alerts can be generated to notify IT teams or trigger automated actions. The second assessment involves using log analysis tools and techniques to detect anomalies, errors, security breaches or performance issues by looking for trends and patterns from correlated data. The deeper analysis aggregates and correlates data from multiple logs to gain insights into system behavior, identify patterns and troubleshoot problems. Log analysis techniques may involve parsing log entries, correlating events and applying data analysis methods to detect trends, anomalies or potential security threats.

In log parsing, logs from different systems and applications may have different formats and structures. Since the data is coming from different sources, it must be normalized. Normalizing log data involves standardizing different log formats, timestamps and data elements. It ensures consistency and facilitates effective log analysis and comparison across multiple sources. Log parsing techniques extract relevant information from log entries and convert them into a consistent format that is easier to analyze. Regular expressions and parsing libraries are commonly used for this purpose. Event data is then correlated. Event correlation involves analyzing log entries to identify relationships and associations between events. This technique helps uncover patterns and dependencies that may indicate security incidents, performance issues or operational anomalies. Tools like SIEM systems provide event correlation capabilities.

Once the data is correlated, trends and patterns may emerge. Pattern matching techniques involve searching for predefined patterns within log data. This approach helps identify specific events or behaviors of interest, such as known attack signatures or error conditions. Pattern matching can be done using specialized log analysis software. Statistical analysis techniques can also be employed to analyze log data and identify outliers, trends or abnormal behaviors. Statistical methods like mean, median, standard deviation or time-series analysis

 ©ISACA. All Rights Reserved.

can help detect anomalies and unusual patterns in log entries.

Reporting Concerns

The information gathered from log management should be communicated to the appropriate levels within the organization. The IT security team establishes clear and documented procedures for reporting concerns from log monitoring. The team should define the steps to be followed, specifying who should be notified, how to escalate issues and the appropriate channels for reporting. Incidents uncovered during analysis should be classified based on the severity or criticality of the reported concerns based on predefined criteria. Classification helps in prioritizing the response and allocating appropriate resources.

Next, the team develops and maintains an incident response plan that outlines the steps to be taken when concerns are raised. The plan should include roles, responsibilities, communication protocols, containment and mitigation strategies and post-incident analysis procedures. Concerns must be reported once they are identified. Delays in reporting can lead to further damage or compromise of systems and data. The reporting process should be efficient, and all stakeholders should be informed promptly. The reporting process must also adhere to any applicable regulatory or legal requirements. There should be proper documentation of reported concerns, actions taken and outcomes for auditing, compliance and future reference.

The report should clearly communicate the nature of the concern, providing relevant details and contextual information while avoiding unnecessary jargon. The use of concise and easily understandable language is necessary to ensure the report is comprehensible to technical and non-technical stakeholders. Information such as the source of the concern (e.g., specific event logs, alerts or indicators), affected systems or assets, potential impact and any actions taken or recommended should be included. The report should include recommended containment, mitigation and remediation action plans based on best practices, industry standards and the organization's incident response plan. Action plans should contain a process for follow-up and ongoing communication regarding reported concerns to keep stakeholders informed of the progress, status and resolution of the reported concerns.

Log Management Integration With SIEM and IT Governance

Operational log management is closely tied to SIEM systems and IT governance frameworks. In many ways, operational logs are a foundation for SIEM and IT governance programs.

Log management and SIEM are related concepts but serve different purposes in cybersecurity. Logs serve as a valuable data source for SIEM tools, enhancing threat detection and response capabilities. While log management focuses on storing and analyzing logs, SIEM extends those capabilities by integrating data from multiple log sources and incorporating real-time monitoring, event correlation and threat detection to enhance an organization's security posture and incident response capabilities. Log management can be a stand-alone function or an essential component of a SIEM solution, depending on the organization's security needs, resources and compliance requirements.

Additionally, log management aligns with IT governance frameworks, such as COBIT or Information Technology Infrastructure Library (ITIL), ensuring adherence to industry best practices. Log management plays a crucial role in incident management by providing valuable data for incident detection, diagnosis and resolution. Logs can be used to identify the root cause of incidents, track the sequence of events leading up to an incident and analyze the impact on services. Log data can help expedite the incident resolution process, minimize downtime and restore services to normal operation.

Log management contributes to problem management by providing insights into recurring incidents or underlying issues. Analyzing logs can help identify patterns, trends or commonalities that indicate systemic problems. Log data can be used to support problem investigation, root cause analysis and the development of permanent solutions or workarounds.

Log management supports change management by providing visibility into the effects of changes made to the IT environment. Logs can help verify whether changes were successfully implemented, identify any unexpected consequences or issues resulting from changes and assess the overall impact on IT services. Logs can be reviewed before, during and after changes are made to validate the outcomes and ensure compliance with change management processes.

Log management enables the monitoring of IT services through the collection and analysis of logs related to service performance, availability and security. Logs can

©ISACA. All Rights Reserved.

be used to generate reports on service-level metrics such as uptime, response times, error rates or compliance with SLAs. These reports help assess service quality, identify improvement areas and demonstrate compliance with ITIL and other ITSM requirements.

Logs contain valuable information about the configuration of systems, applications and devices. Log management can support configuration management by providing an audit trail of configuration changes, capturing configuration-related events and assisting in configuration reconciliation or verification.

Logs can be a rich source of knowledge and insights for IT support teams. Log management systems can contribute to knowledge management processes by facilitating capturing, organizing and retrieving relevant log data. Log entries can be used to identify the need to create knowledge articles, troubleshooting guides or FAQs that assist support staff in resolving incidents or problems efficiently.

Operational log management as an IT control ensures that an organization has visibility into its IT infrastructure, monitors events effectively, detects anomalies or security incidents promptly and maintains compliance with relevant regulations and policies.

4.10 IT Service Level Management

The fundamental premise associated with ITSM is that IT can be managed through a series of discrete processes that provide service to the business. Although each process area may have different and distinct characteristics, processes are highly interdependent. After defining the processes, services can be better managed through SLAs that maintain and improve customer satisfaction (i.e., with the end business).

ITSM focuses on business deliverables and covers infrastructure management of IT applications that support and deliver IT services. This management includes fine-tuning IT services to meet the changing demands of the enterprise and measuring and demonstrating improvements in the quality of IT services offered with a reduction in the cost of service in the long term.

IT services can be better managed with SLAs, and the services offered form a basis for such agreements. There is a possibility of a gap between customer expectations and the services offered, and this is narrowed by an SLA, which completely defines the nature, type, time and other relevant information for the services being offered. SLAs can also be supported by operational level agreements (OLAs), internal agreements covering the delivery of services that support the IT organization's delivery of services.

For example, when a complaint is received, the help desk looks for an available solution from the KEDB after classifying and storing the complaint as an incident. Repeated or major incidents may lead to problems that require a problem-management process. If changes are needed, the change management group of the process/program can provide a supporting role after consulting the configuration management group.

Any required change goes through the change management process, whether it originated as a solution to a problem, an enhancement or something else. The cost-benefit and feasibility studies are reviewed before the changes are accepted and approved. The risk of the changes should be studied, and a fallback plan should be developed. The change may be for one configuration item or multiple items, and the change management process invokes the configuration management process.

For example, the software can comprise multiple systems, each containing different programs and each program having different modules. Configurations can be maintained at the system, program or module levels. The organization may have a policy providing that any changes made at the system level be released as a new version. It may also decide to release a new version if changes are made at the program level for another application.

Service management metrics should be captured and appropriately analyzed to enhance the quality of service. Many organizations have leveraged the ITIL and/or ISO 20000 to improve their ITSM.

ITIL was developed as a detailed framework with hands-on information for achieving successful operational service management of IT based on business value delivery.

ISO 20000 is the international ITSM standard that enables IT organizations (in-house, outsourced or external) to ensure that their ITSM processes align with business needs and international best practices.

4.10.1 Service Level Agreements

An SLA is an agreement between an IT organization and a customer that details the services to be provided. The IT organization could be an internal IT department or an external IT service provider; the customer is the business. The business may acquire IT services such as email services, an intranet, an enterprise resource planning (ERP) system, etc., from an internal IT organization. The

 ©ISACA. All Rights Reserved.

business may acquire IT services from an external IT service provider, such as Internet connectivity, hosting of a public website, etc.

An SLA describes the services in nontechnical terms from the customer's viewpoint. During the agreement period, it serves as the standard for measuring and adjusting the services.

Service-level management is the process of defining, agreeing on, documenting and managing levels of service that are required and cost-justified. Service-level management deals with more than the SLAs themselves; it includes the production and maintenance of the service catalog, service review meetings and service improvement plans (SIPs) for areas that are not achieving their SLAs.

The aim of service-level management is to maintain and improve customer satisfaction and to improve the service delivered to the customer. With a clear definition of the service level, the IT organization or service provider can design the service appropriately, and the customer can monitor the performance of the IT services. The IT organization or service provider must improve the services provided if they do not meet the SLA terms. If SLA terms are not met, the service provider may have to pay a fine or reduce its billing based on its contractual obligations.

Characteristics of IT services used to define an SLA should include accuracy, completeness, timeliness and security. Many tools are available to monitor the efficiency and effectiveness of services provided by IT personnel, including:

- **Exception reports**—These automated reports identify all applications that did not successfully complete their operations or otherwise malfunctioned. An excessive number of exceptions may indicate:
  - Poor understanding of business requirements
  - Poor application design, development or testing
  - Inadequate operating instructions
  - Inadequate operations support
  - Inadequate operator training or performance monitoring
  - Inadequate sequencing of tasks
  - Inadequate system configuration
  - Inadequate capacity management
- **System and application logs**—Logs generated from various systems and applications should be reviewed to identify all application problems. These logs provide additional useful information regarding activities performed on the computer, because most abnormal system and application events will generate a record in the logs. Because of the size and complexity of the logs, it is difficult to manually review them. Programs that analyze the system logs and report on defined items have been developed. Using this type of software, the auditor can carry out tests to ensure that:
  - Only approved programs can access sensitive data.
  - Only authorized IT personnel can access sensitive data.
  - Software utilities that can alter data files and program libraries can be used only for authorized purposes.
  - Approved programs are run only when scheduled; conversely, unauthorized runs do not occur.
  - The correct data file generation is accessed for production purposes.
  - Data files are adequately protected.
- **Operator problem reports**—These manual reports are used by operators to log computer operations problems and their resolutions. IS management should review operator responses to determine whether operator actions were appropriate or additional training should be provided.
- **Operator work schedules**—These schedules are generally maintained manually by IS management to assist in human resource planning. By ensuring proper staffing of operation support personnel, IS management is assured that the service requirements of end users will be met. This is especially important during periods of critical or heavy computer use. These schedules should be flexible enough for proper cross-training and emergency staffing requirements.

Many IT departments define the level of service they will guarantee to users of IT services. This level of service is often documented in an SLA. Defining the service level with a contractual relationship between the IT department and the end user or customer is particularly important. SLAs are often tied to chargeback systems, in which a certain percentage of the cost is apportioned from the end-user department to the IT department. When functions of the IT department are performed by a third party, it is important to have an outsourcing SLA.

Service levels are often defined to include hardware and software performance targets (such as user response time and hardware availability) but can also include a wide range of other performance measures. Such measures might be related to financial performance (e.g., year-to-year incremental cost reduction), human resources (e.g., resource planning, staff turnover, development or training) or risk management (e.g., compliance with control objectives). The IS auditor should be aware of

©ISACA. All Rights Reserved.

the different types of measures available and ensure they are comprehensive and include risk, security and control measures as well as efficiency and effectiveness measures.

4.10.2 Monitoring of Service Levels

Defined service levels must be regularly monitored by an appropriate level of management to ensure that the objectives of IS operations are achieved. It is important to review the impact on the customers and other stakeholders of the organization.

For example, a bank may monitor the performance and availability of its automated teller machines (ATMs). One of the metrics may be the availability of ATM services at expected levels (99.9 percent); however, monitoring the impact on customer satisfaction due to nonavailability may also be appropriate. An SLA of 99.9 percent means the ATM can be nonfunctional for about three and a half days each year. Similar metrics may be defined for other services like email and the Internet.

Monitoring service levels is essential for outsourced services, particularly if a third party directly provides services to an organization's customers. Failure to achieve service levels will have more of an impact on the organization than on the third party. For example, fraud due to control weakness at a third party may result in reputation loss for the organization.

It is important to note that when service delivery is outsourced, only the responsibility for service provision is outsourced—accountability is not and still rests with the organization. If the organization outsources service delivery, the IS auditor should determine how management gains assurance that the controls at the third party are properly designed and operating effectively. Several techniques can be used by management, including questionnaires, onsite visits or an independent third-party assurance report, such as a Statement on Standards for Attestation Engagements 18 (SSAE 18) SOC 1 report or AT-101 (SOC 2 and SOC 3) report.

4.10.3 Service Levels and Enterprise Architecture

Defining and implementing enterprise architecture (EA) helps an organization align service delivery (see section 2.4 Enterprise Architecture and Considerations for more information). Organizations may use multiple service delivery channels, such as mobile apps, the Internet, service outlets, third-party service providers and automated kiosks. These channels use different technologies all serviced by the same backend database.

When considering availability and recovery options, EA best helps align operational requirements to address the service delivery objectives. For example, an unacceptable recovery time may lead to choosing fault-tolerant, high-availability architecture for critical service delivery channels (see section 4.16.3 Recovery Alternatives for more information).

4.11 Database Management

DBMS software aids in organizing, controlling and using the data needed by application programs. A DBMS provides the facility to create and maintain a well-organized database. Primary functions include reduced data redundancy, decreased access time and basic security over sensitive data.

DBMS data is organized in multilevel schemes, with basic data elements such as a field (e.g., Social Security number) at the lowest level. The levels above each field have different properties depending on the architecture of the database.

The DBMS can include a data dictionary that identifies fields along with their characteristics and their uses. Active data dictionaries require entries for all data elements and assist application processing of data elements—by providing validation characteristics or print formats, for example. Passive dictionaries are only repositories of information that can be viewed or printed.

A DBMS can control user access at multiple levels:
- User and the database
- Program and the database
- Transaction and the database
- Program and data field
- User and transaction
- User and data field

Some of the advantages of a DBMS include:
- Data independence for application systems
- Ease of support and flexibility in meeting changing data requirements
- Transaction processing efficiency
- Reduction of data redundancy
- Ability to maximize data consistency
- Ability to minimize maintenance cost through data sharing
- Opportunity to enforce data/programming standards
- Opportunity to enforce data security
- Availability of stored data integrity checks

 ©ISACA. All Rights Reserved.

- Facilitation of terminal users' ad hoc access to data, especially through designed query language/ application generators

4.11.1 DBMS Architecture

Data elements required to define a database are called metadata. Metadata includes data used to define logical and physical fields, files, data relationships, queries, etc. There are three types of metadata: conceptual schema, external schema and internal schema. If the schemas are not adjusted to smoothly work together, the DBMS may not be adequate to meet users' needs.

Detailed DBMS Metadata Architecture

Within each level, there is a data definition language (DDL) component for creating the schema representation necessary for interpreting and responding to a user's request. At the external level, a DBMS will typically accommodate multiple DDLs for several application programming languages compatible with the DBMS. The conceptual level will provide appropriate mappings between the external and internal schemas. External schemas are location-independent of the internal schema.

Data Dictionary/Directory System

A data dictionary/directory system (DD/DS) helps define and store source and object forms of all data definitions for external schemas, conceptual schemas, internal schemas and all associated mappings. The data dictionary contains an index and description of all the items stored in the database. The directory describes the location of the data and the access method.

DD/DS provides the following functional capabilities:

- A DDL processor, which allows the database administrator to create or modify a data definition for mappings between external and conceptual schemas
- Validation of the definition provided to ensure the integrity of the metadata
- Prevention of unauthorized access to, or manipulation of, the metadata
- Interrogation and reporting facilities that allow the DBA to make inquiries about the data definition

DD/DS can be used by several DBMSs; therefore, using one DD/DS could reduce the impact of changing from one DBMS to another DBMS. Some of the benefits of using DD/DS include:

- Enhanced documentation
- Common validation criteria
- Facilitated programming by reducing the need for data definition
- Standardized programming methods

4.11.2 Database Structure

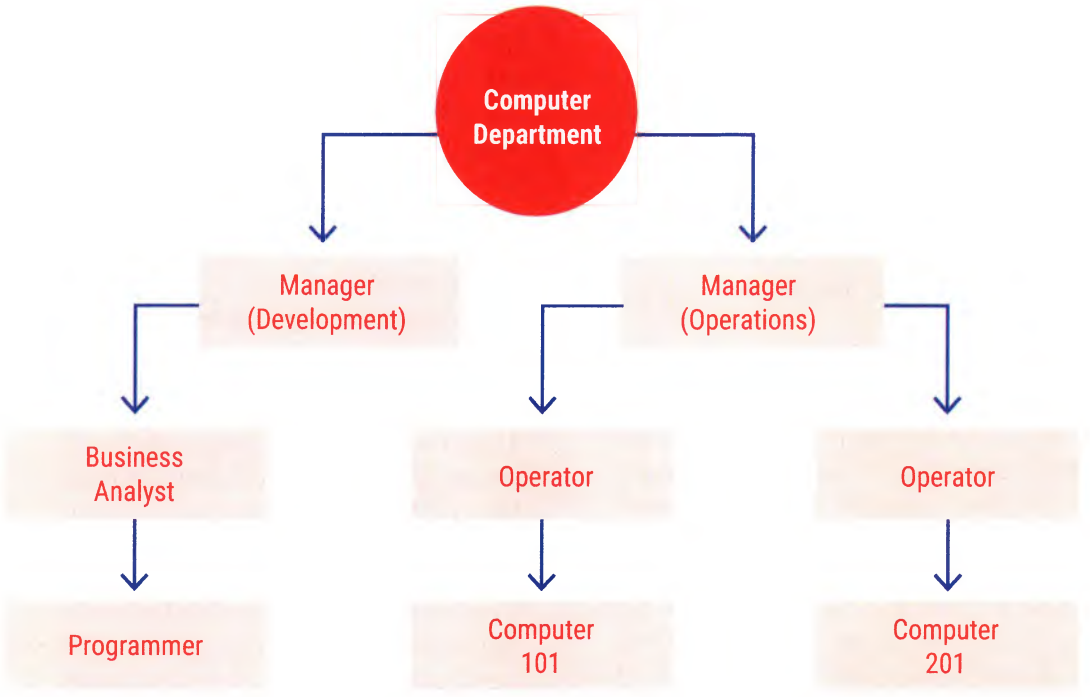
There are four major database structure types: hierarchical, network, relational and object-oriented. Most DBMSs have internal security features that interface with the OS access control mechanism/package. A combination of the DBMS security features and the security package functions is often used to cover all required security functions. Types of DBMS structures are discussed in the following paragraphs.

Hierarchical Database Model

This model has a hierarchy of parent and child data segments. To create links between them, this model uses parent-child relationships. These are 1:N (one-to-many) mappings between record types represented by logical trees, as shown in **figure 4.21**. A child has only one parent segment, so data duplication is necessary to express relationships with multiple parents. Subordinate segments are retrieved through the parent segment. Reverse pointers are not allowed. When the data relationships are hierarchical, the database is easy to implement, modify and search. The registry in Microsoft Windows is an example of a hierarchical database. This model is also used in geographic information systems.

©ISACA. All Rights Reserved.

Figure 4.21—Organization of a Hierarchical Database

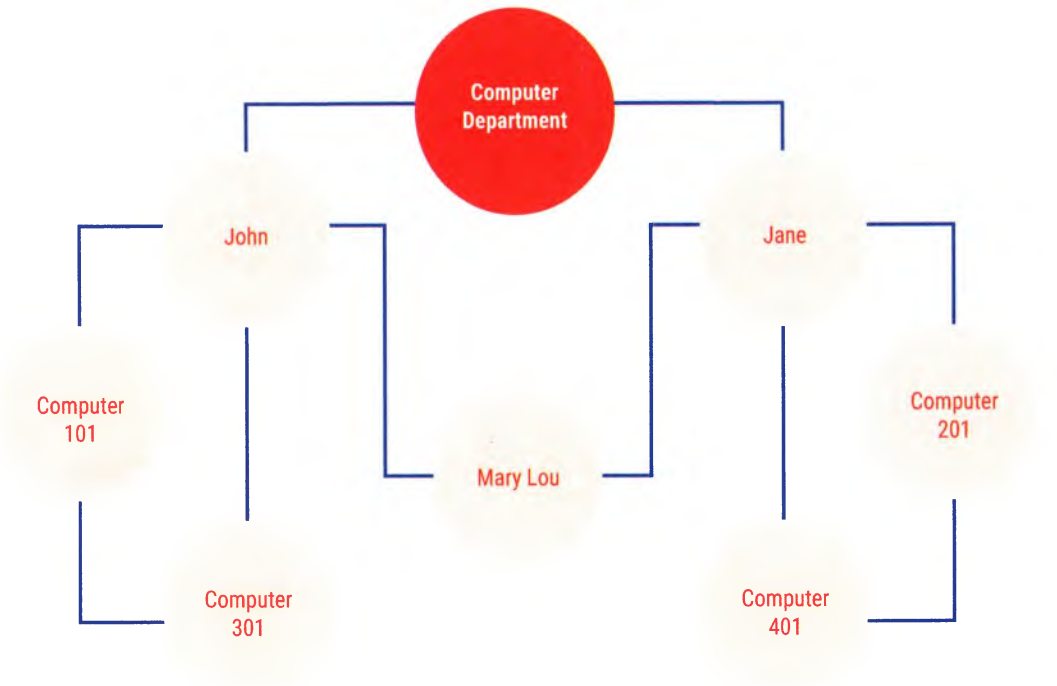


Network Database Model

The basic data modeling construct in the network model is called a set. A set is formed by an owner record type, a member record type and a name. A member record type can have that role in more than one set, so a multi-owner relationship is allowed. An owner record type can also be a member or owner in another set. Usually, a set defines a 1:N relationship, although one-to-one (1:1) is permitted. A disadvantage of the network model is that such structures can be extremely complex and difficult to comprehend, modify or reconstruct in case of failure. This model is rarely used in current environments. See **figure 4.22**. The hierarchical and network models do not support high-level queries. The user programs must navigate the data structures.

 ©ISACA. All Rights Reserved.

Figure 4.22—Organization of a Network Database



Relational Database Model

An example of a relational database is shown in **figure 4.23**. The relational model is based on set theory and relational calculations. A relational database allows the definition of data structures, storage/retrieval operations and integrity constraints. In such a database, the data and relationships among the data are organized in tables. A table is a collection of rows, also known as tuples, and each tuple in a table contains the same columns. Columns, called domains or attributes, correspond to fields. Tuples are equal to records in a conventional file structure. Relational databases are used in most common ERP Systems. Common relational database management systems (RDBMS) include Oracle, IBM, DB2 and Microsoft structured query language (SQL) Server.

Relational tables have the following properties:

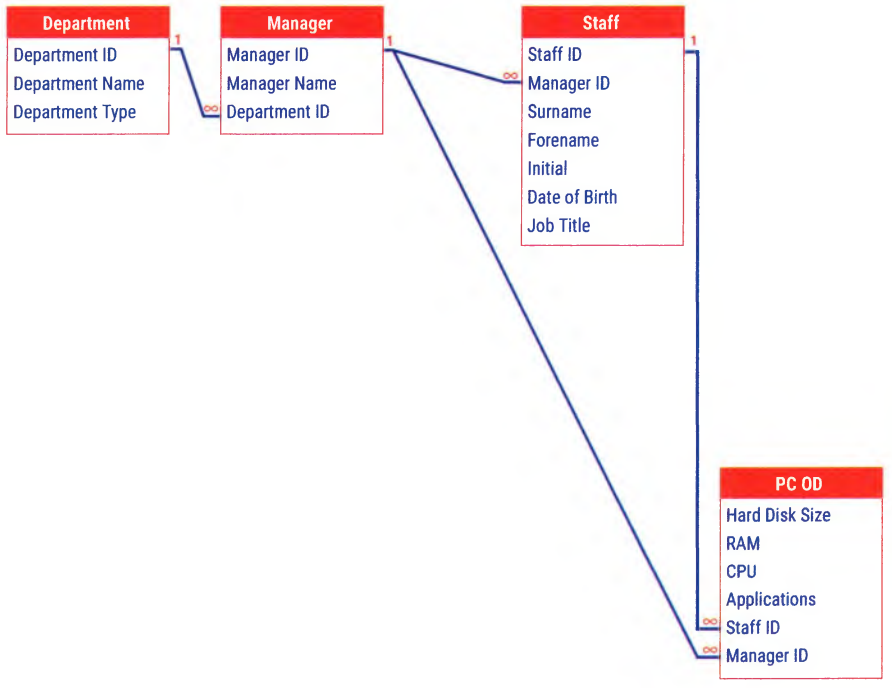
- Values are atomic (i.e., a single, irreducible unit).
- Each row is uniquely identifiable.
- Column values are of the same kind.
- The sequence of columns is insignificant.
- The sequence of rows is insignificant.
- Each column has a unique name.

Certain fields may be designated as keys, so indexing will make searches for specific field values quicker. If fields in two different tables take their values from the same set, a join operation can select related records in the two tables by matching values in those fields. This can be extended to joining multiple tables on multiple fields. These relationships are only specified at retrieval time, so relational databases are dynamic. The relational model is independent from the physical implementation of the data structure and has many advantages over the hierarchical and network database models. With relational databases, it is easier:

- To understand and implement a physical database system
- To convert from other database structures
- To implement projection and join operations (i.e., reference groups of related data elements not stored together)
- To create new relations for applications
- To implement access control over sensitive data
- To modify the database

©ISACA. All Rights Reserved.

Figure 4.23—Organization of a Relational Database



A key feature of relational databases is the use of normalization rules to minimize the amount of information needed in tables to satisfy structured and unstructured queries to the database. Generally followed, normalization rules include:

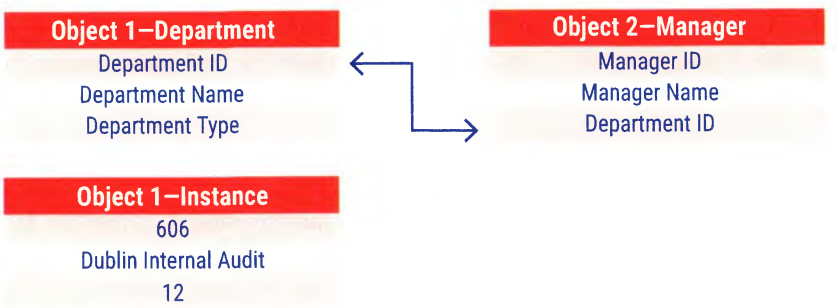
- A given instance of a data object has only one value for each attribute.
- Attributes represent elementary data items; they should contain no internal structure.
- Each tuple (record) consists of a primary key that identifies some entity and a set of zero or more mutually independent attribute values that describe the entity in some way (fully dependent on the primary key).
- Any foreign key should have a null value or should have an existing value linking to other tables; this is known as referential integrity.

Object-Oriented Database Management System

An example of an object-oriented database management system (OODBMS) is shown in **figure 4.24**. In an OODBMS, information is stored as objects (as used in object-oriented programming) rather than data (as in rational databases). This means that all of the features related to object-oriented programming can be applied, including encapsulation (i.e., the creation of data types or classes, including objects) and inheritance (i.e., classes inherit features from other classes). This results in objects that contain both executable code and data. The actual storage of the object in the database is achieved by assigning a unique identifier to each object. When referenced, these objects are loaded into virtual memory, allowing them to be found quickly. OODBMS occupies a niche in areas such as engineering, science and spatial databases and is often used when a database is made up of graphics, diagrams or sounds that cannot be easily defined or queried by relational databases.

 ©ISACA. All Rights Reserved.

Figure 4.24—Organization of an Object-Oriented Database



NoSQL

NoSQL databases were developed in response to a rise in the volume of data stored on the Internet, commonly known as big data. Much of this data is unstructured audio, video, tweets, logs, blogs, etc. This data cannot be broken out into components, which is required for a relational database; however, NoSQL databases may also support SQL, hence the term "Not only SQL." NoSQL databases may support object orientation (as per OODBMS) and other database technologies, as shown in **figure 4.25**.

Figure 4.25—NoSQL Database Technologies

Data Model	Description
Key value	All items in the database are stored as an attribute name (key) with its value.
Column-oriented	All of the values of a column are put together, followed by all the values of the next column, then the values of the next column, etc.
Graph database	The databases are based on graph theory (mathematical models of the relationship between objects).
Document-oriented	The database manages, stores and retrieves document-oriented information using storage methods such as XML and JSON.
Time series	Data points are stored and queried with timestamps (e.g., stock data, logs and sensor data).

Figure 4.25—NoSQL Database Technologies (cont.)

Data Model	Description
Spatial	The database stores and queries spatial data, such as maps, geographical and GPS coordinates.

The advantages of NoSQL databases include sharding—the ability to partition a database horizontally across database servers to spread the workload (important when dealing with big data)—and dynamic schemas—schemas do not have to be defined before adding data (as in relational databases). Common NoSQL databases include MongoDB and Cassandra.

4.11.3 Database Controls

Database integrity and availability must be maintained. This is ensured through controls that:

- Establish and enforce definition standards
- Establish and implement data backup and recovery procedures to ensure database availability
- Establish the necessary levels of access controls, including privileged access, for data items, tables and files to prevent accidental or unauthorized access
- Establish controls to ensure that only authorized personnel can update the database
- Establish controls to handle concurrent access problems, such as multiple users attempting to update the same data elements simultaneously (e.g., transaction commit, locking of records/files).
- Establish controls to ensure the accuracy, completeness and consistency of data elements and relationships in a database. It is important that these controls, if possible, be contained in the table/column definitions. In this way, there is no possibility that

©ISACA. All Rights Reserved.

these rules will be violated because of programming flaws or through the use of utilities to manipulate data.
- Use database checkpoints at junctures in the job stream that minimize data loss and recovery efforts to restart processing after a system failure
- Perform database reorganization to reduce unused disk space and verify defined data relationships
- Follow database restructuring procedures when making logical, physical and procedural changes
- Use database performance reporting tools to monitor and maintain database efficiency (e.g., available storage space, buffer size, CPU use, disk storage configuration and deadlock conditions)
- Minimize the ability to use non-system tools or other utilities (e.g., those outside security control to access the database)
- Consider implementation of database activity monitoring (DAM) technology, which can establish the security policy and monitoring, auditing and reporting over the IS aspects of a database

4.11.4 Database Reviews

An IS auditor should review the design, access, administration, interfaces, portability and database-supported IS controls when auditing a database, as shown in **figure 4.26**.

Figure 4.26—Database Reviews

Areas to Review	Questions to Consider
Logical schema	• Do all entities in the entity-relation diagram exist as tables or views? • Are all relations represented through foreign keys? • Are constraints specified clearly? • Are nulls for foreign keys allowed only when they follow the cardinality expressed in the entity-relation model?
Physical schema	• Has allocation of initial and extension space (storage) for tables, logs, indexes and temporary areas been executed based on the requirements? • Are indexes by primary key or keys of frequent access present? • If the database is not normalized, is justification accepted?
Access time reports	• Are indexes used to minimize access time? • Have indexes been constructed correctly? • Are any open searches not based on indexes justified?
Database security controls	• Are security levels for all users and their roles identified within the database, and are access rights for all users and/or groups of users justified? • Do referential integrity rules exist, and are they followed? • How is a trigger created, and when does it fire? • Is there a system for setting passwords? Does change of passwords exist, and is it followed? • How many users have been given system administrator privileges? Do these users require the privilege to execute their job function? • Has an auditing utility been enabled? Are audit trails being monitored? • Can database resources be accessed without using database management systems (DBMS) commands and structured query language (SQL) statements? • Is system administrator authority granted to the job scheduler? • Are actual passwords embedded into database utility jobs and scripts? • Has required encryption been enabled? • Are copies of production data authorized? • Are copies of production data altered or masked to protect sensitive data?
Interfaces with other programs/ software	• Are integrity and confidentiality of data unaffected by data import and export procedures? • Have mechanisms and procedures been put in place to ensure consistency and integrity during concurrent accesses?

 ©ISACA. All Rights Reserved.

Figure 4.26—Database Reviews (cont.)

Areas to Review	Questions to Consider
Backup and disaster recovery procedures and controls	• Do backup and disaster recovery procedures exist to ensure the reliability and availability of the database? • Are there technical controls to ensure high availability and/or fast database recovery?
Database-supported IS controls	• Is access to shared data appropriate? • Are adequate change procedures used to ensure the integrity of the database management software? • Is data redundancy minimized by the database management system? If redundant data exists, is appropriate cross-referencing maintained within the system's data dictionary or other documentation? • Is the integrity of the database management system's data dictionary maintained?
IT asset management	• Has an owner been designated? • Have copies of the contracts/service level agreements (SLAs) been retained? • What is the license agreement? Has compliance with it been achieved?

©ISACA. All Rights Reserved.

Page intentionally left blank

Part B: Business Resilience

Business resilience describes an organization's ability to adapt to disruptions and incidents to maintain continuous operations and protect its assets. Most organizations have some DRPs in place to recover IT infrastructure, critical systems and associated data. However, many organizations have not developed plans for how key business units will function during IT disruption. CISA candidates should be aware of the components of disaster recovery and business continuity plans (BCPs), the importance of aligning one with the other, and the need to align DRPs and BCPs with the organization's goals and risk tolerance. Also of importance are data backup, storage, retention and restoration.

4.12 Business Impact Analysis

Business impact analysis (BIA) is a critical step in developing the business continuity strategy and implementing the risk countermeasures, particularly the BCP.

BIA evaluates the critical processes (and IT components supporting them) and determines time frames, priorities, resources and interdependencies. Even if an extensive risk assessment was done before BIA, and the criticality and risk are input into BIA, the rule of thumb is to double-check. Often, the BIA uncovers some less visible but vital components that support the critical business process. The contractual commitments (in a BCP context) should also be considered if IT activities have been outsourced to third-party service providers.

To perform this phase successfully, one should understand the organization, key business processes and IT resources used by the organization to support the key business processes. Often, this understanding may be obtained from the risk assessment results. BIA requires a high level of senior management support/sponsorship and extensive IT and end-user personnel involvement. The criticality of the information resources (e.g., applications, data, networks, system software, facilities) that support an organization's business processes must be approved by senior management.

For the BIA, it is important to include all types of information resources and to look beyond traditional information resources (i.e., database servers).

Information systems consist of multiple components. Some components (e.g., database servers or storage arrays) are visible. Other components, like gateways and transport servers, are collected for the BIA from the parts of the organization that own critical processes/applications. Impact bands are developed to evaluate the impact of downtime for a particular process/application (i.e., high, medium, low). Each process's impact is estimated in time (hours, days, weeks). The same approach is used to estimate the impact of data loss. The financial impact may be estimated using the same techniques, assigning a financial value to a particular impact band if necessary.

Data for the BIA may be collected on the time frames needed to supply vital resources—how long the organization may run if a supply is broken or when the replacement has arrived. For example, how long will the bank run without plastic cards with chips to be personalized into credit cards, or when will IT need to have desktop workstations shipped in after a disaster?

There are different approaches to performing a BIA. One popular approach is a questionnaire approach, which involves developing a detailed questionnaire and circulating it to key users in IT and end-user areas. The information gathered is tabulated and analyzed. The BIA team will contact the relevant users for any additional information that may be required. Another popular approach is to interview groups of key users. The information gathered during these interview sessions is tabulated and analyzed for development of a detailed BCP plan and strategy. A third approach is to bring relevant IT personnel and end users (i.e., those owning the critical processes) together in a room to come to a conclusion regarding the potential business impact of various levels of disruptions. The latter method may be used after all the data is collected. Such a mixed group should decide quickly on acceptable downtime and vital resources.

Whenever possible, the BCP team should analyze past transaction volume to determine the impact on the business if the system was unavailable for an extended period. This would substantiate the BCP team's interview process for performing a BIA.

The three main questions that should be considered during the BIA phase are depicted in **figure 4.27**.

©ISACA. All Rights Reserved.

Figure 4.27—BIA Considerations

1. What are the different business processes? Each process needs to be assessed to determine its relative importance. Indications of criticality include:
   - The process supports health and safety, such as hospital patient records and air traffic control systems.
   - Disruption of the process causes a loss of income to the organization or exceptional, unacceptable costs.
   - The process is necessary to meet legal or statutory requirements.
   - The process affects a significant number of users or business segments.

   A process can be critical or noncritical depending on factors such as time and mode of operation (e.g., business hours or automated teller machine [ATM] operations).
2. What critical information resources are related to an organization's critical business processes? This is the first consideration because disruption to an information resource is not a disaster unless it is related to a critical business process (e.g., an organization losing its revenue-generating business processes due to an IS failure).

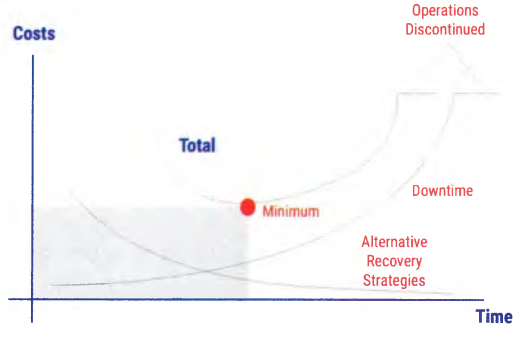
   Other examples of potential critical business processes may include:
   - Receiving payments
   - Producing goods or services
   - Paying employees
   - Advertising
   - Dispatching finished goods
   - Complying with legal and regulatory requirements
3. What is the critical recovery period for information resources in which business processing must be resumed before significant or unacceptable losses are suffered? In large part, the length of the period for recovery depends on the nature of the business or service being disrupted. For instance, financial institutions, such as banks and brokerage firms, usually have a much shorter critical recovery period than manufacturing firms. Also, the time of year or day of the week may affect the window for recovery. For example, if a bank experiences a major outage on Saturday at midnight, it has a longer time to recover than if it experiences a major outage on Monday at midnight, assuming the bank is not processing on Sunday.

Two independent cost factors should be considered when deciding on the BCP approach, as shown in **figure 4.28**. One is the downtime cost of the disaster. In the short run (e.g., hours, days and weeks), this component grows quickly, with the impact of disruption increasing the longer it lasts. At a certain point, it stops growing, reflecting the moment when the business can no longer function. The cost of downtime (increasing with time) has many components (depending on the industry and the specific company and circumstances). Among them are the cost of idle resources (e.g., in production); declines in sales (e.g., orders); financial costs (e.g., inability to invoice or collect); delays (e.g., procurement); and indirect costs (e.g., loss of market share, image and goodwill).

The other factor is the cost of the alternative corrective measures (i.e., the BCP implementation, maintenance and activation). This cost decreases with the target chosen for recovery time. The recovery cost also has many components (most of which are rigid-inelastic). These include the costs of preparing and periodically testing the BCP, maintaining offsite backup premises, insurance coverage, alternative site arrangements, etc.

The cost of alternative recovery strategies may be plotted as discrete points on the time and cost coordinates and a curve can be drawn joining the points (**figure 4.28**). The curve as a whole is representative of all possible strategies.

Figure 4.28—Disruption Costs vs. Recovery Costs



Each possible strategy has a fixed-base cost (i.e., it does not change with time until an eventual disaster occurs).

 ©ISACA. All Rights Reserved.

Note that the fixed-base cost of each possible strategy will normally differ. Suppose the business continuity strategy aims at a longer recovery time. It will be less expensive than a more stringent requirement in that case, but it may be more susceptible to downtime costs spiraling out of control. The shorter the target recovery time, the higher the fixed cost. The organization pays for the cost of planning and implementation even if no disaster occurs.

If there is a disaster, variable costs will significantly increase (e.g., a warm site contract may consist of a flat annual fee plus a daily fee for actual occupation). Also, extra staff, overtime, transportation and other logistics (e.g., staff per diem, new communication lines, etc.) need to be considered. Variable costs will depend on the strategy implemented.

Having plotted the two curves—downtime costs and costs of alternative recovery strategies—**figure 4.28** shows the total cost curve (the sum of the other two cost curves). An organization would choose the point at which those total costs are minimal.

In summary, the sum of all costs—downtime and recovery—should be minimized. The first group (downtime costs) increases with time, and the second (recovery costs) decreases with time; the sum usually is a U curve, and the lowest cost can be found at the bottom.

Note

The CISA candidate will not be tested on calculations of costs.

4.12.1 Classification of Operations and Criticality Analysis

A system's risk ranking involves determining risk based on the impact derived from the critical recovery period and the likelihood that an adverse disruption will occur. Many organizations use risk of occurrence to determine a reasonable cost of being prepared. For example, they may determine that there is a 0.1 percent risk (or 1 in 1,000) that the organization will suffer a serious disruption over the next five years. If the assessed impact of a disruption is US$10 million, the maximum reasonable cost of being prepared might be US$10 million × 0.1 percent = US $10,000 over five years. Such a method is called the annual loss expectancy (ALE). From this risk-based analysis process, critical systems can be prioritized in developing recovery strategies. The risk ranking procedure should be performed with IS processing and end-user personnel.

A typical risk ranking system may contain the classifications found in **figure 4.29**.

Figure 4.29—Classification of Systems

Classification	Description
Critical	These functions cannot be performed unless they are replaced by identical capabilities. Critical applications cannot be replaced by manual methods. Tolerance to interruption is very low; therefore, the cost of interruption is very high.
Vital	These functions can be performed manually, but only for a brief period. There is a higher tolerance to interruption than critical systems and, therefore, somewhat lower interruption costs, provided that functions are restored within a certain time frame (usually five days or less).
Sensitive	These functions can be performed manually, at a tolerable cost and for an extended period. While they can be performed manually, it is usually a difficult process that requires additional staff.
Nonsensitive	These functions may be interrupted for an extended period, at little or no cost to the company, and require little or no catching up when restored.

The next phase in continuity management is identifying the various recovery strategies and available alternatives for recovering from an interruption and/or disaster. Selecting an appropriate strategy based on the BIA and criticality analysis is the next step for developing BCPs and DRPs. The metrics that help determine the recovery strategies are the recovery point objective (RPO), recovery time objective (RTO) and mean time to repair (MTTR). For additional information on RPO, RTO and MTTR, see section 4.16 Disaster Recovery Plans.

4.13 System and Operational Resilience

System resilience refers to the ability of a system to withstand and adapt to unexpected disruptions, stresses or failures while maintaining its core functions and minimizing the impact on its overall performance. It encompasses the system's capacity to absorb shocks,

©ISACA. All Rights Reserved.

recover quickly and continue functioning effectively under adverse conditions. It includes designing systems that can withstand hardware failures, network outages, cyberattacks or software bugs. Resilient systems are built with redundant components, failover mechanisms and robust data backup strategies to ensure continuous operation and data integrity.

4.13.1 Application Resiliency and Disaster Recovery Methods

Protecting an application against a disaster entails providing a way to restore it as quickly as possible, for example, with clustering. A cluster is a type of software (agent) installed on every server (node) in which the application runs. It includes management software that permits control of and tuning the cluster behavior. Clustering protects against any single point of failure (loss of a resource that would result in loss of service or production). The main purpose of clustering is higher availability.

There are two deployment configuration types: active-passive and active-active.

In active-passive clusters, the application runs on only one (active) node. In contrast, other (passive) nodes are used only if the application fails on the active node. In this case, cluster agents constantly watch the protected application and quickly restart it on one of the remaining nodes. This cluster type does not require any special setup from the application side (i.e., the application does not need to be cluster-aware). Hence, it is one of the major ways to ensure application availability and disaster recovery. In active-active clusters, the application runs on every node of the cluster. With this setup, cluster agents coordinate the information processing between all nodes, balancing the load and coordinating concurrent data access. When an application in such a cluster fails, users normally do not experience downtime (possibly missing uncompleted transactions).

Active-active clusters require that the application be built to utilize the cluster capabilities (for instance, if the transaction is not completed on the node that failed, some other remaining node will try to rerun the transaction). Such clusters are less common than active-passive and provide quick application recovery, load balancing and scalability. This type of cluster puts a greater demand on network latency. Organizations often use a combination of cluster setups; for example, active-active for a particular processing site and active-passive between the sites. This combination protects applications against local software or hardware failure (active-active) and against site failure (active-passive). Clusters with a span of one city are called metro-clusters. In contrast, clusters spanning cities, countries and continents are called geo-clusters.

Although it is possible to develop cluster software in-house, it generally is not economically viable, and there are several solutions available from major software vendors. Often, clustered applications require sharing the data between all cluster nodes. Active-active clusters generally require that the same storage be available to all nodes. Active-passive clusters are less demanding and require that the data be replicated from the active node to others.

4.13.2 Telecommunication Networks Resiliency and Disaster Recovery Methods

The plan should contain the organization's telecommunication networks. Today, telecommunication networks are key to business processes in large and small organizations; therefore, the procedures to ensure continuous telecommunication capabilities should be prioritized.

Telecommunication networks are susceptible to the same natural disasters as data centers, but also are vulnerable to several disastrous events unique to telecommunications. These include central switching office disasters, cable cuts, communication software glitches, security breaches connected to hacking and human errors. It is the responsibility of the organization, not the local exchange carrier, to ensure constant communication capabilities. The local exchange carrier is not responsible for providing backup services. However, many do back up the main components within their systems. Therefore, the organization should make provisions for backing up its telecommunication facilities.

The IPF's BCP should provide adequate telecommunications capabilities to maintain critical business processes. Telecommunications capabilities include telephone voice circuits, WANs (connections to distributed data centers), LANs (work group PC connections) and third-party Electronic Data Interchange (EDI) providers. The critical capacity requirements should be identified for the various thresholds of outage for each telecommunications capability, such as two, eight or 24 hours. Uninterruptible power supplies (UPSs) should be sufficient to provide backup to telecommunications and computer equipment.

 ©ISACA. All Rights Reserved.

Methods for network protection are:

- **Redundancy**—This involves a variety of solutions, including:
  - Providing extra capacity with a plan to use the surplus capacity if the normal primary transmission capability is unavailable. For a LAN, a second cable can be installed through an alternate route if the primary cable is damaged.
  - Providing multiple paths between routers
  - Using dynamic routing protocols, such as Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Providing failover devices to avoid single points of failures in routers, switches, firewalls, etc.
  - Saving configuration files for recovery if network devices, such as those for routers and switches, fail. For example, organizations should use Trivial File Transport Protocol (TFTP) servers. Most network devices support TFTP for saving and retrieving configuration information.
- **Alternative routing**—The method of routing information via an alternate medium, such as copper cable or fiber optics. This method uses different networks, circuits or endpoints if the normal network is unavailable. Most local carriers are deploying counter-rotating fiber-optic rings. These rings have fiber-optic cables transmitting information in two directions and in separate cable sheaths for increased protection. Currently, these rings connect through one central switching office. However, future expansion of the rings may incorporate a second central office into the circuit. Some carriers offer alternate routes to different points of presence or alternative central offices. Other examples include cellular and microwave communication as alternatives to land circuits and couriers as alternatives to electronic transmissions.
- **Diverse routing**—The method of routing traffic through split cable facilities or duplicate cable facilities with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit, and subject to the same interruptions, as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes. However, the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. However, acquiring this type of access is time consuming and costly. Most carriers provide alternate and diverse routing facilities, although most services are transmitted over terrestrial media. These cable facilities are usually located in the ground or a basement. Ground-based facilities are at great risk due to the aging infrastructures of cities. In addition, cable-based facilities usually share a room with mechanical and electrical systems that can impose great risk due to human error and disastrous events.
- **Long-haul network diversity**—Many vendors of recovery facilities have provided diverse long-distance network availability, using terrestrial circuits among the major long-distance carriers. This ensures long-distance access if any single carrier experiences a network failure. Several major carriers now have installed automatic rerouting software and redundant lines that provide instantaneous recovery if a break occurs in their lines. The IS auditor should verify that the recovery facility has these vital telecommunications capabilities.
- **Last-mile circuit protection**—Many recovery facilities provide a redundant combination of local carrier terrestrial circuits, microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing also is used.
- **Voice recovery**—Many services, especially in the financial and retail industries, are dependent on voice communications. Redundant cabling and Voice over Internet Protocol are common approaches to deal with failures.
- **Satellite connectivity**—In some locations, certain telecommunication options are not available. Broadband satellite service and temporary satellite options can provide connectivity indistinguishable from cellular networks that depend on towers.

4.14 Data Backup, Storage and Restoration

Because data is the most critical asset for many organizations, data backup, storage and potential restoration are key considerations. Laws and regulations may impact how an enterprise can handle data and should be considered in developing appropriate methods.

4.14.1 Data Storage Resiliency and Disaster Recovery Methods

Often used as a common recovery method, redundant array of independent disks (RAID) is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance

©ISACA. All Rights Reserved.

improvement or both. RAID is used to improve the performance and reliability of data storage systems. It can create large logical disks from multiple physical disks or create multiple logical disks from a single physical disk.

Many vendors offer storage arrays—hardware that hides all the complexities of forming logical volumes from physical disks, thus completely removing the need for low-level configuration. Typically, these storage arrays provide major RAID levels; however, that does not remove the need for responsible IT staff to understand the implications of the different RAID configurations.

Storage arrays provide data replication features to protect data against site failure, ensure successful application recovery (with or without clusters) and ensure data is saved to the disk on one site and appears on the other. Depending on the available network bandwidth and latency, this data replication may be synchronous (i.e., the local disk write is not confirmed until the data is written to the disk on the other site), asynchronous (data is replicated on a scheduled basis) or adaptive (switching from one mode to another depending upon the network load).

The array-based (hardware) replication is absolutely transparent to the application (i.e., no special provisions are needed from the OS or the application side).

If there is no disk array, the data stored on local server volumes (RAID or not) can still be replicated to a remote site using host-based data replication solutions that act similarly to hardware-based solutions.

4.14.2 Backup and Restoration

Because data is the most critical asset for many organizations, data backup, storage and potential restoration are key considerations for the enterprise. Planning these activities in accordance with the BIA, RPO and RTO is crucial for an effective data backup and restoration strategy as the activities must aim at minimizing data loss in alignment with budgets and business objectives. Laws and regulations may impact how an enterprise can handle data and should be considered in developing appropriate methods.

To ensure that the critical activities of an organization (and supporting applications) are not interrupted in the event of a disaster, secondary storage media are used to store software application files and associated data for backup purposes. Even if an organization uses cloud-based backups, there is still a physical location where the backup servers store the information. Cloud-based backups, also known as cloud backups or online backups, involve storing data and system backups on remote servers or infrastructure provided by a cloud service provider. Instead of traditional backup methods, such as local storage, cloud backups leverage the scalability, accessibility and reliability of cloud computing to safeguard data.

Traditional secondary storage media include mirrored disks (local or remote) and network storage. The removable media are typically recorded in one facility and stored in one or more remote physical facilities (offsite libraries). The number and locations of these remote storage facilities are based on the availability of use and perceived business interruption risk. Maintaining the inventory (catalog) of the remote storage facility can be performed automatically (vaulting solutions) or manually. In the latter case, the offsite librarian is responsible for maintaining a continuous inventory of the libraries' contents, controlling access to library media and rotating media between various libraries as needed. As the amount of information increases, keeping manual inventories of media backups (local or remote) becomes increasingly difficult. This task is being replaced gradually by integrated backup and recovery solutions that handle the backup catalogs—remote and local.

As a common control for backup data, the backup itself should be immutable, or unable to be altered or changed. An immutable backup is a way of protecting data that ensures the data is fixed, unchangeable, encrypted or unable to be modified. Backups can be stored on a public cloud since it provides the ability to make backups immutable. For example, some cloud service providers provide backup storage that can be rendered immutable, preventing anyone, even users with admin access rights, from modifying, deleting or encrypting the data.

Offsite Library Controls

It is very important to implement strict controls over physical and logical data. Unauthorized access, loss or tampering with this information (either onsite or while in transit) could impact the information system's ability to support critical business processes, putting the very future of an organization at risk.

Controls over the offsite storage library include:

- Secure physical access to library contents, ensuring only authorized personnel have access.
- Encrypt backup media, especially in transit.
- Ensure that physical construction can withstand fire, heat, water, etc.

 ©ISACA. All Rights Reserved.

- Locate the library away from the data center, preferably in a facility not subject to the same disaster event to avoid the risk of a disaster affecting both facilities.
- Ensure an inventory of all storage media and files stored in the library is maintained for the specified retention time.
- Ensure a record of all storage media and files moved into and out of the library is maintained for the specified retention/expiration time.
- Ensure that a catalog of information regarding the versions and location of data files is maintained for the specified retention time and protected against unauthorized disclosure.

The retention times for different records must follow the enterprise retention policy.

Cloud Backup

A cloud backup refers to the practice of securely storing the offsite storage library in a remote data center operated by a third-party cloud service provider. This kind of storage is becoming increasingly popular because it allows the backup destination to be in a disconnected infrastructure that facilitates data protection from threats such as ransomware, which is increasingly targeting backup infrastructure.

Controls over cloud backups typically include:
- Encrypt the data-in-transit as it traverses the Internet to reach the remote data center.
- Ensure that encrypted data is stored in the cloud library and that access to the encryption keys is granted on a need-to-know basis.
- Verify that backup and restore times are appropriate to ensure the RTOs and RPOs. While a typical restore test generally is performed only on samples, the IS auditor must ensure that a real restore would require network transfers for a larger part—potentially the entirety—of the infrastructure in scope.

Security and Control of Offsite Facilities

The offsite IPF must be as secure and controlled as the originating site. This includes having adequate physical access controls, such as locked doors, no windows and active surveillance. The offsite facility should not be easily identifiable from the outside. This is to prevent intentional sabotage of the offsite facility should the destruction of the originating site be from a malicious attack. The offsite facility should not be subject to the same disaster event that affected the originating site.

The offsite facility should possess the same constant environmental monitoring and control as the originating site or as dictated by business requirements. This includes monitoring the humidity, temperature and surrounding air to achieve the optimum conditions for storing optical and magnetic media and, if applicable, servers, workstations, storage arrays and media libraries. The proper environmental controls include a UPS operating on a raised floor with proper smoke and water detectors installed, climate controls, monitoring for temperature and humidity, and a working/tested fire extinguishing system. Provisions for storage should ensure that paper records do not create a fire hazard. Additional controls should be implemented in case of specific legal, regulatory or business requirements.

Media and Documentation Backup

A crucial element of a DRP (onsite or offsite) is the availability of adequate data. Duplication of important data and documentation, including offsite storage of backup data and paper records, is a prerequisite for any recovery.

If information is processed and stored in a confidential environment at the primary site, and if backup is to be stored in a similarly secure location, care should be exercised to ensure that the means of transporting data, whether in the form of physical backup media or via mirrored backups on the network, extend adequate protection to the information.

Types of Backup Devices and Media

Backup devices and media must be chosen based on a variety of factors:
- **Standardization**—Very specific technologies require more support for the primary and offsite facility, increasing costs.
- **Capacity**—Backup media should have adequate capacity to reduce the number of media necessary to implement a backup set.
- **Speed**—Processes to back up and restore should be completed in an acceptable time to comply with business requirements.
- **Price**—Backup devices are only part of the costs; attention must be paid to media prices.

There are a lot of different devices and media types available. The technology chosen must be adequate for business needs. **Figure 4.30** provides some examples.

©ISACA. All Rights Reserved.

Figure 4.30—Types of Media

Portability	Small Amounts, Few Changes	Large Amounts, Frequent Changes
Removable media	CDs, DVDs, removable hard drives or solid-state drives	Tape-based backup systems (digital data storage [DDS], digital audio tape [DAT], digital linear tape [DLT], advanced intelligent tape [AIT], linear tape-open [LTO])
Nonremovable media		Disk-based backup e.g., virtual tape libraries (VTLs), disk snapshots, host-based or disk-array-based replication

There are different types of disk-based backup systems:

- Virtual tape library (VTL) systems consist of disk storage (typically mid-range disk arrays) and software that control backup and recovery data sets. For an external user (backup and recovery software), VTLs behave like a conventional tape library; however, data is stored on a disk array. For disaster recovery purposes, a VTL's contents are often replicated from a primary site to a backup site using the hardware-based replication provided by a disk array.
- Host-based replication is executed at the host (server) level by special software running on the host server and on the target server. It can occur in real time (synchronous mode, when the data is not written to the primary site until the backup site sends confirmation the replicated data has arrived and been safely written to the disk) or with some delay (asynchronous mode, when data is transferred to the backup site with some delay). The software packages are available from major software vendors.
- Disk-array-based replication is the same as host-based replication; however, the replication is performed at the disk array level, completely hidden from servers and applications. This feature is available from all major hardware vendors supplying mid-range and high-end disk arrays. The replication can be completed via SAN or LAN.
- Snapshot technology is flexible, allowing different momentary copies of volumes or file systems. Depending upon the types of snapshots, either a full copy is created each time or only the changed blocks of data or files are replicated. This technology is especially efficient and effective with backup and recovery software. For instance, when a snapshot is taken and mounted on a different server, a full backup is performed, thus saving the production system from the overhead load. Another example is replicating data to a remote site, making snapshots on the remote site, and using them for backup and recovery, thus using the server equipment at the backup site.

In an environment in which server virtualization is used, disk-based backup systems can provide an excellent disaster recovery solution because entire virtual servers may be replicated to the recovery site.

Copies of data taken for offsite backup must be given the same level of security as the original files. Therefore, the offsite facility and transportation arrangements must meet the security requirements for the most sensitive class of data on the backup media.

Periodic Backup Procedures

Both data and software files should be backed up periodically following the defined RPO. The backup schedule period may differ per application program or software system. For instance, the locations (folders or volumes) where the application data is stored must be backed up regularly since daily transactions frequently change the data. The locations where application configuration and software files (application or OS) are stored are updated less frequently—only when configurations change or a patch is applied. Often, online/real-time systems that perform large-volume transaction processing require nightly or hourly backups or use data replication at a separate remote processing facility.

Scheduling periodic backups often can be accomplished via an automated backup/media management system and automated job scheduling software. Using the integrated solution for backup/recovery procedures and media management will prevent erroneous or missed backup cycles due to operator error. Schedules describing the backup of certain data are included in the backup procedures.

Modern backup and recovery solutions include special software, called agents, installed on the protected servers and workstations. These agents collect the data (data files, configuration files, software application files) and

 ©ISACA. All Rights Reserved.

ship it to the backup and recovery servers that convert data for subsequent storage on a disk. The same agents are used for data restoration.

Frequency of Rotation

Data and software backup must allow for the continuing occurrence of change. A copy of the file or record, as of some point in time, must be retained for backup purposes. All changes or transactions that occur during the interval between the copy and the current time also are retained.

Considerations for establishing file backup schedules include:

- The frequency of the backup cycle and depth-of-retention generations must be determined for each application.
- The backup procedures must anticipate failure at any step of the processing cycle.
- For legacy systems, master files should be retained at appropriate intervals, such as at the end of an updating procedure, to synchronize files and systems.
- Transaction files should be presented to coincide with master files so a prior generation of a master file can be brought completely up to date to recreate a current master file.
- DBMS requires specialized backup, usually provided as an integral feature of the DBMS or the special part of the backup and recovery software (agent) designed especially for the particular make and version of the database.
- It may be necessary to secure a license to use certain vendor software at an alternate site; this should be arranged before the need arises.
- Backup for custom-built software must include object-code and source-code libraries and provisions for maintaining program patches on a current basis at all backup locations.
- Backup hardware should be available at the offsite facility and compatible with backup media. Also, for long-term retention it is necessary to have technical support and maintenance agreements to guarantee that the alternate backup hardware will work properly in case of restoration.

Likewise, any documentation required for the consistent and continual operation of the business should be preserved in an offsite backup facility. This includes source documents required for the restoration of the production database. As with data files, the offsite copies should be updated to ensure their usefulness. It is important to remember that adequate backup is a prerequisite to successful recovery.

Types of Media and Documentation Rotated

Without software, computer hardware is of little value. Software, including OSs, programming languages, compilers, utilities, application programs and copies of paper documentation—such as operational guides, user manuals, records, data files, databases, etc.—should be maintained and stored offsite in their current status. This information provides the raw materials and finished products for the IS processing cycle and should be stored offsite.

Figure 4.31 describes the documentation to be backed up and stored offsite.

Figure 4.31—Offsite Storage

Classification	Description
Operating procedures	Application run books, job stream control instructions, operating system (OS manuals and special procedures
System and program documentation	Flow charts, program source code listings, program logic descriptions, statements, error conditions and user manuals
Special procedures	Any procedures or instructions that are out of the ordinary, such as exception processing, variations in processing and emergency processing
Input source documents, output documents	Duplicate copies, photocopies, microfiche, microfilm reports or summaries required for auditing, conducting historical analysis, performing vital work, satisfying legal requirements or expediting insurance claims
Business continuity plan (BCP)	A copy of the correct plan for reference

Sensitive data stored offsite should be stored in a fire-resistant magnetic media container. When the data is shipped back to the recovery site, the data should be stored and sealed in the magnetic media container.

Every organization should have a policy governing what is stored and for how long. Backup schedules and rotation media to be used in an offsite location are important. This rotation of media can be performed via management software.

©ISACA. All Rights Reserved.

4.14.3 Backup Schemes

There are three main schemes for backup: full, incremental and differential. Each one has its advantages and disadvantages. Usually, the methods are combined to complement each other.

Full Backup

This backup scheme copies all files and folders to the backup media, creating one backup set (with one or more media, depending on media capacity). The main advantage is having a unique repository in case of restoration, but it requires more time and media capacity than other methods.

Incremental Backup

An incremental backup copies the files and folders that have changed or are new since the last incremental or full backup. If there is a full backup on day 1, the incremental backup on day 2 will copy only the changes from day 1 to day 2. On day 3, it will copy only the changes from day 2 to day 3, and so on. Incremental backup is a faster method of backup. It requires less media capacity, but all backup sets must restore all changes since a full backup and restoration will take more time.

Figure 4.32 provides an example of a full-plus-incremental backup scheme. On day 1, there was a full backup and all files were saved to backup media. On days 2 through 7, there were incremental backups. On day 2, file 1 changed. On day 3, file 2 changed. On day 4, file 3 changed. On day 5, file 4 changed. The X shows which files were backed up on which days.

Figure 4.32—Full Plus Incremental Backup Scheme

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
File 1	X	X					
File 2	X		X				
File 3	X			X			
File 4	X				X		

Differential Backup

A differential backup copies all files and folders that have been added or changed since a full backup was performed. This type of backup is faster, requires less media capacity than a full backup and requires only the last full and differential backup sets to make a full restoration. It requires less time to restore than incremental backups but is slower and requires more media capacity than incremental backups because backed-up data is cumulative.

Figure 4.33 depicts a full-plus-differential backup scheme. On day 1, there is a full backup. On days 2 through 7, there are differential backups. On day 2, file 1 changed. On day 3, file 2 changed. On day 4, file 3 changed. On day 5, file 4 changed. The X shows which files were backed up.

Figure 4.33—Full Plus Differential Backup Scheme

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
File 1	X	X	X	X	X		
File 2	X		X	X	X		
File 3	X			X	X		
File 4	X				X		

Note that in differential backups all files or folders that were changed since a full backup are repeatedly copied to the backup media.

Method of Rotation

Although there are various approaches to the rotation of media, one of the more accepted techniques is the grandfather-father-son method. Daily backups (son) are made over the course of a week in this method. The last backup taken during the week becomes the backup for that week (father). The earlier daily backup media are then rotated for reuse as backup media for the second week. At the end of the month, the last weekly backup is retained as the backup for that month (grandfather). Earlier weekly backup media are then rotated for reuse in subsequent months. At the end of the year, the last monthly backup becomes the yearly backup. Monthly and annual storage media are normally retained and not subject to the rotation cycle. See **figures 4.34** and **4.35** for examples of typical rotation cycles. Testing all aspects of the DRP is the most important factor in achieving success in an emergency. The main objective of testing is to ensure that executing the plans will result in the successful recovery of the infrastructure and critical business processes.

 ©ISACA. All Rights Reserved.

Testing should focus on:

- Identifying gaps
- Verifying assumptions
- Testing timelines
- Implementing effective strategies
- Reviewing personnel performance
- Planning accurately and currently

Testing promotes collaboration and coordination among teams and is a useful training tool. Many organizations require complete testing annually. In addition, testing should be considered on the completion or major revision of each draft plan or complementary plan and should follow changes in key personnel and technologies or in the business/regulatory environment.

Testing must be carefully planned and controlled to avoid placing the business at increased risk. To ensure that all plans are regularly tested, the IS auditor should be aware of the testing schedule and tests to be conducted for all critical functions.

All tests must be fully documented with pretest, test and posttest reports. Test documentation should be reviewed by the IS auditor. Information security should also be validated during the test to ensure it is not compromised. A key element to this approach is that backups rotated offsite should not be returned for reuse until their replacements have been sent offsite. For example, the backup media for week 1 should not be returned from offsite storage until the month-end backup is safely stored offsite. Variations of this method can be used depending on whether quarterly backups are required and on the amount of redundancy an organization may wish to have.

Figure 4.34—Typical Rotation Cycle, Sample A

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
Week 1	Media 1	Media 2	Media 3	Media 4	Media 5	Media 6	Media 7 (week Media)
Week 2	Media 1	Media 2	Media 3	Media 4	Media 5	Media 6	Media 8 (week Media)
Week 3	Media 1	Media 2	Media 3	Media 4	Media 5	Media 6	Media 9 (week Media)
Week 4	Media 1	Media 2	Media 3	Media 4	Media 5	Media 6	Media 10 (week Media)
Week 5	Media 1	Media 2	Media 3	Media 4	Media 5	Media 6	Media 7 (week Media)

Figure 4.35—Typical Rotation Cycle Sample B



Record Keeping for Offsite Storage

An inventory of contents at the offsite storage location should be maintained. This inventory should contain information such as:

- Data set name, volume serial number, date created, accounting period and offsite storage bin number for all backup media
- Document name, location, pertinent system and date of last update for all critical documentation

Automated media management systems usually have options that help record and maintain this information. If backup media are carried between facilities, then both receipt and shipment logs should be maintained to assist in tracking in case of losses.

©ISACA. All Rights Reserved.

3-2-1 Backup Strategy

The 3-2-1 backup strategy saves multiple copies of data on different storage devices and at different locations. A 3-2-1 backup strategy reduces the impact of a single point of failure, such as a media error or stolen device. The 3-2-1 backup strategy involves:

- Creating one primary backup and two copies of the data
- Saving backups to two different types of media
- Keeping at least one backup file offsite

Keep in mind that this option may not be available from cloud service providers.

4.15 Business Continuity Plan

The purpose of business continuity/disaster recovery planning is to enable a business to continue operations should any kind of disturbance arise. Rigorous planning and commitment of resources are necessary to adequately plan for such an event.

The first step in preparing a new BCP, or in updating an existing one, is to identify the business processes of strategic importance—the key processes responsible for both the permanent growth of the business and the fulfillment of the business goals. Ideally, the BCP/DRP should be supported by a formal executive policy that states the organization's overall recovery target and empowers those involved in developing, testing and maintaining the plans.

The risk management process should begin with a risk assessment based on the key processes. The risk is directly proportional to the impact on the organization and the probability of occurrence of the perceived threat. Thus, the result of the risk assessment should be the identification of:

- Human resources, data, infrastructure elements and other resources (including those provided by third parties) that support the key processes
- Potential vulnerabilities—the dangers or threats to the organization
- Estimated probabilities of the occurrence of threats
- Efficiency and effectiveness of existing risk mitigation controls (risk countermeasures)

BCP is primarily the responsibility of senior managers, as they are entrusted with safeguarding the assets and the organization's viability, as defined in the BCP/DRP policy. The BCP is generally followed by the business and supporting units to provide a reduced but sufficient level of functionality in the business operations immediately after encountering an interruption, while recovery occurs. The plan should address all functions and assets required to continue as a viable enterprise. This includes continuity procedures necessary to survive and minimize the consequences of business interruption.

BCP takes into consideration:

- Critical operations that are necessary for the survival of the organization
- Human/material resources supporting them

In addition to the plan for the continuity of operations, the BCP includes:

- The DRP used to recover a facility rendered inoperable, including relocating operations
- The restoration plan used to return operations to normality, whether in a restored or new facility

Depending on the organization's complexity, there could be one or more plans to address the various aspects of business continuity and disaster recovery. Those plans do not necessarily have to be integrated into one single plan. However, each must be consistent with other plans for a viable BCP strategy.

It is highly desirable to have a single integrated plan to ensure that:

- There is proper coordination among various plan components.
- Resources committed are used most effectively, and there is reasonable confidence that with the plan's application the organization will survive a disruption.

Even if similar processes of the same organization are handled at a different geographic location, the BCP and DRP solutions may differ for different scenarios. Solutions may differ due to contractual requirements. For example, if the same organization is processing an online transaction for one client and the back office is processing one for another client, a BCP solution for the online service will significantly differ from the one for the back-office processing.

4.15.1 IT Business Continuity Planning

IT business continuity planning uses the same approach as enterprise business continuity planning, except that the continuity of IT processing is threatened. IT processing is critical because most key business processes depend on the availability of key systems, infrastructure components and data.

The IT BCP should be aligned with the strategy of the organization. The criticality of the various application systems deployed in the organization depends on the nature of the business and the value of each application to the business.

 ©ISACA. All Rights Reserved.

The value of each application to the business is directly proportional to the information system's role in supporting the organization's strategy. The components of the information system (including the technology infrastructure components) are then matched to the application's (e.g., the value of a computer or a network is determined by the importance of the application system that uses it). Therefore, the information system BCP/DRP is a major component of an organization's overall business continuity and disaster recovery strategy. If the IT plan is separate, it must be consistent with and support the corporate BCP. Throughout the IT business continuity (sometimes referred to as IT service continuity) planning process, the organization's overall BCP should be considered, and it should be supported by the executive policy. All IT plans must be consistent with and support the corporate BCP. This means that alternate processing facilities that support key operations must be ready, be compatible with the original processing facility and have up-to-date plans regarding their use.

All possible steps must be taken to reduce or remove the likelihood of a disruption using the methods described in other sections of this manual. Examples include:

- Minimize threats to the data center by considering location:
  - Not on a flood plain
  - Not on or near an earthquake fault line
  - Not close to an area where explosive devices or toxic materials are regularly used
- Use resilient network topographies, such as Loop or Mesh, with alternative processing facilities already built into the network infrastructure.

Developing and testing an information system BCP/DRP is a major component of an organization's overall business continuity and disaster recovery strategy. The plan is based on the coordinated use of whatever risk countermeasures are available for the organization (e.g., duplicate processing facility, redundant data networks, resilient hardware, backup and recovery systems, data replication, etc.). If the IT plan is a separate plan (or multiple separate plans), it must be consistent with and support the corporate BCP.

Establishing dependencies among critical business processes and applications, the information system and IT infrastructure components is a subject of risk assessment. The resulting dependencies map, with threats to and vulnerabilities of the components/dependencies (along with the key applications grouped by their criticality), is the outcome of the risk assessment.

After the risk assessment identifies the importance of the IS components to the organization and the threats to and vulnerabilities of those components, a remedial action plan can be developed to establish the most appropriate methods to protect them. There is always a choice of risk mitigation measures (risk countermeasures) to remove the threat and/or fix the vulnerability.

The risk can be either estimated qualitatively (assigning qualitative values to the impact of the threat and its probability) or calculated quantitatively (assigning a monetary value to the impact [i.e., loss] and assigning a probability).

Note

The CISA candidate will not be tested on the actual calculation of risk analysis; however, the IS auditor should be familiar with risk analysis calculation.

Suppose the organization is willing to investigate the extent of the business's losses from the disruption. In that case, the organization may conduct a BIA, discussed in section 4.12 Business Impact Analysis. The BIA allows the organization to determine the maximum downtime possible for a particular application and how much data could be lost. The BIA also allows the organization to quantify the losses as they grow after the disruption, thus allowing it to decide on the technology (and facilities) used to protect and recover its key information assets (information system, IT components, data, etc.).

Risk assessment and BIA results are fed into the IS business continuity strategy, which outlines the main technology and principles behind IT protection and recovery as well as the road map to implement the technology and principles.

As the IT business continuity strategy and its overarching IT strategy are executed, the IT infrastructure of the organization changes. New risk countermeasures are introduced, and old ones become obsolete. The information system BCP must be changed accordingly and retested periodically to ensure the changes are satisfactory.

Like any BCP, an information system BCP is much more than a plan for information systems. A BCP identifies what the business will do during a disaster. For example, where will employees report to work? How will orders be taken while the computer system is restored? Which vendors should be called to provide needed supplies? A subcomponent of the BCP is the IT DRP. This typically details the process IT personnel will use to restore the computer systems, communications, applications and

©ISACA. All Rights Reserved.

data. The DRP may be included in the BCP or provided as a separate document altogether, depending on the needs of the business.

Not all systems will require a recovery strategy. When determining recovery options, an overriding factor is that the cost should never exceed the benefit (this usually becomes clear after completing a BIA). One of the important outcomes of a BIA, apart from the RTO and RPO, is a way to group information systems according to their recovery time. This usually guides the selection of the technological solutions (i.e., controls) supporting business continuity and IT disaster recovery.

IT disaster recovery usually takes place in unusual, stressful circumstances (e.g., fire, flood, hurricane devastation). Security controls (both physical and IS) may not function. It is, therefore, recommended that the organization implement an information security management system (ISMS) to maintain the integrity, confidentiality and availability of IS both in normal and abnormal conditions.

It is important to note that disruptions of services provided by third parties, such cloud services, may not be recoverable by the contracting organization. In some cases, the organization must wait for the vendor to recover access to the service and implement its own BCP before service is restored.

4.15.2 Disasters and Other Disruptive Events

Disasters cause critical information resources to be inoperative for some time, adversely impacting organizational operations. The disruption could last a few minutes to several months, depending on the extent of damage to the information resource. Most important, disasters require recovery efforts to restore operational status.

A disaster may be caused by natural calamities—such as earthquakes, floods, tornados, severe thunderstorms and fire—which cause extensive damage to the processing facility and the locality in general. Other disastrous events causing disruptions may occur when expected services—such as electrical power, telecommunications, natural gas supply or other delivery services—are no longer supplied to the company due to a natural disaster or other cause.

Not all critical disruptions in service or disasters are due to natural causes. A disaster could also be caused by events precipitated by human beings, such as terrorist attacks, hacker attacks or human error. Service disruption is sometimes caused by system malfunctions, accidental file deletions, untested application releases, loss of backup, network denial-of-service (DoS) attacks, intrusions and viruses. These events may require taking action to recover operational status to resume service. Such actions may necessitate restoring hardware, software or data files.

Many disruptions start as minor incidents. Normally, the help desk acts as an early warning system to recognize the first signs of an upcoming disruption. Such disruptions (e.g., gradually deteriorating database performance) often go undetected. Until these creeping disasters strike (e.g., the database halts), they cause only infrequent user complaints.

Based on risk assessment, worst-case scenarios and short- and long-term fallback strategies are formulated in the IS business continuity strategy and included in the BCP. In the short term, an alternate processing facility may be needed to satisfy immediate operational needs (as in the case of a major natural disaster). In the long term, a new permanent facility must be identified for disaster recovery and equipped to continue IS processing services regularly.

Pandemic Planning

Pandemics can be defined as epidemics or outbreaks of infectious diseases in humans that can spread rapidly over large areas, possibly worldwide, such as flu outbreaks. There are distinct differences between pandemic planning and traditional business continuity planning, and, therefore, the IS auditor should evaluate an organization's preparedness for pandemics or other outbreaks. Pandemic planning presents unique challenges; unlike natural disasters, technological disasters, malicious acts or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration.

Dealing With Damage to Image, Reputation or Brand

Damaging rumors may arise from many sources and may or may not be associated with a serious incident or crisis. Whether they are spontaneous or a side effect of a business continuity or disaster recovery problem, their consequences may be devastating. One of the worst consequences of crises is the loss of trust. Effective public relations (PR) activities in an organization may play an important role in helping to contain the damage to the enterprise's image and ensure that a crisis is not made worse. Certain industries (e.g., banks, healthcare

organizations, airlines, petroleum refineries, chemical facilities, transportation systems, nuclear power plants or other organizations with relevant social impact) should have elaborate protocols for dealing with accidents and catastrophes.

A few basic good practices should be considered and applied by an organization experiencing a major incident. Irrespective of the resultant objective consequences of an incident (delay or interruption in service, economic losses, etc.), a negative public opinion or negative rumors can be costly. Reacting appropriately in public (or to the media) during a crisis is not simple. A properly trained spokesperson should be appointed and prepared beforehand. Normally, a senior legal counsel or a PR officer is the best choice. No one, except for the spokesperson, should make any public statement, regardless of the person's rank in the organizational hierarchy.

As part of the preparation, the spokesperson should draft and keep on file a generic announcement with blanks to be filled in with the specific circumstances. This should not be deviated from because of improvisation or time pressure. The announcement should not state the causes of the incident but should indicate that an investigation has been started and results will be reported. Liability should not be assumed. The system or the process should not be blamed.

Unanticipated/Unforeseeable Events

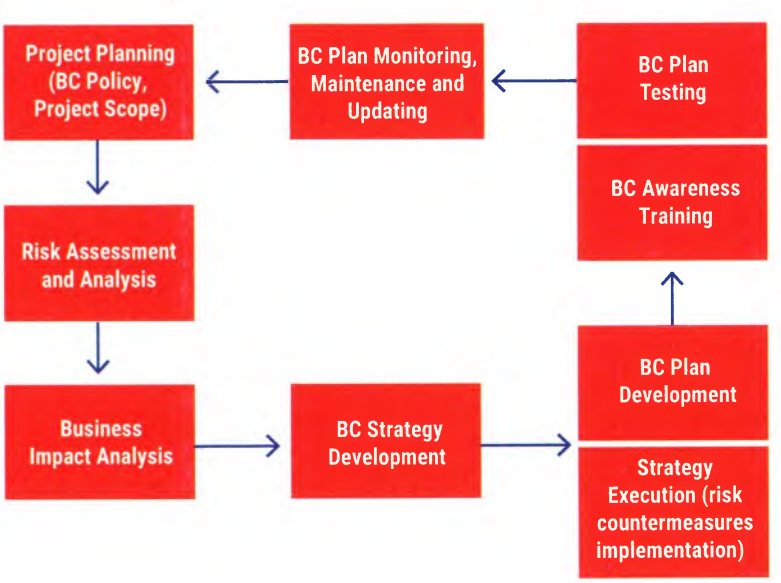
Management should consider the possible impacts of unforeseeable (black swan) events on the organization's business. Black swan events are a surprise (to the observer), have a major effect and are often inappropriately rationalized with the benefit of hindsight. Black swan events cannot be expected or planned for. Although these events are very rare, they can have such a crippling impact on the organization that—based on the criticality of the process, industry or activity—management should start thinking about contingency planning to meet such events.

Forbidding senior executives with shared responsibilities from traveling together is another example of proactive management, ensuring that the organization would not be left without a senior manager if a common disaster should occur.

4.15.3 Business Continuity Planning Process

The business continuity planning process can be divided into the life cycle phases in **figure 4.36**.

Figure 4.36—Business Continuity Planning Life Cycle



©ISACA. All Rights Reserved.

4.15.4 Business Continuity Policy

A business continuity policy is a document approved by top management that defines the extent and scope of the organization's business continuity effort (a project or an ongoing program). The business continuity policy can be broken into public and internal sections. The business continuity policy serves several purposes, including:

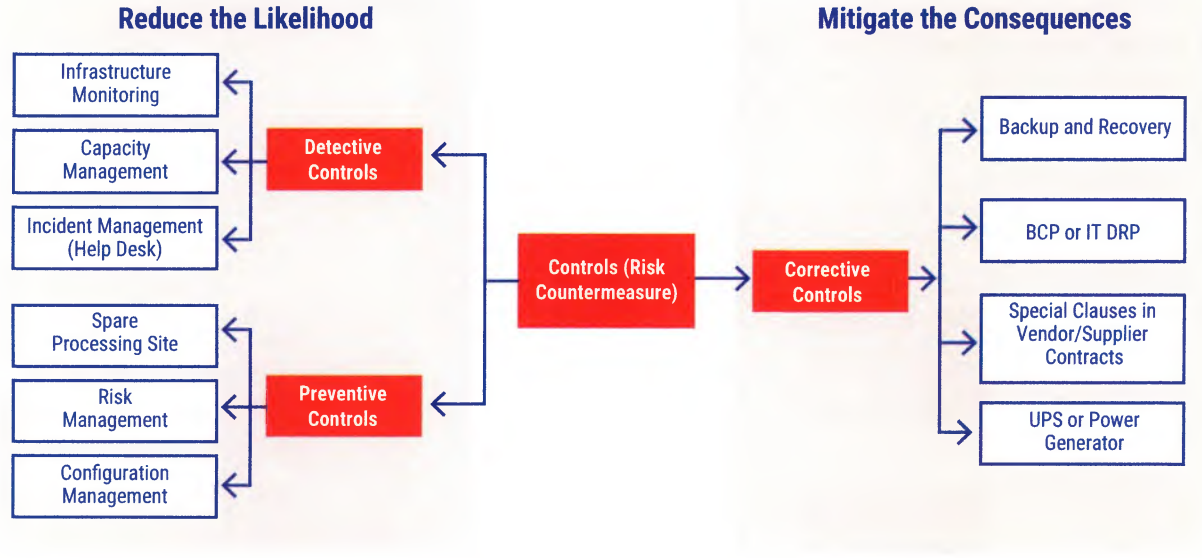
- Providing a message to internal stakeholders (i.e., employees, management, board of directors) in its internal portion that the company is undertaking the business continuity effort, committing its resources and expecting all areas of the enterprise to do the same
- Communicating to external stakeholders (i.e., shareholders, regulators, authorities, etc.) that the organization is seriously treating its obligations (e.g., service delivery, compliance)
- Empowering those responsible for business continuity
- Stating the general principles on which business continuity will be based, such as a risk assessment, BIA and system redundancy targets

A business continuity policy should be proactive. It should state that the organization will use all possible controls to detect and prevent disruptions, and if disruption occurs, the organization has the controls necessary to mitigate any consequences. The policy is later reflected in the IT business continuity strategy and during its execution.

The BCP (or IT DRP) is an organization's most critical corrective control. It depends on other effective controls, particularly incident management and backup and recovery solutions.

Figure 4.37 describes how controls function regarding incidents and mitigation of their impacts.

Figure 4.37—Incident and Impact Relationship Diagram



To be effective, the incident management group needs adequate staffing, support and training in crisis management, and the BCP should be well designed, documented, drill tested, funded and audited.

4.15.5 Business Continuity Planning Incident Management

Incidents are dynamic by nature. They evolve, change with time and circumstances and are often rapid and unforeseeable. Because of this, incident management should also be dynamic, proactive and well-documented. An incident is any unexpected event, even if it causes no significant damage. (See section 5.14 Security Incident Response Management for more information.)

 ©ISACA. All Rights Reserved.

All incidents should be categorized depending on an estimate of the damage they could cause to the organization. Classification can change while the incident is resolved. A classification system can include the following categories: negligible, minor, major and crisis:

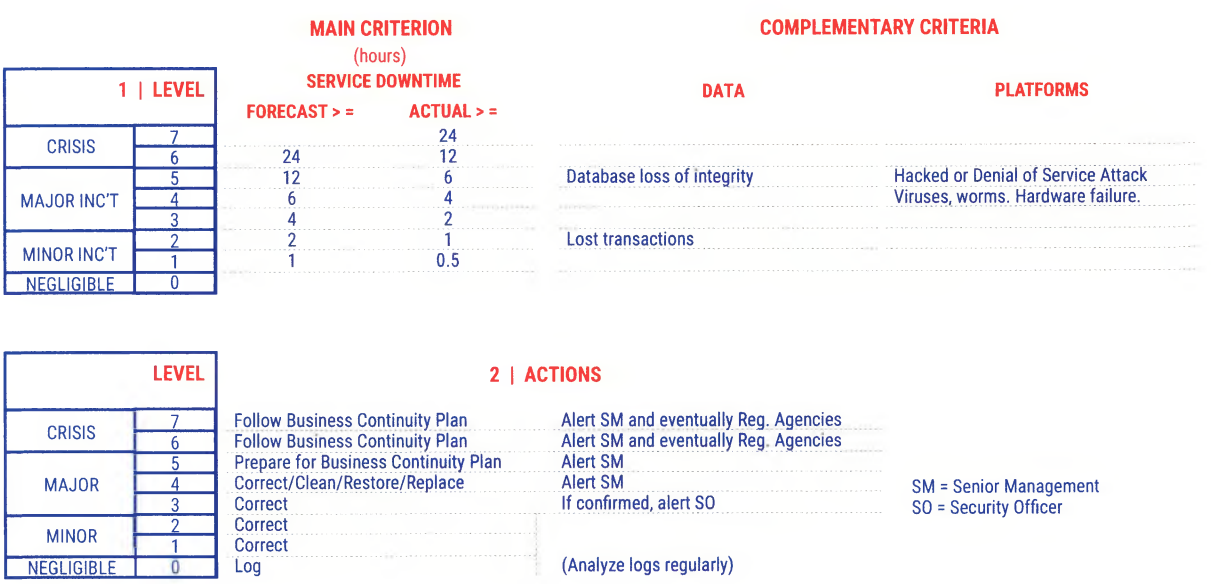
- Negligible incidents cause no perceptible or significant damage. For example, brief OS crashes with full information recovery or momentary power outages with UPS backup are negligible incidents.
- Minor incidents produce no harmful material or financial impact of relative importance. A minor incident could be an Internet outage within a specific office in a large corporation. The impacted users would lose access to the Internet, network resources and cloud-based applications, but the incident would be considered minor because it was localized to a single office.
- Major incidents cause a negative material impact on business processes and may affect other systems, departments or even outside clients. A ransomware attack could be classified as a major incident. The attack could pervasively compromise servers, workstations and devices rendering them inoperable and leading to disruption, financial losses and impacted customers.
- A crisis is a major incident that can have serious material impact on the continued functioning of an organization's IT infrastructure, systems and services, substantially disrupting business operations. It may also adversely impact other systems or third parties. The severity of the impact depends on the industry and circumstances and is generally directly proportional to the time elapsed from the inception of the incident to the time of its resolution.

Minor, major and crisis incidents should be documented, classified and revisited until corrected or resolved. This is a dynamic process because a major incident may decrease in extent momentarily and later expand to become a crisis incident.

Negligible incidents can be analyzed statistically to identify any systemic or avoidable causes.

Figure 4.38 shows an example of an incident classification system and reaction protocol.

Figure 4.38—Incident/Crisis Levels



1 | LEVEL		MAIN CRITERION (hours) SERVICE DOWNTIME FORECAST > =	ACTUAL > =	COMPLEMENTARY CRITERIA DATA	PLATFORMS
CRISIS	7		24		
	6	24	12		
MAJOR INC'T	5	12	6	Database loss of integrity	Hacked or Denial of Service Attack
	4	6	4		Viruses, worms. Hardware failure.
	3	4	2		
MINOR INC'T	2	2	1	Lost transactions	
	1	1	0.5		
NEGLIGIBLE	0				

LEVEL		2 | ACTIONS		
CRISIS	7	Follow Business Continuity Plan	Alert SM and eventually Reg. Agencies	
	6	Follow Business Continuity Plan	Alert SM and eventually Reg. Agencies	
MAJOR	5	Prepare for Business Continuity Plan	Alert SM	
	4	Correct/Clean/Restore/Replace	Alert SM	SM = Senior Management
	3	Correct	If confirmed, alert SO	SO = Security Officer
MINOR	2	Correct		
	1	Correct		
NEGLIGIBLE	0	Log	(Analyze logs regularly)	

Source: Personas Y Tecnicas Multimedia SL © 2007. All rights reserved. Used by permission.

Service can include commitments to both external customers and internal departments. SLAs often regulate service delivery, which may state the maximum downtime and recovery estimates. With some exceptions, severity is driven to a large extent by the estimated downtime.

Other criteria may include the impact on data or platforms and the degree to which the organization's functioning is adversely impacted. A conservative fail-safe approach would assign any nonnegligible incident a starting, provisional severity level 3 (seen in **figure 4.38**). As the incident evolves, this level should be reevaluated regularly by the person or team in charge, often referred to as an incident response or firecall team.

The security officer or other designated individual should be notified of all relevant incidents as soon as any triggering event occurs. The designated individual should then follow a pre-established escalation protocol (e.g., calling in a spokesperson, alerting top management and involving regulatory agencies) that might be established in a recovery plan, such as the IT DRP.

4.15.6 Development of Business Continuity Plans

Based on the inputs from the BIA, criticality analysis and recovery strategy selected by management, a detailed BCP and DRP should be developed or reviewed. The review should address all the issues in the business continuity scope involved in interrupting business processes, including recovering from a disaster. The various factors that should be considered while developing/reviewing the plan are:

- Predisaster readiness covering incident response management to address all relevant incidents affecting business processes
- Evacuation procedures
- Procedures for declaring a disaster (rating and escalation procedures)
- Circumstances under which a disaster should be declared. Not all interruptions are disasters, but a small incident, if not addressed promptly or properly, may lead to a disaster. For example, a virus attack not recognized and contained in time may bring down the entire IT facility.
- Clear identification of responsibilities in the plan
- Clear identification of persons responsible for each function in the plan
- Clear identification of contract information
- Step-by-step explanations of recovery processes
- Clear identification of the various resources required for recovery and continued operation of the organization

The plan should be documented and written in simple language that is understandable to all.

It is common to identify teams of personnel who become responsible for specific tasks in case of disasters. The plan must be structured so different teams can easily address their areas of responsibility. Copies of the plan should be maintained offsite.

4.15.7 Other Issues in Plan Development

The personnel responsible for the most critical resources must react to the interruption/disaster. Therefore, management and user involvement are vital to the success of the BCP execution. User management involvement is essential to identifying critical systems, their associated critical recovery times and the specification of needed resources. The three major personnel divisions that require involvement in the formulation of the BCP are support services (those who detect the first signs of incident/disaster), business operations (those who may suffer from the incident) and information processing support (those who are going to run the recovery).

Because the underlying purpose of BCP is the recovery and resumption of business operations, it is essential to consider the entire organization, not just IS processing services, when developing the plan. If a uniform BCP does not exist for the entire organization, the plan for IS processing should be extended to include planning for all divisions and units that depend on IS processing functions.

When formulating a plan, the following items should be included:

- A list of the staff required to maintain critical business functions in the short, medium and long term, with redundant contact information (backups for each contact)
- The configuration of building facilities, desks, chairs, telephones, etc., required to maintain critical business functions in the short, medium and long term
- The resources required to resume/continue operations (not necessarily IT or even technology resources)

4.15.8 Components of a Business Continuity Plan

Depending on an organization's size and/or requirements, a BCP may consist of more than one plan document. A BCP should include:

- Continuity of operations plan
- DRP
- Business resumption plan

A BCP may also include:

- Continuity of support plan/IT contingency plan
- Crisis communications plan

 ©ISACA. All Rights Reserved.

- Incident response plan
- Transportation plan
- Occupant emergency plan
- Evacuation and emergency relocation plan

One example of the components of a BCP is shown in **figure 4.39**.

Figure 4.39—Components of a Business Continuity Plan

Plan	Purpose	Scope	Plan Relationship
Business continuity plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Addresses mission/business processes at a lower or expanded level from COOP Mission Essential Functions (MEFs)	Mission/business process-focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs
Continuity of operations plan (COOP)	Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives	Addresses MEFs at a facility; information systems (IS) are addressed based only on their support of the mission-essential functions	MEF-focused plan that may also activate several business unit-level BCPs, ISCPs or DRPs, as appropriate
Crisis communications plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors	Addresses communications with personnel and the public; not information system-focused	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event
Critical infrastructure protection (CIP) plan	Provides policies and procedures for the protection of national critical infrastructure components as defined in the National Infrastructure Protection Plan	Addresses critical infrastructure components that are supported or operated by an agency or organization	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets
Cyber incident response plan	Provides procedures for mitigating and correcting a cyberattack, such as a virus, worm or Trojan horse	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information	Information system-focused plan that may activate an ISCP or DRP depending on the extent of the attack
Disaster recovery plan (DRP)	Provides procedures for relocating IS operations to an alternate location	Activated after major system disruptions with long-term effects	Information system-focused plan that activates one or more ISCPs for recovery of individual systems
Information system contingency plan (ISCP)	Provides procedures and capabilities for recovering an information system	Addresses single information system recovery at the current or, if appropriate, alternate location	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP and/or BCP

©ISACA. All Rights Reserved.

Figure 4.39—Components of a Business Continuity Plan (cont.)

Plan	Purpose	Scope	Plan Relationship
Occupant emergency plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not mission/ business process- or IS-based	Incident-based plan initiated immediately after an event, preceding a COOP or DRP activation

Source: National Institute of Standards and Technology, *NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems*, USA, 2010. Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

For the planning, implementation and evaluation phase of the BCP, the following should be agreed on:

- Policies that will govern all of the continuity and recovery efforts
- Goals/requirements/products for each phase
- Alternate facilities to perform tasks and operations
- Critical information resources to deploy (e.g., data and systems)
- Persons responsible for completion
- Available resources to aid in deployment (including humans)
- Scheduling of activities with priorities established

Most BCPs are created as procedures that accommodate recovery of information systems (i.e., data storage, servers, etc.), user workstations, other selected equipment (e.g., card readers, barcode scanners, printers, etc.) and the network (e.g., channels, equipment). Copies of the plan should be kept offsite—at the recovery facility, the media storage facility and possibly at the homes of key decision-making personnel. Organizations frequently place an electronic version of the plan on a mirrored website.

Key Decision-Making Personnel

The plan should contain a telephone list or call tree (i.e., a notification directory of key decision-making IT and end-user personnel required to initiate and carry out recovery efforts). This is usually a telephone directory of people who should be notified if an incident/disaster or catastrophe occurs, and it often can be automated. Points to remember when preparing the list are:

- In the event of a widespread disaster or a fire/ explosion during normal business hours that heavily damages the organization's offices, many team leaders may not be available.
- The call tree should be highly redundant, maintained on hard copy and possibly on an intranet and updated regularly.

This directory should contain the following information:

- A prioritized list of contacts (i.e., who gets called first)
- Primary and emergency telephone numbers and addresses for each critical contact person. These usually will be key team leaders responsible for contacting their team members.
- Phone numbers and addresses for representatives of equipment and software vendors
- Phone numbers of contacts within companies that have been designated to provide supplies and equipment or services
- Phone numbers of contact persons at recovery facilities, including hot-site representatives and predefined network communications rerouting services
- Phone numbers of contact persons at offsite media storage facilities and the contact persons within the company who are authorized to retrieve media from the offsite facility
- Phone numbers of insurance company agents
- Phone numbers of contacts at contract personnel services
- Phone numbers and contacts of legal/regulatory/ governmental agencies, if required
- A procedure to ascertain how many people were reached while using the call tree

Backup of Required Supplies

The plan should have provisions for all supplies necessary to continue normal business activities in the recovery effort. This includes detailed, up-to-date hard copy procedures that can be followed easily by staff and by contract personnel unfamiliar with the standard and recovery operations. Also, a supply of special forms, such as check stock, invoices and order forms, should be secured at an offsite location.

If the data entry function depends on certain hardware devices and/or software programs, those programs and equipment should be provided at the hot site. The same applies to cryptographic equipment, including electronic keys (e.g., RSA tokens and USB keys).

Insurance

The plan should contain key information about the organization's insurance. The IT processing insurance policy is usually a multi-peril policy designed to provide various types of IT coverage. It should be constructed in modules to adapt to the insured's particular IT environment.

Note

Specifics on insurance policies are not tested on the CISA exam because they differ from country to country. The test covers what should be included in policies and third-party agreements, not specific types of coverage.

Specific types of coverage available are:

- **IT equipment and facilities**—Provides coverage for physical damage to the IPF and owned equipment. (Leased equipment insurance should be obtained when the lessee is responsible for hazard coverage.) The IS auditor is cautioned to review these policies because many obligate insurance vendors to replace non-restorable equipment only with "like kind and quality," not necessarily with new equipment from the same vendor that supplied the damaged equipment.
- **Media (software) reconstruction**—Covers damage to IT media that is the insured's property and for which the insured may be liable. Insurance is available for on-premises, off-premises or in-transit situations. It covers the actual reproduction cost of the property. The amount of coverage needed includes programming costs to reproduce the damaged media, backup expenses and physical replacement of media devices.
- **Extra expense**—Designed to cover the extra costs of continuing operations following damage or destruction at the IPF. Extra-expense insurance is based on the availability and cost of backup facilities and operations. The extra expense can also cover the loss of net profits caused by computer media damage. This coverage provides reimbursement for monetary losses resulting from suspending operations due to the physical loss of equipment or media. An example of a situation requiring this type of coverage is if the information processing facilities were on the sixth floor and the first five floors were destroyed by fire. In this case, operations would be interrupted even though the IPF remained unaffected.
- **Business interruption**—Covers the loss of profit due to the disruption of the company's activity caused by any IT organization's malfunction
- **Valuable papers and records**—Covers the actual cash value of papers and records (not defined as media) on the insured's premises against direct physical loss or damage
- **Errors and omissions**—Provides legal liability protection if the professional practitioner commits an act, error or omission that results in financial loss to a client. This insurance was originally designed for service bureaus but is now available from several insurance companies for protecting systems analysts, software designers, programmers, consultants and other IS personnel.
- **Fidelity coverage**—Usually takes the form of banker's blanket bonds, excess fidelity insurance and commercial blanket bonds and covers loss from dishonest or fraudulent employee acts. This type of coverage is prevalent in financial institutions operating their own IPFs.
- **Media transportation**—Provides coverage for potential loss or damage to media in transit to off-premises IPFs. Transit coverage wording in the policy usually specifies that all documents must be filmed or otherwise copied. When the policy does not specifically state that data be filmed before being transported and the work is not filmed, management should obtain a letter from the insurance carrier that specifically describes the carrier's position and coverage if data is destroyed.

Most insurance covers only financial losses based on the historical level of performance and not on the current level of performance. The IS auditor should ensure that the valuation of insured items, such as technical equipment, infrastructure and data, is appropriate and current. Also, insurance does not compensate for the loss of reputation, image, goodwill, etc.

4.15.9 Plan Testing

If they are tested, most business continuity tests fall short of a full-scale test of all operational portions of the organization. This should not preclude performing full or partial testing. One of the purposes of the business continuity test is to determine how well the plan works or which portions of the plan need improvement.

The test should be scheduled during a time that will minimize disruptions to normal operations. Weekends are generally a good time to conduct tests. It is important

©ISACA. All Rights Reserved.

that the key recovery team members are involved in the test process and allotted the necessary time to put their full effort into it. The test should address all critical components and simulate actual primetime processing conditions, even if the test is conducted during off hours.

Specifications

Tasks the test should strive to accomplish include:

- Verify the completeness and precision of the BCP.
- Evaluate the performance of the personnel involved in the exercise.
- Appraise the training and awareness of all employees, not just business continuity team members.
- Evaluate the coordination among the business continuity team and external vendors and suppliers.
- Measure the ability and capacity of the backup site to perform prescribed processing.
- Assess the vital records retrieval capability.
- Evaluate the state and quantity of equipment and supplies relocated to the recovery site.
- Measure the overall operational and IT processing performance related to maintaining the business entity.

Note

Assessing the results and the value of the BCP and the DRP tests is an important part of the IS auditor's responsibility.

Test Execution

Testing consists of the following phases:

- **Pretest**—The actions necessary to set the stage for the actual test. These range from placing tables in the proper operations recovery area to transporting and installing backup telephone equipment. These activities are outside the realm of those that would take place in the case of a real emergency, in which there was no forewarning of the event and, therefore, no time to take preparatory actions.
- **Test**—This is the real action of the business continuity test. Actual operational activities are executed to test the specific objectives of the BCP. Data entry, telephone calls, IS processing, handling orders, and moving personnel, equipment and suppliers should occur. Evaluators review staff members as they perform the designated tasks. This is the actual test of preparedness to respond to an emergency.
- **Posttest**—The cleanup of group activities. This phase comprises such assignments as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third-party systems. The posttest cleanup also includes formally evaluating the plan and implementing indicated improvements.

In addition, the following types of tests may be performed:

- **Desk-based evaluation (tabletop or paper test)**—A paper walk-through involving major players in the plan's execution who determine what might happen in a particular type of service disruption. They may walk through the entire plan or just a portion. The paper test usually precedes the preparedness test.
- **Preparedness test**—Usually a localized version of a full test, wherein actual resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan. It can be a cost-effective way to gradually obtain evidence of the plan's effectiveness. It also provides a means to improve the plan in increments.
- **Full operational test**—One step away from a service disruption. The organization should have tested the plan well on paper and locally before completely shutting down operations. For purposes of the BCP testing, this is a disaster.

Documentation of Results

During every test phase, detailed documentation of observations, problems and resolutions should be maintained. Each team should have a diary form with specific steps and information to record, which can be used as documentation. This documentation is important historical information to facilitate recovery during a real disaster. Additionally, the insurance company or the local authorities may ask for it. The documentation also aids in performing a detailed analysis of the plan's strengths and weaknesses.

Results Analysis

It is important to have ways to measure the plan's success and test it against the stated objectives. Therefore, results must be quantitatively gauged instead of evaluated through observation alone.

Specific measurements vary depending on the test and the organization; however, the following general measurements usually apply:

- **Time**—Elapsed time for completion of prescribed tasks, delivery of equipment, assembly of personnel and arrival at a predetermined site
- **Amount**—Amount of work performed at the backup site by clerical personnel and IS processing operations

 ©ISACA. All Rights Reserved.

- **Count**—The number of vital records successfully carried to the backup site versus the required number and the number of supplies and equipment requested versus actually received. Also, the number of critical systems successfully recovered can be measured with the number of transactions processed.
- **Accuracy**—Accuracy of the data entry at the recovery site versus normal accuracy (as a percentage). Also, the accuracy of actual processing cycles can be determined by comparing output results with those for the same period processed under normal conditions.

Plan Maintenance

Plans and strategies for business continuity should be reviewed and updated regularly to reflect continuing recognition of changing requirements or unscheduled revisions when an important change affects the plans and strategies. Factors that may impact business continuity requirements and the need for the plan to be updated include:

- A strategy that is appropriate at one point in time may not be adequate as the needs of the organization change (e.g., business processes, new departments, changes in key personnel).
- New resources/applications may be developed or acquired.
- Changes in business strategy may alter the significance of critical applications or deem additional applications as critical.
- Software or hardware environment changes may make current provisions obsolete or inappropriate.
- New events or a change in the likelihood of events may cause disruption.
- Changes may be made to key personnel or their contact details.

An important step in maintaining a BCP is updating and testing it whenever relevant changes occur within the organization. It is also desirable to include BCP as part of the SDLC process.

The responsibility for maintaining the BCP falls on the BCP coordinator. Specific plan maintenance responsibilities include:

- Develop a schedule for periodic review and maintenance of the plan, advising all personnel of their roles and the deadlines for receiving revisions and comments.
- Call for unscheduled revisions when significant changes have occurred.
- Review revisions and comments and update the plan within a certain number of days (e.g., 30 days, two weeks) of the review date.
- Arrange and coordinate scheduled and unscheduled tests of the BCP to evaluate its adequacy.
- Participate in the scheduled plan tests, which should be performed at least once per year on specific dates. For scheduled and unscheduled tests, the coordinator will write evaluations and integrate changes to resolve unsuccessful test results into the BCP within a certain number of days (e.g., 30 days, two weeks).
- Develop a schedule for training recovery personnel in emergency and recovery procedures as outlined in the BCP. Training dates should be scheduled within 30 days of each plan revision and scheduled plan test.
- Maintain records of BCP maintenance activities—testing, training and reviews.
- Periodically update the notification directory of all personnel changes—including phone numbers, responsibilities or statuses within the company—at least quarterly (shorter periods are recommended).

A software tool for administering continuity and recovery plans may be useful for tracking and following up on maintenance tasks.

4.15.10 Business Continuity Management Good Practices

The need to revisit and improve the business continuity program continually and periodically is critical to developing a successful and robust recovery strategy for an organization, irrespective of whether the organization is at the initial stage of developing a BCP. To enhance business continuity management capabilities (and to comply with regulatory guidelines), some organizations have started adopting good practices from industry-independent and industry-specific entities and regulatory agencies.

Some examples include:

- **Business Continuity Institute (BCI)**—Provides good practices for business continuity management
- **Disaster Recovery Institute International (DRII)**—Provides professional practices for business continuity professionals
- **US Federal Emergency Management Association (FEMA)**—Provides business and industry guidance for emergency management
- **ISACA**—COBIT provides guidance on relevant IT controls
- **US National Institute of Standards and Technology (NIST)**—Promotes innovation and

©ISACA. All Rights Reserved.

industrial competitiveness by advancing measurement science, standards and technology
- **US Federal Financial Institutions Examination Council (FFIEC)**—An interagency body in the United States composed of several federal regulatory agencies responsible for overseeing and regulating financial institutions
- **US Health and Human Services (HHS)**—Describes requirements for managing health information in the Health Insurance Portability and Accountability Act (HIPAA)
- **ISO 22301:2019: Security and resilience**—Business continuity management systems—Requirement—A framework for establishing, implementing, maintaining and continually improving a business continuity management system within an organization

To ensure continuous service, a BCP should be written to minimize the impact of disruptions. The BCP should be based on the long-range IT plan. It should support and be aligned with the overall business continuity strategy. The process of developing and maintaining an appropriate DRP/BCP is as follows:
- Conduct a risk assessment.
- Identify and prioritize the systems and other resources required to support critical business processes during a disruption.
- Identify and prioritize threats and vulnerabilities.
- Prepare BIAs for the effect of the loss of critical business processes and their supporting components.
- Choose appropriate controls and measures for recovering IT components to support critical business processes.
- Develop a detailed plan for recovering IS facilities (DRP).
- Develop a detailed plan for the critical business functions to continue to operate at an acceptable level (BCP).
- Test the plans.
- Maintain the plans as the business changes and systems develop.

4.15.11 Auditing Business Continuity

The IS auditor's tasks related to business continuity include:
- Understand and evaluate business continuity strategy and its connection to business objectives.
- Review the BIA findings to ensure that they reflect current business priorities and current controls.
- Evaluate the BCPs to determine their adequacy and currency by reviewing the plans and comparing them to appropriate standards and/or government regulations, including the RTO, RPO and other metrics defined by the BIA.
- Verify that the BCPs are effective by reviewing the results from previous tests performed by IT and end-user personnel.
- Evaluate cloud-based mechanisms.
- Evaluate offsite storage to ensure its adequacy by inspecting the facility and reviewing its contents, security and environmental controls.
- Verify the arrangements for transporting backup media to ensure they meet the appropriate security requirements.
- Evaluate the ability of personnel to respond effectively in emergencies by reviewing emergency procedures, employee training and results of tests and drills.
- Ensure that the plan maintenance process is in place and effective and covers periodic and unscheduled revisions.
- Evaluate whether the business continuity manuals and procedures are written simply and understandably. This can be achieved through interviews and determining whether all the stakeholders understand their roles and responsibilities concerning business continuity strategies.

Reviewing the Business Continuity Plan

When reviewing the plan, IS auditors should verify that the basic elements of a well-developed plan are evident. It is important to remember when working with third parties that the right to audit and the scope of an audit may be restricted or limited by contracts.

Specific audit procedures should be carried out to address basic BCP elements.

Review the Document

The IS auditor should:
- Obtain a copy of the current business continuity policy and strategy.
- Obtain a current copy of the BCP or manual.
- Obtain a copy of the most recent BIA findings and identify the RTO, RPO and other key strategic directives.
- Sample the distributed copies of the manual and verify that they are current.
- Verify whether the BCP supports the overall business continuity strategy.
- Evaluate the effectiveness of the documented procedures for invoking the BCP execution.
- Evaluate the procedure for updating the manual. Are updates applied and distributed promptly?

 ©ISACA. All Rights Reserved.

Are specific responsibilities documented for the maintenance of the manual?

Review the Applications Covered by the Plan

The IS auditor should:

- Review the identification, priorities and planned support of critical applications, both server-based and workstation-based.
- Determine whether all applications have been reviewed for their tolerance level during a disaster.
- Determine whether all critical applications (including PC applications) have been identified.
- Determine whether the secondary site has the correct versions of all system software. Verify that all the software is compatible; otherwise, the system cannot process production data during recovery.

Review the Business Continuity Teams

The IS auditor should:

- Obtain a member list for each recovery/continuity/response team.
- Obtain a copy of agreements relating to the use of backup facilities.
- Review the list of business continuity personnel (i.e., emergency hot-site contacts, emergency vendor contacts, etc.) for appropriateness and completeness.
- Call a sample of the people indicated and verify that their phone numbers and addresses are correct and that they possess a current copy of the business continuity manual.
- Interview them to understand their assigned responsibilities in case of interruption/disaster situations.

Plan Testing

The IS auditor should:

- Evaluate the procedures for documenting the tests.
- Review the backup procedures followed for each area covered by the DRP.
- Determine whether the backup and recovery procedures are being followed.

In addition to the previous steps, the IS auditor should:

- Evaluate whether all written emergency procedures are complete, appropriate, accurate, current and easy to understand.
- Identify whether the transactions reentered in the system through the recovery process need to be separately identified from the normal transactions.
- Determine whether all recovery/continuity/response teams have written procedures to follow in the event of a disaster.
- Determine whether a suitable procedure exists for updating the written emergency procedures.
- Determine whether user recovery procedures are documented.
- Determine whether the plan adequately addresses movement to the recovery site.
- Determine whether the plan adequately addresses recovering from the recovery site.
- Determine whether items necessary to reconstruct the IPF are stored offsite, such as blueprints, hardware inventory and wiring diagrams.

Questions to consider include:

- Who is responsible for the administration or coordination of the plan?
- Is the plan administrator/coordinator responsible for keeping the plan current?
- Where is the DRP stored?
- What critical systems are covered by the plan?
- What systems are not covered by the plan? Why not?
- What equipment is not covered by the plan? Why not?
- Does the plan operate under any assumptions? What are they?
- Does the plan identify rendezvous points for the disaster management committee or emergency management team to meet and decide if business continuity should be initiated?
- Are the documented procedures adequate for a successful recovery?
- Does the plan address disasters of varying degrees?
- Are telecommunication backups (both data and voice line backups) addressed in the plan?
- Where is the backup facility site?
- Does the plan address relocation to a new IPF if the original center cannot be restored?
- Does the plan include procedures for merging master file data, automated media management system data, etc., into predisaster files?
- Does the plan address loading data processed manually into an automated system?
- Are formal backup procedures and responsibilities specified?
- What training in using backup equipment and established procedures has been given to personnel?
- Are the restoration procedures documented?
- Are regular and systematic backups of required sensitive and/or crucial applications and data files being taken?
- Who determines the methods and frequency of data backup for stored critical information?
- What type of media is being used for backups?

©ISACA. All Rights Reserved.

- Is offsite storage used to maintain backups of critical information required for onsite or offsite operations processing?
- Is there adequate documentation to perform a recovery in case of disaster or data loss?
- Does the plan include a schedule for testing and training?
- Are the requirements for normal operations and disasters defined in the relevant SLAs about how the service will operate?

Evaluation of Prior Test Results

The BCP coordinator should maintain historical documentation of the results of previous business continuity tests. The IS auditor should review the results and determine whether actions requiring correction have been incorporated into the plan. Also, the IS auditor should evaluate BCP/DRP prior to testing for thoroughness and accuracy in accomplishing their objectives. Test results should be reviewed to determine whether the relevant results were achieved and to determine problem trends and appropriate resolutions of problems.

Evaluation of Offsite Storage

The offsite storage facility should be evaluated to ensure that critical media and proper documentation are present, synchronized and current. The evaluation should address data files, applications software, applications documentation, systems software, systems documentation, operations documentation, necessary supplies, special forms and a copy of the BCP. The IS auditor should perform a detailed inventory review, including testing for correct dataset names, volume serial numbers, accounting periods and bin locations of media. The IS auditor should also review the documentation, compare it for currency with production documentation, evaluate the availability of the facility, and ensure that it conforms with management's requirements. The IS auditor should also review the method of transporting backup data to and from the offsite storage facility to ensure it does not represent a weakness in the ISMS.

Evaluation of Security at the Offsite Facility

The security of the offsite facility should be evaluated to ensure that it has the proper physical and environmental access controls. These controls include:

- Ability to limit access to authorized users of the facility
- Raised flooring
- Humidity controls
- Temperature controls
- Specialized circuitry
- Uninterruptible power supply
- Water detection devices
- Smoke detectors
- Appropriate fire extinguishing system

The IS auditor should examine the equipment for current inspection and calibration tags. This review should also consider the security requirements of media transportation.

Interviewing Key Personnel

The IS auditor should interview key personnel required for the successful recovery of business operations. All key personnel should understand their responsibilities and provide up-to-date detailed documentation describing their tasks.

Reviewing the Alternative Processing Contract

The IS auditor should obtain a copy of the contract with the vendor of the alternative processing facility. The vendor's references should be checked to ensure reliability, and all vendor promises should be verified in writing. The contract review should:

- Ensure that the contract is written clearly and understandably
- Ensure there was a legal review for required terms and conditions to meet all applicable laws and regulations
- Reexamine and confirm the organization's agreement with the rules for sites shared with other subscribers
- Ensure that insurance coverage ties in with and covers all (or most) disaster expenses
- Ensure that tests can be performed at the hot site at regular intervals
- Review and evaluate communications requirements for the backup site
- Ensure that a lawyer specializing in such contracts reviews enforceable source code escrow
- Determine the limitation recourse tolerance in the event of a breached agreement

Reviewing Insurance Coverage

Insurance coverage must reflect the actual cost of recovery. When considering the insurance premium (cost), the coverage for media damage, business interruption, equipment replacement and business continuity processing should be reviewed for adequacy. The specific risk areas should be found within the BIA, customer contracts, SLAs and regulatory impacts resulting from a break in business operations.

Note

The CISA candidate should know what critical provisions must be included in insurance policies to safeguard the organization.

4.16 Disaster Recovery Plans

Disaster recovery planning in support of business operations/provisioning IT service is an element of an internal control system established to manage availability and restore critical processes/IT services in the event of an interruption. The purpose of this continuous planning process is to ensure that cost-effective controls are in place to prevent possible IT disruptions and to recover the IT capacity of the organization in the event of a disruption. The importance of the availability of individual applications/IT services depends on the importance of the business processes they support. The importance and urgency of these business processes and corresponding IT services and applications can be defined through performing a BIA and assigning RPOs and RTOs. The availability of business data and the ability to process and handle it are vital to any organization's sustainable development and/or survival. Planning for disasters is an important part of the risk management and business continuity planning processes.

Disaster recovery planning is a continuous process. After the criticality of business processes and supporting IT services, systems and data is determined, it is periodically reviewed and revisited. There are at least two important outcomes of disaster recovery planning:

1. Changes in IT infrastructure (servers, networks, data storage systems, etc.), supporting processes (increasing maturity), procedures and organizational structure (new headcount or new roles). These changes are combined into programs spanning three to five years, often called IT DR strategies.
2. DRPs developed as part of the DR process that directs the response to incidents ranging from simple emergencies to full-blown disasters. The plan types range from department-level, simple procedures down to modular, multitiered plans that cover multiple locations and multiple lines of business.

The ultimate goal of the disaster recovery planning process is to respond to incidents that may impact people as well as the ability of operations to deliver goods and services to the marketplace and to comply with regulatory requirements.

Disaster recovery planning may be subject to various compliance requirements depending upon geographic location, nature of business and the legal and regulatory framework. Organizations engage third parties to perform the activities on their behalf, and those third parties are subject to compliance. Most compliance requirements focus on continuity of service; however, human safety is the most essential aspect. For example, in case of fire, safe evacuation comes first; restoring service is a secondary activity.

Just as with business continuity, if a disaster occurs at a third-party facility that provides services to the organization, the contracting organization may have no recourse but to wait for the vendor to enact its DRP before services are recovered.

This section focuses on the key activities an organization must perform to proactively plan for and manage a disaster's consequences.

4.16.1 Recovery Point Objective, Recovery Time Objective and Mean Time to Repair

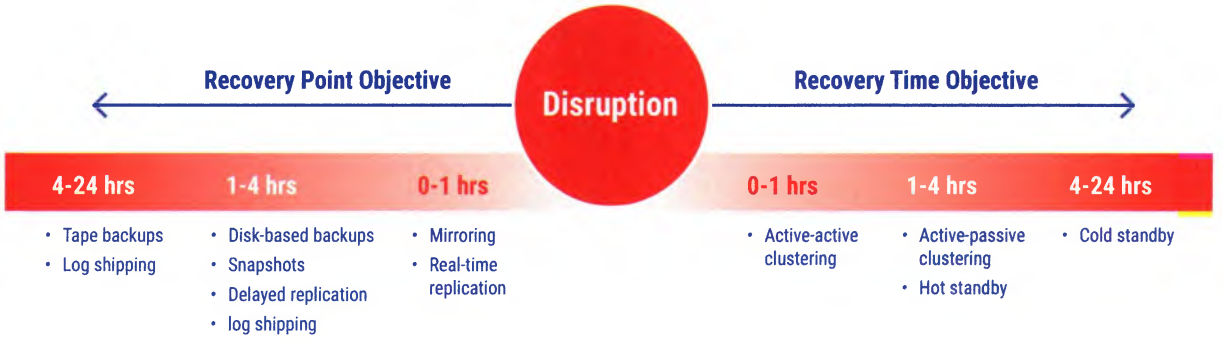
The RPO is determined based on the acceptable data loss in case of disruption of operations. It indicates the earliest time in which it is acceptable to recover the data. For example, if the process can afford to lose the data up to four hours before the disaster, the latest backup should be up to four hours before disaster or interruption. The transactions during the RPO period and interruption need to be entered after recovery (known as catch-up data).

It is almost impossible to recover the data completely. Even after entering incremental data, some data is still lost. This is referred to as orphan data. The RPO directly affects the technology to back up and recover data.

The RTO is determined based on the acceptable downtime in case of a disruption of operations. It indicates the earliest point when business operations (and supporting IT systems) must resume after a disaster. **Figure 4.40** shows the relationship between the RTO and RPO and gives examples of technologies used to meet the RPOs and RTOs.

©ISACA. All Rights Reserved.

Figure 4.40—Relationship Between RTO and RPO



Both concepts are based on time parameters. The nearer the time requirements are to the center (0-1 hour), the higher the cost of the recovery strategies. If the RPO is in minutes (the lowest possible acceptable data loss), then data mirroring or real-time replication should be implemented as the recovery strategy. If the RTO is in minutes (lowest acceptable time down), a hot site, dedicated spare servers (and other equipment) and clustering must be used. Disaster tolerance is the time gap within which the business can accept the unavailability of IT critical services; therefore, the lower the RTO, the lower the disaster tolerance.

RTO affects the technology used to make applications/IT systems available—what to use for recovery (e.g., warm site, hot site, clusters). RPO usually affects data protection solutions (backup and recovery, synchronous or asynchronous data replication).

Note

The CISA candidate should know which recovery strategies would be best with different RTO and RPO parameters.

MTTR is a measure of the average time it takes to repair a failed system or device. It is calculated by dividing the total time spent on repairs by the number of repairs performed. MTTR is an important metric for businesses and organizations because it can have a significant impact on productivity and costs.

A high MTTR means that systems and devices are down for longer periods of time, which can lead to lost productivity and revenue. A low MTTR means that systems and devices are repaired quickly, which minimizes downtime and disruption. MTTR can be affected by a number of factors, such as:

- The complexity of the system or device being repaired
- The availability of spare parts
- The skill and experience of the repair technicians
- The number of repair technicians available
- The organization's maintenance procedures

In addition to RTO, RPO and MTTR, some additional parameters are important in defining the recovery strategies. These include:

- **Interruption window**—The maximum period the organization can wait from the point of failure to the critical services/applications restoration. After this time, the progressive losses caused by the interruption are unaffordable.
- **Service delivery objective (SDO)**—Level of services to be reached during the alternate process mode until the normal situation is restored. This is directly related to the business needs.
- **Maximum tolerable outages (MTOs)**—Maximum time the organization can support processing in an alternate mode. After this point, different problems may arise, especially if the alternate SDO is lower than the usual SDO, and the amount of information to be updated can become unmanageable.

4.16.2 Recovery Strategies

A recovery strategy identifies the best way to recover a system (one or many) in case of interruption, including disaster. It provides guidance based on which detailed recovery procedures can be developed. Different strategies should be considered, and all alternatives should be presented to senior management. Senior management should select the most appropriate strategies

from the alternatives provided and accept the inherent residual risk.

The selected strategies should be used to further develop the detailed BCP.

The selection of a recovery strategy depends on:
- The criticality of the business process and the applications supporting the processes
- Cost
- Time required to recover
- Security

There are various strategies for recovering critical information resources. The appropriate strategy is the one with an adequate recovery time cost that is reasonable compared to the impact and likelihood of occurrence as determined in the BIA. The recovery cost is a measure of preparing for possible disruptions (e.g., the fixed costs of purchasing, maintaining and regularly testing redundant computers and maintaining alternate network routing) and the variable costs of putting them into use in the event of a disruption. The former costs can often be insured against, but the latter generally cannot. However, the premiums for disaster insurance usually will be lower if there is a suitable plan.

Generally, each IT platform that runs an application supporting a critical business function will need a recovery strategy. The most appropriate alternative, in terms of cost to recover and impact cost, should be selected based on the relative risk level identified in the BIA.

4.16.3 Recovery Alternatives

When the normal production facilities become unavailable, the business may use alternate facilities to sustain critical processing until the primary facilities can be restored. **Figure 4.41** lists the most common recovery alternatives.

Figure 4.41—Recovery Alternatives

Recovery Alternative	Description
Cold site	A facility with space and basic infrastructure adequate to support the resumption of operations but lacking any IT or communications equipment, programs, data or office support. A plan that specifies use of a cold site must include a provision to acquire and install the requisite hardware, software and office equipment to support critical applications when the plan is activated. To use a sports analogy, a cold site is like having a substitute on the bench, ready to be called into the game.
Mobile site	A packaged, modular processing facility mounted on transportable vehicles and kept ready to be delivered and set up at a location that may be specified upon activation. A plan using mobile processing must specify the site locations that may be used. The plan must provide right-of-access to the sites selected by the vendor and the company. The plan must also provide necessary ancillary infrastructure to support the sites, such as access roads, water, waste disposal, power and communications.
Warm site	A complete infrastructure, partially configured with IT, usually with network connections and essential peripheral equipment such as disk drives and controllers. The equipment may be less capable than the standard production equipment yet still be adequate to sustain critical applications on an interim basis. Typically, employees would be transferred to the warm site, and current versions of programs and data would need to be loaded before operations could resume at the warm site. Using the sports analogy, a warm site is a substitute player warming up and getting ready to enter the game.

©ISACA. All Rights Reserved.

Figure 4.41—Recovery Alternatives (cont.)

Recovery Alternative	Description
Hot site	A facility with space and basic infrastructure and all the IT and communications equipment required to support critical applications, along with office furniture and equipment for use by the staff. Hot sites usually maintain installed versions of the programs required to support critical applications. Data also may be duplicated to the hot site in real or near-real time. If not, the most recent backup copies of data may need to be loaded before critical applications can be resumed. Although hot sites may have a small staff assigned, employees are usually transferred to the hot site from the primary site to support operations upon activation. Using a sports analogy, a hot site is a substitute on the sideline waiting to enter the game.
Mirrored site	A fully redundant site with real-time data replication from the production site. Mirrored sites are fully equipped and staffed and can assume critical processing with no interruption perceived by the users.
Reciprocal agreements	Agreements between separate but similar companies to temporarily share their IT facilities if one company loses processing capability. Reciprocal agreements are not considered a viable option due to the constraints of maintaining hardware and software compatibility between the companies, the complications of maintaining security and privacy compliance during shared operations, and the difficulty of enforcing the agreements should a conflict arise when a plan is activated.
Reciprocal agreements with other organizations	Agreements between two or more organizations with unique equipment or applications. Under a typical agreement, participants promise to assist each other during an emergency. These agreements are less frequently used than traditional reciprocal agreements.

Alternatives that provide the fastest recovery time require the most dedicated resources on an ongoing basis and thus incur the greatest cost to the company. Management will establish an optimal RTO and select an appropriate recovery alternative by comparing the business costs associated with the interruption of critical processes (developed in the BIA) to the cost of the various alternative options.

The alternate site should be selected with consideration that it will be located beyond the geographic area affected by any disruptive events considered in the plan. Rather than specifying a particular separation distance, the impact and nature of the disruptive events should be considered in determining an adequate separation from the primary site.

Regardless of which type of alternative processing is used, the plan needs to include a provision to establish network communication to the alternate site. The plan should provide redundant solutions to ensure that communications can be established at the alternate site following the interruption of normal processing by any anticipated cause.

The alternate processing facility can be provided by a third-party vendor or the company's own resources. When the company owns the facility, conflicts can be prevented or quickly resolved by senior management. When the facility is provided by a third party, the company needs to have clearly stated contracts ensuring that following a disaster it will get access to the resources it needs without delay. Consideration must be given to the likelihood that multiple companies must use the alternate processing facility simultaneously. Other companies in the area may also be trying to restore critical processing.

Contractual Provisions

Contractual provisions for the use of third-party sites should cover the following:

- **Configurations**—Are the hardware and software configurations for the facility adequate to meet company needs? Is there a provision to update the configurations and conduct tests to ensure that the configurations remain adequate over time?
- **Disaster**—Is the definition of disaster broad enough to meet anticipated needs?
- **Access**—Is the use of the facility exclusive? Does the customer have to share the available space if multiple customers declare a disaster? Does the company have guaranteed assurance that it will have adequate access to the site and its resources following a disaster?

 ©ISACA. All Rights Reserved.

Does the agreement satisfactorily specify how access conflicts will be resolved?

- **Priority**—Does the agreement provide the company with satisfactory priority following a disaster? Does the agreement preclude sharing the needed resources with governmental entities that might preempt the company following a disaster?
- **Availability**—Will the facility be available to the company immediately when needed?
- **Speed of availability**—How soon after a disaster will facilities be available?
- **Subscribers per site**—Does the agreement limit the number of subscribers per site?
- **Subscribers per area**—Does the agreement limit the number of subscribers in a building or area?
- **Preference**—Who gets preference if there are common or regional disasters? Is there backup for the backup facilities? Is the use of the facility exclusive or shared among multiple customers that simultaneously declare a disaster? Does the vendor have more than one facility available for subscriber use?
- **Insurance**—Is there adequate insurance coverage for company employees at the backup site? Will existing insurance reimburse those fees?
- **Use period**—How long is the facility available for use? Is the period adequate? What technical support will the site operator provide? Is it adequate?
- **Communications**—Are the communications adequate? Are the communication connections to the backup site sufficient to permit unlimited communication with the alternate site if needed?
- **Warranties**—What warranties will the vendor make regarding the site's availability and the facilities' adequacy? What liability limitations exist, and can the company accept those terms?
- **Audit**—Is there a right-to-audit clause permitting an audit of the site to evaluate the logical, physical and environmental security?
- **Testing**—What testing rights are included in the contract? Check with the insurance company to determine any reduction of premiums that may be forthcoming due to the backup site's availability.
- **Reliability**—Can the vendor attest to the reliability of the site(s) being offered? Ideally, the vendor should have a UPS, limited subscribers, sound technical management, reliable computer hardware and software compatibility guarantees.
- **Security**—Can the site be adequately secured to comply with the company's security policy?

Procuring Alternative Hardware

Companies planning to use a cold or warm site must include in their plan the provision to acquire hardware and software to equip the site upon activation. Companies can acquire and store the necessary equipment and software beforehand or plan to acquire the hardware and software when needed. A key factor in the decision is whether the company uses standard systems that can be readily acquired when replacements are needed or if it uses systems that are unique, specialized, outdated or otherwise difficult to acquire on short notice. If companies depend on hardware that is not readily available to support critical business applications, plans must include provisions to acquire the hardware in time to meet the RTO. This fact may dictate that the companies acquire the critical components beforehand and store them so they are available when required.

Additionally, recovery of IT facilities involves telecommunications, which typically entails:

- Network disaster prevention considerations
  - Alternative routing
  - Diverse routing
  - Long-haul network diversity
  - Protection of the local loop
  - Voice recovery
  - Availability of appropriate circuits and adequate bandwidth
  - Server DRPs

4.16.4 Development of Disaster Recovery Plans

IT disaster recovery planning follows a path that aligns with the greater business continuity planning process. The IT disaster recovery strategy is developed after conducting a BIA and risk assessment (or otherwise determining the risk and effectiveness of mitigation controls). Implementing a disaster recovery strategy means making changes to:

- IT systems
- Networks
- IT processing sites
- Organization structure (headcount, roles, positions)
- IT processes and procedures

An IT DRP is a well-structured collection of processes and procedures intended to make the disaster response and recovery effort swift, efficient and effective to achieve synergy between recovery teams. The plan should be documented and written in simple, understandable language.

©ISACA. All Rights Reserved.

IT DRP Contents

Typically, the IT DRP contains:

- Procedures for declaring a disaster (escalation procedures)
- Criteria for plan activation (i.e., in which circumstances the disaster is declared, when the IT DRP is put into action, which scenarios are covered by the plan [loss of the IT system, loss of the processing site, loss of the office])
- Linkage with the overarching plans (e.g., emergency response plan or crisis management plan or BCPs for different lines of business)
- The person (or people) responsible for each function in plan execution
- Recovery teams and their responsibilities
- Contact and notification lists (contact information for recovery teams, recovery managers, stakeholders, etc.)
- The step-by-step explanation of the whole recovery process (i.e., where and when the recovery should take place [the same site or backup site], what has to be recovered [IT systems, networks, etc.], the order of recovery)
- Recovery procedures for each IT system or component. Note the level of detail greatly varies and depends on the practices used in the organization.
- Contacts for important vendors and suppliers
- The clear identification of the various resources required for recovery and continued operation of the organization

IT DRP Scenarios

Although no two disasters are alike, the plan should outline which scenarios are covered, such as:

- Loss of network connectivity
- Loss of a key IT system
- Loss of the processing site (server room)
- Loss of critical data
- Loss of an office
- Loss of key service provider (e.g., cloud)

Normally, this section is quite short; however, it is important to remember that the best plan always accounts for the worst-case conditions (such as the peak of sales, end of the reporting period, etc.).

Recovery Procedures

Depending on the type of disaster, the sequence of the recovery effort may vary; however, the plan should contain a simple, high-level overview of the sequence for every major disaster scenario, referring to the more detailed recovery procedures.

Organization and Assignment of Responsibilities

The DRP should identify the teams with their assigned responsibilities in the event of an incident/disaster. IS and end-user personnel should be identified to review the recovery procedures developed for business/process recovery and key decision-making. The key individuals usually lead teams created in response to a critical function or task defined in the plan. Depending on the size of the business operation, teams may be designated as single-person positions. The involvement of the teams depends on the level of disruption of service and the types of assets lost or damaged. Developing a matrix on the correlation between the teams needed to participate and the estimated recovery effort/level of disruption is a good idea.

Some possible recovery/continuity/response team designations include:

- The incident response team receives information about every incident that can be considered a threat to assets/processes. This reporting can be useful for coordinating an incident in progress or a postmortem analysis. The analysis of all incidents provides input for updating the recovery plans.
- The emergency action team includes first responders, designated fire wardens and bucket crews whose function is to deal with fires or other emergency response scenarios. One of their primary functions is the orderly evacuation of personnel and safeguarding human life.
- The information security team develops the needed steps to maintain a level of information and IT resource security similar to what was in place at the primary site before the contingency, and it implements the needed security measures in the alternative environment. Additionally, this team must continually monitor the security of the system and communication links, resolve any security conflicts that impede the expeditious recovery of the system and ensure the proper installation and functioning of security software. The team also is responsible for securing the organization's assets during the disorder following a disaster.
- The damage assessment team assesses the extent of damage following a disaster. This team should comprise individuals who can assess the damage and estimate the time required to recover operations at the affected site. This team should include staff skilled in testing equipment, knowledgeable about systems and networks, and trained in applicable safety regulations and procedures. In addition, this team is responsible

for identifying possible causes of the disaster and their impact on damage and predictable downtime.

- The emergency management team is responsible for coordinating the activities of all other recovery/continuity/response teams and handling key decision-making. This team determines the activation of the BCP. Other functions entail arranging the finances of the recovery, handling legal matters evolving from the disaster, and handling PR and media inquiries. Team members function as disaster overseers and are required to:
  - Retrieve critical and vital data from offsite storage.
  - Install and/or test systems software and applications at the systems recovery site (hot site, cold site).
  - Identify, purchase and install hardware at the system recovery site.
  - Operate from the system recovery site.
  - Reroute WAN communications traffic.
  - Reestablish the local area user/system network.
  - Transport users to the recovery facility.
  - Restore databases.
  - Supply necessary office goods (e.g., basic supplies, special forms, check stock, keyboards and other computer peripherals).
  - Arrange and pay for employee relocation expenses at the recovery facility.
  - Coordinate systems use and employee work schedules.
- The offsite storage team is responsible for obtaining, packaging and shipping media and records to the recovery facilities and establishing and overseeing an offsite storage schedule for information created during operations at the recovery site.
- The software team is responsible for restoring system packs, loading and testing OS software and resolving system-level problems.
- The applications team travels to the system recovery site and restores the backup system's user packs and application programs. This team may monitor application performance and database integrity as the recovery progresses.
- The emergency operations team consists of shift operators and supervisors who will reside at the recovery site and manage system operations during the disaster and recovery projects. Another responsibility might be coordinating hardware installation if a hot site or other equipment-ready facility is not designated as the recovery center.
- The network recovery team is responsible for rerouting wide-area voice and data communications traffic, reestablishing host network control and access at the system recovery site, providing ongoing support for data communications and overseeing communications integrity.
- The communications team travels to the recovery site and works with the remote network recovery team to establish a user/system network. The communications team is also responsible for soliciting and installing communications hardware at the recovery site and working with local exchange carriers and gateway vendors to reroute local service and gateway access.
- The transportation team serves as a facilities team to locate a recovery site if one has not been predetermined and is responsible for coordinating the transport of company employees to a distant recovery site. It also may assist in contacting employees to inform them of new work locations and scheduling and arranging employee lodgings.
- The user hardware team locates and coordinates the delivery and installation of user terminals, printers, typewriters, photocopiers and other necessary equipment. This team also supports the communications team and any hardware and facilities salvage efforts.
- The data preparation and records team works from terminals connecting to the user recovery site, updating the application database. This team oversees additional data-entry personnel and assists in record salvage, acquiring primary documents and other input information sources.
- The administrative support team provides clerical support to the other teams. It serves as a message center for the user recovery site. This team also may control accounting and payroll functions and ongoing facilities management.
- The supplies team supports the efforts of the user hardware team by contacting vendors and coordinating logistics for an ongoing supply of necessary office and computer supplies.
- The salvage team manages the relocation project. This team also makes a more detailed assessment of the damage to the facilities and equipment than was performed initially, provides the emergency management team with the information required to determine whether planning should be directed toward reconstruction or relocation, provides information necessary for filing insurance claims (insurance is the primary source of funding for the recovery efforts) and coordinates the efforts necessary for immediate records salvage, such as restoring paper documents and electronic media.
- The relocation team coordinates moving from the hot site to a new or restored location. This

©ISACA. All Rights Reserved.

involves relocating the IS processing operations, communications traffic and user operations. This team also monitors the transition to normal service levels.
- The coordination team is responsible for coordinating the recovery efforts across various offices at different locations. If significant IT functions have been offshored to distant geographical locations, this team acts as the focus for coordination between the organization and the third-party service providers.
- The legal affairs team is responsible for handling the legal issues arising due to any incident or unavailability of services (e.g., according to new laws enacted by many countries, the organization is responsible for securing its IT assets, and will be liable for damages to innocent parties in case of incidence).
- The recovery test team tests various plans that have been developed and analyzes the results.
- The training team provides training to users for business continuity and disaster recovery procedures.

Note

The IS auditor should have knowledge of these responsibilities; however, the CISA candidate will not be tested on these specific assignments as they vary from organization to organization.

4.16.5 Disaster Recovery Testing Methods

Critical applications and infrastructure are identified for testing based on the risk assessment and BIA. These should be developed into a testing schedule. Recovery plans that have not been tested leave an organization with an unacceptable likelihood that plans will not work. As testing plans cost time and resources, an organization should carefully plan and develop test objectives to ensure that measurable benefits can be achieved. Once the objectives have been defined, an independent third party, such as the IS auditor, should be present to monitor and evaluate the test. One result of the evaluation step should be a list of recommendations to improve the plan.

In summary, testing should include:
- Develop test objectives.
- Execute the test.
- Evaluate the test.
- Develop recommendations to improve the effectiveness of testing processes and recovery plans.
- Implement a follow-up process to ensure that recommendations are implemented.

It is extremely unlikely that no recommendations will result and everything will work as planned. If it does, a more challenging test should likely have been planned.

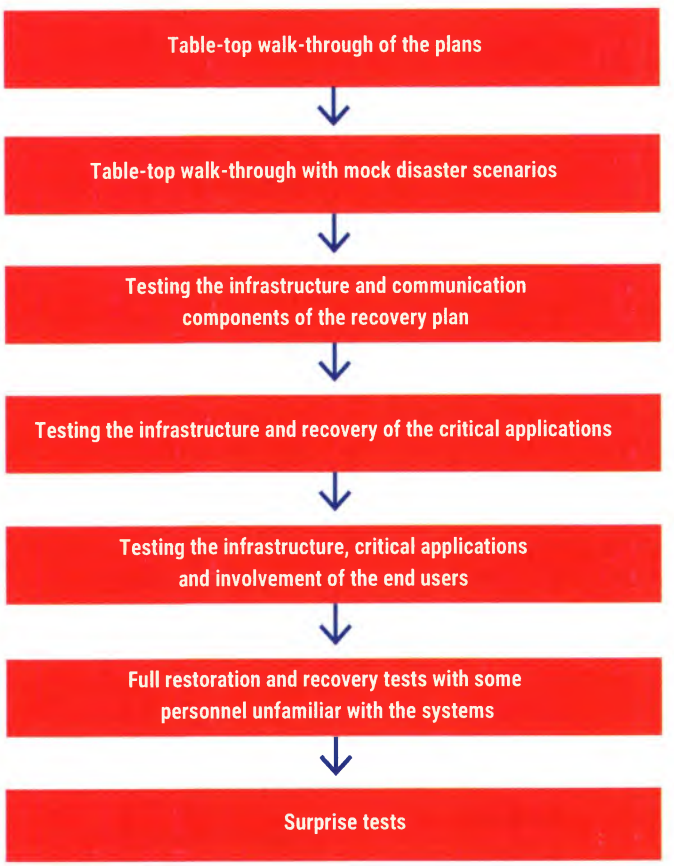
Types of Tests

The types of disaster recovery tests include:
- **Checklist review**—This is a preliminary step to a real test. Recovery checklists are distributed to all recovery team members to review and ensure that the checklist is current.
- **Structured walk-through**—Team members physically implement the plans on paper and review each step to assess its effectiveness and identify enhancements, constraints and deficiencies.
- **Simulation test**—The recovery team roleplays a prepared disaster scenario without activating processing at the recovery site.
- **Parallel test**—The recovery site is brought to operational readiness, but operations at the primary site continue normally.
- **Full interruption test**—Operations are shut down at the primary site and shifted to the recovery site to follow the recovery plan; this is the most rigorous form of testing but is expensive and potentially disruptive.

Testing should start simply and increase gradually, stretching previous tests' objectives and success criteria to build confidence and minimize risk to the business. **Figure 4.42** shows how tests can become progressively more challenging.

 ©ISACA. All Rights Reserved.

Figure 4.42—Progression of Disaster Recovery Tests



Most recovery tests fall short of a full-scale test of all operational portions of the enterprise. This should not preclude performing full or partial testing because one of the purposes of the disaster recovery test is to determine how well the plan works or which portions of the plan need improvement. Surprise tests are advantageous because they are similar to real-life incident response situations. However, they can be terribly disruptive to production and operations and can alienate individuals who are in some way disrupted by them. The test should be scheduled during a time that will minimize disruptions to normal operations, such as long weekends. The key recovery team members must be involved in the test process and allotted the time to devote their full effort. The test should address all critical components and simulate actual prime-time processing conditions, even if the test is conducted during off hours. Ideally, full-interruption tests should be performed annually after individual plans have been tested separately with satisfactory results.

Testing

The test should accomplish the following tasks:

- Verify the completeness and precision of the response and recovery plan.
- Evaluate the performance of the personnel involved in the exercise.
- Appraise the demonstrated training and awareness level of individuals not part of the recovery/response team.
- Evaluate coordination among team members and external vendors and suppliers.
- Measure the ability and capacity of the backup site to perform prescribed processing.
- Assess the vital records retrieval capability.
- Evaluate the state and quantity of equipment and supplies relocated to the recovery site.

©ISACA. All Rights Reserved.

- Measure the overall performance of operational and IS systems processing activities related to maintaining the business entity.

As with business continuity testing, DRP testing includes:

- **Pretest**—The pretest consists of the actions necessary to set the stage for the actual test, including transporting and installing required backup equipment, gaining access to the recovery site, accessing recovery documentation, etc.
- **Test**—The test is the real action of the disaster recovery test. Actual operational activities are executed to test the specific objectives of the plan. Applications are failing over; data entry and business processing should take place. Evaluators should review staff members as they perform the designated tasks. This is the actual test of preparedness to respond to an emergency.
- **Posttest**—The posttest is the cleanup of group activities. This phase comprises assignments, such as restoring the applications to the primary location and returning all resources to their proper place, disconnecting equipment, returning personnel to their normal locations and deleting all company data from third-party systems. The posttest cleanup also includes formally evaluating the plan and implementing indicated improvements. During every test phase, detailed documentation of observations, problems and resolutions should be maintained. Each team should have a diary with specific steps and information recorded. This documentation is important historical information to facilitate recovery during a real disaster. It also aids in performing a detailed analysis of the strengths and weaknesses of the plan.

Test Results

Metrics should be developed and used to measure the plan's success and test against the stated objectives. Results should be recorded and evaluated quantitatively, as opposed to basing evaluations on verbal descriptions alone. The resulting metrics should be used to measure the plan's effectiveness and, more importantly, improve it. Although specific measurements vary depending on the test and the organization, these metrics usually apply:

- **Time**—Elapsed time for completion of prescribed tasks. This is essential to refine the estimated response time for every escalation task. Was the RTO met?
- **Data**—Was all required data recovered? Was the RPO met? Was the recovery point aligned (where required) across all interconnected applications?
- **Amount**—Amount of work performed at the backup site by clerical personnel and the number of IS processing operations. Does the recovery site allow the required throughput?
- **Percentage and/or number**—The number of critical systems successfully recovered can be measured with the number of transactions processed.
- **Accuracy**—Accuracy of the data entry at the recovery site versus normal accuracy (as a percentage). The accuracy of actual processing cycles can be determined by comparing output results with those for the same period processed under normal conditions.

4.16.6 Invoking Disaster Recovery Plans

The BCP and DRP should be very closely aligned. As noted in section 4.15 Business Continuity Plan, a designated individual should be notified of all relevant incidents as soon as any triggering event occurs. This person should then follow a pre-established escalation protocol (e.g., calling in a spokesperson, alerting top management and involving regulatory agencies), which may be followed by invoking a recovery plan, such as the information technology DRP.

The required teams should be mobilized once the incident is evaluated to confirm which tested scenario it most closely resembles. Examples include:

- Loss of network connectivity
- Loss of a key IT system
- Loss of the processing site (server room)
- Loss of critical data
- Loss of an office
- Loss of key service provider (e.g., cloud)

There may be multiple ways to respond to a given incident. Possibilities should be evaluated with those most likely to deliver the required RPO and RTO. Documented recovery procedures should then be followed. Recovery procedures may not include all required recovery steps as testing may not have been comprehensive or the selected scenario may not exactly match the incident. Therefore, response teams may need to evaluate their options at each step. All decisions made should be documented and used to update the recovery procedures after normal service has been achieved.

Case Study

An IS auditor has been asked to represent the internal audit department of her organization on a task force to define the requirements for a new branch automation project for Pinkwater Bank, a community bank with 16 branches. This new system would handle deposits, loans and confidential customer information.

The branches are located within the same geographic area, so the director of branch operations has suggested using a microwave radio system to provide connectivity due to its low cost of operation and the fact that it is a private (not public) network. The director also has strongly suggested that it would be preferable to provide each branch with a backup connection to the Internet using a direct coaxial cable (from the local cable television provider) if the microwave system develops a fault.

The direct Internet connection would also be connected to a wireless access point at each branch to provide free wireless access to customers. The director also asked that each branch be provided with mail and application servers administered by each branch's administrative manager. The IS auditor was informed by the bank's IT manager that the cable service provider would encrypt all traffic sent over the direct coaxial connection to the Internet.

Following the preliminary work, Pinkwater Bank develops revised BCPs and DRPs for its headquarters facility and network of 16 branch offices. The current plans have not been updated in more than eight years, during which time the organization has grown by over 300 percent. At the headquarters facility, there are approximately 750 employees. These individuals connect over a LAN to an array of more than 60 application, database and file print servers in the corporate data center and over a frame relay network to the branch offices. Traveling users access corporate systems remotely by connecting over the Internet using a VPN. Users at headquarters and branch offices access the Internet through a firewall and proxy server in the data center.

Critical applications have an RTO of between three and five days. Branch offices are 30 to 50 miles from one another, with none closer than 25 miles to the headquarters facility. Each branch office has between 20 and 35 employees, plus a mail server and a file/print server. Backup media for the data center are stored at a third-party facility that is 35 miles away. Backups for servers located at the branch offices are stored at nearby branch offices using reciprocal agreements.

Current contracts with a third-party hot site provider include 25 servers, work area space equipped with desktop computers to accommodate 100 individuals, and a separate agreement to ship up to two servers and 10 desktop computers to any branch office that declares an emergency. The contract term is three years, with equipment upgrades occurring at renewal time. The hot site provider has multiple facilities throughout the country if the primary facility is used by another customer or rendered unavailable by the disaster. Senior management desires that any enhancements be as cost-effective as possible.

1. In reviewing the information for this project, what would be the **MOST** important concern regarding the use of microwave radio systems based on the above scenario?

   A. Susceptibility to interception of transmitted data
   B. Lack of available data transmission encryption solutions
   C. Likelihood of a service outage
   D. Cost overruns in implementation

2. Which of the following would **BEST** reduce the likelihood of business systems being successfully attacked from the public Internet through the wireless network?

   A. Scanning all connected devices for malware
   B. Segmenting internal network and public Internet access through a firewalled subnet
   C. Logging all access and issuing alerts for failed logon attempts
   D. Limiting all network access to regular business hours and standard protocols

3. When negotiating new contracts with the vendor, which of the following should the IS auditor recommend to management concerning the hot site in this situation?

   A. Desktops at the hot site should be increased to 750.
   B. An additional 35 servers should be added to the hot site contract.
   C. All backup media should be stored at the hot site to shorten the RTO.
   D. Desktop and server equipment requirements should be reviewed quarterly.

©ISACA. All Rights Reserved.

4. When negotiating new contracts with the vendor, which of the following should the IS auditor recommend to management concerning branch office recovery?

   A. Add each of the branches to the existing hot site contract.
   B. Ensure branches have sufficient capacity to back each other up.
   C. Relocate all branch mail and file/print servers to the data center.
   D. Add additional capacity to the hot site contract equal to the largest branch.

Answers on page 348

 ©ISACA. All Rights Reserved.

Page intentionally left blank

Chapter 4 Answer Key

Case Study

1. **A. Lack of encryption is the most important concern since microwave radio systems are easy to tap.**
   B. Lack of scalability is important but not as important as ensuring the confidentiality and integrity of customer data.
   C. The likelihood of a service outage is important but not as important as ensuring the confidentiality and integrity of customer data.
   D. Cost overruns in implementation are important but not as important as ensuring the confidentiality and integrity of customer data.

2. A. Scanning for malware would not detect the use of investigative tools designed to harvest passwords or reveal network vulnerabilities.
   B. Isolating the wireless network by placing it on a firewalled subnet would best reduce the likelihood of attack.
   C. Logging access would not prevent a successful attack.
   D. Limiting access to normal business hours would not prevent a successful attack.

3. A. Because not all employee job functions are critical during a disaster, it is not necessary to contract the same number of desktops at a recovery facility as the number of employees.
   B. Similarly, not every server is critical to the continued operation of the business. Only a subset will be required.
   C. Because there is no assurance that the hot site will not already be occupied, storing backup media at the facility would not be advisable. These facilities are generally not designed to provide extensive media storage, and frequent testing by other customers could compromise the security of the media.
   D. As equipment needs in a rapidly growing business are subject to frequent change, quarterly reviews are necessary to ensure that the recovery capability keeps pace with the organization.

4. A. Adding each branch to the hot site contract would be far more expensive.
   B. The most cost-effective solution is to recommend that branches have sufficient capacity to accommodate critical personnel from another branch. Because critical job functions would represent only perhaps 20 percent of the staff from the affected branch, accommodations for only four to seven critical staff members would be needed.
   C. Relocating branch servers to the data center could result in performance issues. It would not address the question of where to locate displaced employees.
   D. Adding capacity to the hot site contract would not provide coverage, as hot site contracts base their pricing on each location covered.

Chapter 5

Protection of Information Assets

Overview

Domain 5 Exam Content Outline 350
Learning Objectives/Task Statements 350
Suggested Resources for Further Study 350
Self-Assessment Questions 351
Chapter 5 Answer Key 354

Part A: Information Asset Security and Control

5.1 Information Asset Security Policies, Frameworks, Standards and Guidelines 357
5.2 Physical and Environmental Controls 365
5.3 Identity and Access Management 373
5.4 Network and Endpoint Security 409
5.5 Data Loss Prevention 434
5.6 Data Encryption 440
5.7 Public Key Infrastructure 454
5.8 Cloud and Virtualized Environments 459
5.9 Mobile, Wireless and Internet of Things Devices 475

Part B: Security Event Management

5.10 Security Awareness Training and Programs 493
5.11 Information System Attack Methods and Techniques 498
5.12 Security Testing Tools and Techniques 513
5.13 Security Monitoring Logs, Tools and Techniques 524
5.14 Security Incident Response Management 532
5.15 Evidence Collection and Forensics 537

Case Study

Case Study 545
Chapter 5 Answer Key 546

©ISACA. All Rights Reserved.

Overview

The purpose of this chapter is to discuss the techniques, challenges and best practices involved in the protection of information assets. Information should be protected at various points in its life cycle; notably, in process, in transit and at rest. Measures should be put in place to mitigate risk to information such as unauthorized access, use, disclosure, modification and destruction. Effective information protection requires a multidisciplinary approach involving people, processes and information technology and typically revolves around the objectives of confidentiality, integrity and availability (CIA).

This domain represents 26 percent of the CISA examination (approximately 39 questions).

Domain 5 Exam Content Outline

Part A: Information Asset Security and Control

1. Information Asset Security Policies, Frameworks, Standards and Guidelines
2. Physical and Environmental Controls
3. Identity and Access Management
4. Network and End-point Security
5. Data Loss Prevention
6. Data Encryption
7. Public Key Infrastructure
8. Cloud and Virtualized Environments
9. Mobile, Wireless and Internet-of-Things Devices

Part B: Security Event Management

1. Security Awareness Training and Programs
2. Information System Attack Methods and Techniques
3. Security Testing Tools and Techniques
4. Security Monitoring Logs, Tools and Techniques
5. Security Incident Response Management
6. Evidence Collection and Forensics

Learning Objectives/Task Statements

Within this domain, the IS auditor should be able to:

- Conduct audits in accordance with IS audit standards and a risk based IS audit strategy.
- Conduct post-audit follow up to evaluate whether identified risk has been sufficiently addressed.
- Utilize data analytics tools to enhance audit processes.
- Evaluate the role and/or impact of automatization and/or decision-making systems for an organization.
- Evaluate audit processes as part of quality assurance and improvement programs.
- Determine whether the organization has defined ownership of IT risk, controls and standards.
- Evaluate the organization's storage, backup and restoration policies and processes.
- Evaluate whether IT vendor selection and contract management processes meet business, legal and regulatory requirements.
- Evaluate supply chains for IT risk factors and integrity issues.
- Evaluate controls at all stages of the information systems development life cycle.
- Evaluate whether effective processes are in place to support end users.
- Evaluate the organization's data governance program.
- Evaluate the organization's privacy program.
- Evaluate data classification practices for alignment with the organization's data governance program, privacy program and applicable external requirements.
- Evaluate the organization's problem and incident management program.
- Evaluate the organization's log management program.
- Evaluate the organization's policies and practices related to asset life cycle management.
- Evaluate risk associated with shadow IT and end-user computing to determine effectiveness of compensating controls.
- Evaluate the organization's information security program.
- Evaluate the organization's threat and vulnerability management program.
- Utilize technical security testing to identify potential vulnerabilities.
- Evaluate logical, physical, and environmental controls to verify the confidentiality, integrity and availability of information assets.
- Evaluate the organization's security awareness training program.
- Evaluate potential opportunities and risk associated with emerging technologies, regulations and industry practices.

Suggested Resources for Further Study

Harper, A.; R. Linn; S. Sims; M. Baucom; D. Fernandez; H. Tejeda; M. Frost; *Gray Hat Hacking: The Ethical Hacker's Handbook, 6th Edition*, McGraw Hill, USA, 2022

ISACA, COBIT®, *https://www.isaca.org/resources/cobit*

 ©ISACA. All Rights Reserved.

ISACA, *Security Considerations for Cloud Computing*, USA, 2013, *https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko8hEAC*

International Organization for Standardization/ International Electrotechnical Commission, ISO/IEC 27001: 2022, *Information security, cybersecurity and privacy protection—Information security management systems —Requirements*, Switzerland, 2022, *https://www.iso.org/standard/27001*

International Organization for Standardization/ International Electrotechnical Commission, ISO/IEC 27002: 2022, *Information technology—Security techniques—Code of practice for information security controls*, Switzerland, 2022, *https://www.iso.org/standard/75652.html*

Kegerreis, M.; M. Schiller; C. Davis; *IT Auditing: Using Controls to Protect Information Assets, 3rd Edition*, McGraw Hill, USA, 2019

McClure, S.; J. Scambray; G. Kurtz; *Hacking Exposed 7: Network Security Secrets & Solutions*, McGraw Hill, USA, 2012

Peltier, T.; *Information Security Risk Analysis, 3rd Edition*, Auerbach Publications, USA, 2010

Stamp, M.; *Information Security: Principles and Practice, 2nd Edition*, John Wiley & Sons, USA, 2011

Self-Assessment Questions

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see section About This Manual for more guidance regarding practice questions.

1. An IS auditor reviewing the configuration of a signature-based intrusion detection system (IDS) would be **MOST** concerned if which of the following were discovered?

   A. Auto-update is turned off.
   B. Scanning for application vulnerabilities is disabled.
   C. Analysis of encrypted data packets is disabled.
   D. The IDS is placed between the demilitarized zone (DMZ) and the firewall.

2. Which of the following **BEST** provides access control to payroll data being processed on a local server?

   A. Logging access to personal information
   B. Using separate passwords for sensitive transactions
   C. Using software that restricts access rules to authorized staff
   D. Restricting system access to business hours

3. An information systems (IS) auditor has just completed a review of an organization that has a mainframe computer and two database servers where all production data reside. Which of the following weaknesses would be considered the **MOST** serious?

   A. The security officer also serves as the database administrator.
   B. Password controls are not administered over the two database servers.
   C. There is no business continuity plan (BCP) for the mainframe system's noncritical applications.
   D. Most local area networks (LANs) do not back up file-server-fixed disks regularly.

4. An organization is proposing to install single sign-on (SSO) to give access to all systems. The organization should be aware that:

   A. maximum unauthorized access would be possible if a password were disclosed.
   B. user access rights would be restricted by the additional security parameters.
   C. the security administrator's workload would increase.
   D. user access rights would be increased.

5. When reviewing an implementation of a Voice over Internet Protocol (VoIP) system on a corporate wide area network, an IS auditor should expect to find:

   A. traffic engineering.
   B. an integrated services digital network (ISDN) data link.
   C. wired equivalent privacy encryption of data.
   D. analog phone terminals.

©ISACA. All Rights Reserved.

6. An insurance company is using public cloud computing for one of its critical applications to reduce costs. Which of the following would be of **MOST** concern to the IS auditor?

   A. The inability to recover the service in a major technical failure scenario
   B. The data in the shared environment being accessed by other companies
   C. The service provider not including investigative support for incidents
   D. The long-term viability of the service if the provider should go out of business

7. Which of the following **BEST** determines whether complete encryption and authentication protocols for protecting information while being transmitted exist?

   A. A digital signature with Rivest-Shamir-Adleman (RSA) has been implemented.
   B. Work is being done in tunnel mode with the nested services of authentication header (AH) and encapsulating security payload (ESP).
   C. Digital certificates with RSA are being used.
   D. Work is being done in transport mode with the nested services of AH and ESP.

8. Which of the following concerns about the security of an electronic message would be addressed by digital signatures?

   A. Alteration
   B. Unauthorized reading
   C. Theft
   D. Unauthorized copying

9. Which of the following characterizes a distributed denial of service (DDoS) attack?

   A. Central initiation of intermediary computers to direct simultaneous spurious message traffic at a specified target site
   B. Local initiation of intermediary computers to direct simultaneous spurious message traffic at a specified target site
   C. Central initiation of a primary computer to direct simultaneous spurious message traffic at multiple target sites
   D. Local initiation of intermediary computers to direct staggered spurious message traffic at a specified target site

10. Which of the following is the **MOST** effective preventive antivirus control?

    A. Scanning email attachments on the mail server
    B. Restoring systems from clean copies
    C. Disabling universal serial bus (USB) ports
    D. An online antivirus scan with up-to-date virus definitions

Answers on page 354

Page intentionally left blank

©ISACA. All Rights Reserved.

Chapter 5 Answer Key

Self-Assessment Questions

1. **A. The most important aspect of a signature-based intrusion detection system (IDS) is its ability to protect against known (signature) intrusion patterns. Such signatures are provided by the vendor and are critical to protecting an enterprise from outside attacks.**
   B. One of the key disadvantages of an IDS is its inherent inability to scan for vulnerabilities at the application level.
   C. An IDS cannot break encrypted data packets to identify the source of the incoming traffic.
   D. A demilitarized zone (DMZ) is an internal network segment in which systems (e.g., a web server) accessible to the public are housed. In order to provide the greatest security and efficiency, an IDS should be placed behind the firewall so that it will detect only those attacks/intruders that enter the firewall.

2. A. Logging access to personal information is a good control in that it will allow access to be analyzed if there is concern over unauthorized access. However, it will not prevent access.
   B. Restricting access to sensitive transactions will restrict access only to some of the data. It will not prevent access to other data.
   C. The server and system security should be defined to allow only authorized staff members access to information about the staff whose records they handle on a day-to-day basis.
   D. Restricting system access to business hours would only affect when unauthorized access could occur and would not prevent such access at other times. It is important to consider that the data owner is responsible for determining who is allowed access via the written software access rules.

3. A. The security officer serving as the database administrator, while a control weakness, does not carry the same disastrous impact as the absence of password controls.
   B. The absence of password controls on the two database servers, where production data resides, is the most critical weakness.
   C. Having no business continuity plan (BCP) for the mainframe system's noncritical applications, while a control weakness, does not carry the same disastrous impact as the absence of password controls.
   D. Local area networks (LANs) not backing up regularly, while a control weakness, does not carry the same disastrous impact as the absence of password controls.

4. **A. If a password is disclosed when single sign-on (SSO) is enabled, there is a risk that unauthorized access to all systems will be possible.**
   B. User access rights should remain unchanged by SSO, as additional security parameters might not be implemented.
   C. One of the intended benefits of SSO is the simplification of security administration.
   D. One of the intended benefits of SSO is the unlikelihood of an increased workload.

5. **A. To ensure that quality of service (QoS) requirements is achieved, the Voice over Internet Protocol (VoIP) service over the wide area network should be protected from packet losses, latency or jitter. To reach this objective, network performance can be managed to provide QoS and class of service support using statistical techniques, such as traffic engineering.**
   B. The standard bandwidth of an integrated services digital network (ISDN) data link would not provide the QoS required for corporate VoIP services.
   C. Wired equivalent privacy is an encryption scheme related to wireless networking.
   D. VoIP phones are usually connected to a corporate local area network (LAN) and are not analog.

6. A. Benefits of cloud computing are redundancy and the ability to access systems and data in the event of a technical failure.
   B. Considering that an insurance company must preserve the privacy/confidentiality of customer information, unauthorized access to information and data leakage are the major concerns.
   C. The ability to investigate an incident is important, but most important is addressing the risk of an incident: the exposure of sensitive data.
   D. If a cloud provider goes out of business, the data should still be available from backups.

 ©ISACA. All Rights Reserved.

7. A. A digital signature provides authentication and integrity.
   B. Tunnel mode provides encryption and authentication of the complete (Internet Protocol) IP package. To accomplish this, the authentication header (AH) and encapsulating security payload (ESP) services can be nested.
   C. A digital certificate provides authentication and integrity.
   D. The transport mode provides primary protection for the protocols' higher layers (i.e., protection extends to the data field [payload] of an IP package).

8. **A. A digital signature includes an encrypted hash total of the size of the message as it was transmitted by its originator. This hash would no longer be accurate if the message were subsequently altered, indicating that the alteration had occurred.**
   B. Digital signatures will not identify, prevent or deter unauthorized reading.
   C. Digital signatures will not identify, prevent or deter theft.
   D. Digital signatures will not identify, prevent or deter unauthorized copying.

9. **A. This best describes a distributed denial of service (DDoS) attack. Such attacks are centrally initiated and involve the use of multiple compromised computers. The attacks work by flooding the target site with spurious data, thereby overwhelming the network and other related resources. To achieve this objective, the attacks need to be directed at a specific target and occur simultaneously.**
   B. DDoS attacks are not locally initiated.
   C. DDoS attacks are not initiated using a primary computer.
   D. DDoS attacks are not staggered.

10. A. Scanning email attachments on the mail server is a preventive control. It will prevent infected email files from being opened by the recipients, which would cause their machines to become infected.
    B. Restoring systems from clean copies is a preventive control. It will ensure that viruses are not introduced from infected copies or backups, which would reinfect machines.
    C. Disabling universal serial bus (USB) ports is a preventive control. It prevents infected files from being copied from a USB drive onto a machine, which would cause the machine to become infected.
    D. Antivirus software can be used to prevent virus attacks. Running regular scans can is useful to detect virus infections that have already occurred. Regular updates of the software are required to ensure it can update, detect and treat viruses as they emerge.

©ISACA. All Rights Reserved.

Page intentionally left blank

 ©ISACA. All Rights Reserved.

Part A: Information Asset Security and Control

Protection of information assets includes the key components that ensure CIA of information assets. Many of the topics covered in this chapter may, on the surface, seem very familiar to candidates; however, it is important to note that these topics require a thorough knowledge of the technologies used and the control weaknesses that can be exploited by attackers. CISA candidates should understand the components of physical infrastructure security, logical access issues and the key elements of information security management.

Information security is an essential component of governance and management that affects all aspects of entity-level controls. Information systems (IS) auditors include appropriate information security evaluations throughout their audit work. The information security management function is responsible for the governance, policy, enforcement, monitoring and innovation necessary for businesses to establish cost-effective information security processes, while providing adequate information security assurance within the risk appetite and budget of the organization.

5.1 Information Asset Security Policies, Frameworks, Standards and Guidelines

Information security policies, frameworks, standards and guidelines are helpful to organizations because they can help provide guidance on how information assets are protected and used.

5.1.1 Information Asset Security Policies, Procedures and Guidelines

Policies and procedures provide the basis for maintaining proper operation and control. The IS auditor should review the policies and procedures to determine if they set the tone for proper security and provide a means for assigning responsibility for maintaining a secure IS environment. The policy review should include reviewing the date of the last update to ensure that documents remain current and meet organizational information security needs. An information security policy is a set of rules, directives and practices designed to ensure the protection of information assets. It is a general statement crafted by the organization's senior management and board clearly stipulating the role of information security in the organization.

Key elements of an information security policy include:

- **Scope**—The scope of an information security policy is crafted at a high level and specifies where information is located and who can access it. It should also emphasize where, how and when information can be stored in programs, systems, facilities or other infrastructure.
- **Policy statement**—The policy statement explains the organization's approach to information security. It establishes the environment in which the organization operates, specifies the laws and regulations to be adhered to and describes the types of information the organization should handle.
- **Objectives**—To determine whether any information security program works as intended and in an effective manner, a set of objectives is required. The objectives should be specific, measurable, achievable, realistic and time-bound (SMART). Some of the objectives of an information security policy are:
  - **Confidentiality**—Confidentiality involves keeping information private by protecting it from unauthorized personnel. It ensures that information is available only to authorized individuals.
  - **Integrity**—Integrity entails ensuring that information is reliable, accurate and trustworthy, typically achieved through safeguarding information from being altered or modified without consent.
  - **Availability**—Availability involves ensuring that authorized people in the organization have access to confidential documents required for the achievement of their day-to-day tasks. Routine maintenance to ensure that systems are always up and running is one way to ensure availability.
  - **Information security guidance**—Information security guidance provides a general, organization-wide approach to information security.
  - **Monitoring**—The information security policy seeks to provide documentation of measures in place for the protection of information assets. This objective assists in monitoring to ensure that the organization achieves value from the efficient and effective operation of its information systems.
  - **Governance**—This objective highlights the organization's dedication to embedding strong governance principles. It entails the commitment to structured decision-making, clearly defined roles and responsibilities, and the cultivation of a culture that prioritizes continuous enhancement of information security practices.
  - **Compliance**—In pursuing compliance, the organization typically develops its information

©ISACA. All Rights Reserved.

systems in alignment with application compliance requirements.
  - **Privacy**—An information security policy should provide guidance on ensuring the privacy of customer information and other critical information.

Characteristics of an Information Security Policy

Certain elements are necessary for enabling the establishment and maintenance of an information security policy in the organization. IS auditors should ensure that these elements are in place and provide advice throughout the process:

- **Executive support**—The information security policy should receive buy-in from management. This calls for information security specialists to explain the value of information security to the organization's management. With an understanding of the value of information security, management should be able to support information security initiatives in terms of budget and resources requirements.
- **Business-driven**—The purpose of information security in an organization is to support and extend business objectives, and the policy should be driven by business objectives. IS auditors should evaluate regularly whether the policy is aligned with the business objectives.
- **Simple**—One of the important characteristics of an information security policy is simplicity and user-friendliness. The policy should be a simple document, easy to understand and capable of being used as a reference point by every member of the organization.
- **Integrated**—The information security policy should be an integrated document that addresses the security of all business functions and processes. It should contain issue-specific policies covering various activities, systems or sections in the organization.
- **Accessible**—Accessibility is a critical requirement for the information security policy. It ideally should be accessible to everyone in the organization. A good example of exhibiting accessibility is to post the policy onto the organization's intranet.
- **Strategic**—The information security policy should be strategic in nature, long term in focus and crafted with the intention of being used for several years. It should be part of the organization's strategic objectives to enhance the level of information security.
- **Professional**—Policies should be presented with a high level of professionalism while reinforcing the importance of adherence.
- **Penalties**—An information security policy should contain penalties for noncompliance. The imposition of penalties should be implemented to cultivate a culture of security compliance among all members of the organization.
- **Flexible**—The information security policy should be flexible enough to adapt to changes in the organization's operating environment. It should provide a framework that allows for modifications in line with organizational growth and new security challenges.
- **Regularly updated**—The information security policy should be regularly updated in line with developments in the industry and business operating environments. Policy revisions should be documented, including the last day of modification and the department responsible for the modification.

Some common types of information security policies include:

- **Organizational information security policy**—This policy is the primary blueprint covering the security aspects of the entire organization. It is generic in nature and also known as the master information security policy.
- **System-specific information security policy (SysSP)**—The SysSP is derived from the organizational information security policy that addresses the security aspects of a single system, application or network. It is often enforced through access controls. An example of a system specific policy is a policy addressing the payroll system security.
- **Issue-specific information security policy (ISSP)**—The ISSP builds upon the more generic master information security policy and is typically developed to outline the guidelines for addressing specific threats in an organization.

Figure 5.1 shows typical examples of issue-specific policies.

 ©ISACA. All Rights Reserved.

Figure 5.1—Issue-Specific Information Security Policies

Policy	Policy Description
Acceptable use policy	Outlines the constraints an employee must accept to use an organizational system and/or network
Change control policy	Refers to guidelines for the formal process for making changes to IT, software development and information security processes
Access control policy	Outlines access controls to an organization's data and information systems (IS) and the steps users need to follow to gain access
Incident response policy	Provides an organized approach to how the organization manages, remediates and recovers from information security incidents
Identity and access management (IAM) policy	Typically deals with the authorization of systems and applications to the right employees and how employees, contractors and third parties are authenticated by systems to comply with security standards
Remote access policy	Outlines acceptable methods of remotely and securely connecting to internal organizational networks
Bring your own device (BYOD) policy	Outlines the requirements that employees be allowed to use personal devices to access organizational infrastructure and the steps required to reduce the risk of exposure from employee-owned assets.

Information Security Procedures

Procedures are the step-by-step tasks that should be performed to achieve a certain objective. They typically apply to users, IT staff, operations staff, security members and anyone in the organization who needs to carry out specific tasks. Procedures address aspects like how to install operating systems (OSs), configure security mechanisms, set up new user accounts, assign computer privileges, audit activities, destroy data and report incidents. Procedures are considered the lowest level in the documentation chain as they are closest to the information systems and their users. They should be detailed to support understanding among a wide range of employees.

Information Security Guidelines

A guideline is a description of a particular way of accomplishing something that is less prescriptive than a procedure. Guidelines serve as recommendations to users when specific standards do not apply and assist in the implementation of the standards. They are designed to streamline certain processes according to best practices. Guidelines, by nature, should be general and open to interpretation. They do not need to be strictly followed and allow users leeway in their interpretation.

5.1.2 Information Security Frameworks and Standards

An information security standard is a set of mandatory activities, actions or rules crafted to support policies and their reinforcement. Typical organizational security standards may specify expected user behavior to ensure that specific technologies, applications, parameters and procedures in an organization are implemented uniformly across the organization. In contrast, policies only define the need to use an approved encryption process when sending sensitive information. Some of the advantages of information security standards are:

- They provide a repeatable way of maintaining security, thus helping to achieve consistency in information security management.
- They are typically based on compliance and best practices that enable organizations to make objective decisions concerning the implementation of security practices.
- They facilitate sharing of knowledge and best practices, leading to a common understanding of concepts, terms and definitions regarding information security in an organization.
- They help ensure that products and installations are consistent with the needs of the organization.
- They assist in ensuring information security product functionality and compatibility.

An information security framework refers to a set of processes that define the policies and procedures

©ISACA. All Rights Reserved.

necessary for the successful implementation and ongoing management of an information security program in an organization. It assists in managing risk and reducing vulnerabilities. Recognized frameworks are used to define and prioritize security tasks and manage risk in implementing information security controls. They are often used as a basis for establishing internal policies, procedures and guidelines regarding information security management in an organization. IS auditors should understand the provisions of information security frameworks as applied in the organization.

Information security frameworks vary in terms of their complexity and scale. Organizations should customize applicable frameworks to solve specific information security problems, such as industry-specific requirements or different regulatory compliance goals. Additionally, information security frameworks often overlap for thorough mapping to reduce duplication of effort while addressing gaps. The chosen information security framework should effectively support the organization's operational, compliance and audit requirements. The choice to use a particular information security framework depends on several factors, such as location, type of industry and expected compliance requirements.

An information security standard is a set of guidelines or best practices that organizations can use to improve their information security posture. Standards also assist the organization in the identification and implementation of appropriate information security measures.

Figure 5.2 details some of the common and frequently used information security frameworks and standards.

Figure 5.2—Information Security Frameworks and Standards

Framework	Description
International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27001	ISO/IEC 27001 is an international standard on information security which specifies procedures for the development and maintenance of an information security management system in an organization. ISO/IEC 27001 provides best practices that can be adopted in information security management. It addresses organizational, people, physical and technological controls holistically.
Zachman Framework	The Zachman Framework is a model for classifying and developing enterprise architectures. Developed by John Zachman, it can be used to proactively model organizational functions, processes and elements. It is typically employed in the management of organizational change.
The Open Group Architecture Framework (TOGAF)	TOGAF is an enterprise architecture framework that is used to define business objectives and align them with architecture objectives. It ensures the adoption and application of consistent standards and methodologies by enterprise architecture professionals.
Sherwood Applied Business Security Architecture (SABSA)	SABSA is a model and methodology for the development of risk-driven and opportunity-focused information security enterprise architectures and service management to support critical business functions and processes. It consists of a life cycle starting with strategy planning, design, implementation and managing and measuring components.
COBIT	COBIT is an IT governance framework specifying the best approaches and procedures in the governance of enterprise IT to help organizations to minimize their IT risk while ensuring efficiency in the use of available resources.
NIST Cybersecurity Framework (CSF)	The NIST CSF consists of standards, guidelines and best practices that assist organizations in improving their management of cybersecurity risk. The framework is designed to be flexible and can be integrated with the existing security processes and procedures in an organization. It can be used in any industry or sector.
Information Technology Infrastructure Library (ITIL)	ITIL is a framework that promotes the standardization of IT service management in an organization. It seeks to standardize the processes of selecting, planning, delivering and maintaining the overall IT life cycle within the organization. Such standardization is expected to improve efficiency and IT service delivery.

 ©ISACA. All Rights Reserved.

Figure 5.2—Information Security Frameworks and Standards (cont.)

Framework	Description
The Center for Internet Security (CIS) Critical Security Controls (CSC)	The CIS CSC provides technical security and operational controls that can be applied to any environment. It does not address risk management and focuses solely on reducing risk and increasing resilience for technical infrastructures. Controls include inventory, data protection, log management, malware and penetration testing. CIS controls link with existing risk management frameworks to help remediate identified risk and are critical especially for organizations lacking technical information security information
Payment Card Industry Data Security Standard (PCI DSS)	The PCI DSS standard was developed by major credit card companies for enhancing payment account data security. PCI DSS requirements apply to organizations with environments where cardholder data and/or sensitive authentication data are stored, processed or transmitted, as well as organizations with environments that can impact the security of the cardholder data environment. The standard's requirements extend to organizations that outsource their payment environments or payment operations to third parties.
Security, Trust, Assurance and Risk (STAR)	The STAR program was developed by the Cloud Security Alliance (CSA) as an assurance framework for cloud service providers (CSPs). It combines principles of transparency, rigorous auditing processes and harmonization of standards that reference cloud security. STAR provides organizations with cloud-specific structures for implementation of their information security programs. It consists of voluntary self-assessments, attestations and certifications that allow CSPs to validate their cloud security postures and demonstrate commitment to best practices.
Cloud Control Matrix (CCM)	The CCM was developed by the CSA and is composed of 197 control objectives in 17 domains, covering all key aspects of cloud technology. It is widely used for the systematic assessment of cloud implementation and provides guidance to both consumers and CSPs on which security controls should be implemented in the cloud supply chain. It is generally considered a de facto standard for cloud security assurance and compliance and has been mapped to other industry-accepted security standards, such as the ISO 27001/27002, PCI DSS and NIST CSF. Thus, it provides a way to align security practices with those that already exist in other domains.

The IS auditor should review the use of frameworks in the organization, assess their relevance and determine whether they are achieving their intended purpose. Some of the reasons to use a framework include:

- **Improved information security management**—Frameworks encourage organizations to actively implement the information security measures, processes and controls necessary to continuously improve their information security posture.
- **Effective risk management**—Adherence to information security frameworks reduces the risk of the organization getting breached. Frameworks instill a culture of risk management in the organization.
- **Effective and efficient incident response**—Frameworks ensure the organization has an effective incident response in case of breach.
- **Increased market reach**—Organizations that achieve certification or align with recognized frameworks often achieve new business opportunities and increased competitiveness in the market and are eligible for certain contracts that require those frameworks to be met.
- **Increased security reliability**—Frameworks allow organizations to better understand their security needs and use the correct solutions to protect against identified risk. Using a framework-based approach ensures that adequate controls, processes and procedures are in place, improving the reliability and security of information systems.

Auditing the information security framework of an organization involves the audit of logical access, the use of techniques for testing security and the use of investigation techniques. The information security management framework should be reviewed per the basic elements in an information security framework. Additional areas of concern are risk management, risk assessment results, control design and incident management.

©ISACA. All Rights Reserved.

5.1.3 Information Security Baselines

An information security baseline refers to the specific products, configurations and similar mechanisms that are generally mapped to industry standards and are used to secure information systems. A baseline is a minimum level of security that a system, network or device must adhere to. For example, an organization might specify that all computer systems comply with a minimum trusted computer system evaluation criteria command and control (C2) standard. The baseline plan should be followed with a full security evaluation and plan. **Figure 5.3** illustrates baseline security topics and their associated recommendations.

Figure 5.3—IT Security Baseline Recommendations

Topics	Objective	Recommendations
Environment/ inventory	Establish and maintain an inventory.	Users are expected to follow standards for managing computers connected to the network and to have registered network addresses. The operating system (OS) and owner should be included along with the data provided.
Malware	Install antivirus software with automatic updating.	Antivirus software with an automatic DAT file should be updated at regular intervals, no less than weekly.
Passwords	Recognize the importance of passwords.	Users must use only strong passwords. The IT department should provide password guidance. Departmental accounts are created for workgroups to prevent/avoid password sharing.
Patching	Make it automatic; the less work necessary, the less chance for compromise.	Each machine should be configured for automatic OS and basic software patching. A process should be established that works for the department and minimizes disruptions at inconvenient times. Workstations should be more automated to give system administrators the time to attend to servers as required to minimize the impact on services offered.
Minimizing services offered by systems	Eliminate unnecessary services to reduce security risk and save time in the long run.	To improve basic security and minimize effort to maintain systems, workstations should offer only needed services. Many OSs are installed with services turned on. Removing services reduces a workstation's chances of being compromised and minimizes security risk.
Addressing vulnerabilities	Eliminate many vulnerabilities with good system administration, such as removal of default accounts and deletion of unused accounts to reduce the attack surface.	System compromises can be time-consuming and damage the business's credibility and integrity. Information from organizationwide scans helps to identify vulnerabilities in each system and provides a baseline for comparison when system integrity is in question.
Backups	Allow easy recovery from user mistakes and hardware failure.	Backups should be made offsite for increased security.

Figure 5.4 shows a checklist for a baseline security evaluation.

 ©ISACA. All Rights Reserved.

Figure 5.4—Baseline Security Evaluation Checklist

Topics	Evaluation Questions
Environment/inventory	• What types of data are maintained by the enterprise (e.g., financial, statistical, graphical)? • In what form are they maintained (e.g., spreadsheets, databases)? • Is any critical or confidential information maintained or handled? If so, how is it protected? • Are there any specific requirements for handling data (legal or regulatory requirements)? • Do any machines store or require access to confidential information? • What types of operating systems (OSs) exist? • How many subnets exist? • How many workstations/servers exist? • In how many locations does IT infrastructure exist? • Has wireless infrastructure been deployed? How is it secured? • Are staff instructed on how to lock workstations when they step away? • Are users aware that unexpected email attachments should not be opened? • Are staff aware that many compromises are due to social engineering and the sharing of information? • Does the enterprise have a network diagram that includes IP addresses, room numbers and responsible parties? • Has the enterprise limited and secured physical and remote access to network services? • Is corporate hardware upgraded at regular intervals? • Does the enterprise have a current documented inventory of hardware and software? • Is all corporate software licensed? • Is license documentation available (licenses, purchase orders) if a software audit is required?
Malware protection	• Does the enterprise have an antimalware policy? • Are all workstations running the latest version of antivirus software, scanning engine and virus signature file? • Are DAT files downloaded automatically or manually? If manually, how often and why? • Do staff know who to contact when a virus is found? • Does the antivirus system have a way to defend against zero-day attacks?
Passwords	• Is there a corporate policy requiring strong passwords? • Is the enterprise using software that enforces strong passwords? • Is password caching disabled on all workstations? • Are passwords changed? If so, how often? • Are employees aware that passwords and accounts are not to be shared? • Does the system administrator have written authorization to check for weak passwords? • Is multifactor authentication (MFA) enabled for all users of cloud-based systems?

©ISACA. All Rights Reserved.

Figure 5.4—Baseline Security Evaluation Checklist (cont.)

Topics	Evaluation Questions
Patching	• Are software patches applied to all OSs automatically when possible? If done manually, how often? • Are patches applied to web browsers and applications? If yes, how frequently? • Is each machine backed up before applying a patch? • Are patches tested prior to applying? • Does the department have a documented process for patching? • Are there sufficient sources and subscriptions to be aware of patches to all relevant hardware and software?
Minimizing services offered by systems	• Are services that depend on one another to accomplish job assignments identified? • Have unnecessary services that were installed by default been removed? • Do technical staff review security settings and policies? • Have services offered been identified? • Are security measures for remote access in place? • Does the organization use secure services?
Addressing vulnerabilities/auditing	• Have vulnerabilities discovered by enterprise-wide scans been resolved? • Who is the contact for vulnerability scans? • Do IT staff complete an independent vulnerability scan for the enterprise? • Has the enterprise deployed any form of firewalls or either host or network-based intrusion detection systems (IDSs)? Are any under consideration?
Backup and recovery/business continuity	• Are files regularly backed up? • Are files kept onsite in a secure location? • Are backup files sent offsite to a physically secure location? • Are backup files periodically restored as a test to verify whether they are a viable alternative? • Is it possible to ensure that any forms of media containing confidential and sensitive information are sanitized before disposal? • Is there redundant hardware to allow work to continue in the event of a single hardware failure? • Can the enterprise continue to function if central services are not available? • Can the enterprise continue to function in the event of a wide area network failure? • Have responses been made to abuse issues/incidents? Has recovery been achieved? • Are immutable backups and use of a broker service implemented?

 ©ISACA. All Rights Reserved.

Figure 5.4—Baseline Security Evaluation Checklist (cont.)

Topics	Evaluation Questions
IT staff	• How many IT staff are employed full-time/part-time? • Does each IT staff member have a current job description? • Do job descriptions and evaluations include IT security duties? • Does the department have sufficient documentation to ease the transition of incoming/outgoing staff? • Does the enterprise have a privacy policy? • Are all staff aware of privacy considerations? • Are management/department users aware of the types of (private/nonpublic) information available to system administrators? • Does the enterprise have a privacy policy to address privileged information (confidentiality agreement/nondisclosure agreement)? • Does the enterprise have a firewall, IDS or other software for network diagnosis? • Does the enterprise have tools requiring privileges and access to confidential information acquired via routers, switches, IDSs, firewalls, etc.?

Access Standards

Access standards should be reviewed by the IS auditor to ensure they meet organizational objectives for separating duties, preventing fraud or error, and meeting policy requirements for minimizing the risk of unauthorized access.

Standards for security may be defined:

- At a generic level (e.g., all passwords must be at least eight characters long)
- For specific machines (e.g., all Unix machines can be configured to enforce password changes)
- For specific application systems (e.g., sales ledger clerks can access menus that allow entry of sales invoices but may not access menus that allow check authorization)

5.2 Physical and Environmental Controls

Security of information assets requires physical and environmental security. The IS auditor needs to evaluate applicable controls. In many organizations, physical and environmental controls are designed and implemented by facility management and not by the information security manager or IT. Most IT assets require environmental controls for things like temperature, humidity and power. The IS auditor needs to assess these controls to provide assurance.

5.2.1 Environmental Exposures and Controls

IT infrastructure and information assets are exposed to the environment. The IS auditor should be aware of environmental exposures and the controls used to mitigate them.

Equipment Issues and Exposures Related to the Environment

Environmental exposures are due primarily to naturally occurring events, such as lightning storms, earthquakes, volcanic eruptions, hurricanes, tornados and other types of extreme weather conditions. Such conditions can result in many types of problems. One area of concern is power failures. Generally, power failures can be grouped into four distinct categories, based on the duration and relative severity of the failure:

- **Total failure (blackout)**—A complete loss of electrical power may span from a single building to an entire geographical area and is often caused by weather conditions (e.g., storm, earthquake) or the inability of an electrical utility company to meet user demands (e.g., during summer months).
- **Severely reduced voltage (brownout)**—The failure of an electrical utility company to supply power within an acceptable range (i.e., 108–125 volts alternating current [AC] in the United States). Such failure places a strain on electronic equipment and may limit its operational life or even cause permanent damage.
- **Sags, spikes and surges**—Temporary and rapid decreases (sags) or increases (spikes and surges) in

©ISACA. All Rights Reserved.

voltage levels. These anomalies can cause loss of data, data corruption, network transmission errors or physical damage to hardware devices (e.g., hard disks or memory chips).
- **Electromagnetic interference (EMI)**—Caused by electrical storms or noisy electrical equipment (e.g., motors, fluorescent lighting, radio transmitters). This interference may cause computer systems to hang or crash and may result in damages similar to those caused by sags, spikes and surges.

Short-term interruptions, which last from a few millionths to a few thousandths of a second, can be prevented by using properly placed surge protectors. Intermediate-term interruptions, which last from a few seconds to 30 minutes, can be controlled by uninterruptible power supply (UPS) devices. Finally, long-term interruptions, which last from a few hours to several days, require the use of alternative power generators. These generators may be portable devices or part of the building's infrastructure and are powered by alternative sources of energy such as diesel, gasoline or propane.

Another area of concern deals with water damage/flooding. This is a concern even with facilities located on upper floors of high-rise buildings because water damage often occurs from broken water pipes. Other causes include terrorist threats/attacks, vandalism, electrical shock and equipment failure.

Some questions that organizations must address related to environmental issues and exposures include:
- Is the power supply to the computer equipment properly controlled to ensure that power remains within the manufacturer's specifications?
- Are the air conditioning, humidity and ventilation control systems for the computer equipment adequate to maintain temperatures within manufacturers' specifications?
- Is the computer equipment protected from the effects of static electricity by an antistatic rug or antistatic spray?
- Is the computer equipment kept free of dust, smoke and other particulate matter, such as food?
- Are there policies that prohibit the consumption of food, beverage and tobacco products near computer equipment?
- Are backup media protected from damage from temperature extremes, the effects of magnetic fields and water?
- Is the computer equipment stored in a safe place to prevent theft?
- Is there a periodic maintenance schedule for computer equipment and is it adhered to?
- Are computer hardware failures promptly addressed?

Controls for Environmental Exposures

Environmental exposures should be afforded the same level of protection as physical and logical exposures. When auditing on behalf of an organization that uses a co-located or outsourced datacenter (including cloud environments), the IS auditor should evaluate the adequacy of all potential exposures related to the hosted environment.

Alarm Control Panels

An alarm control panel should ideally be:
- Separated from burglar or security systems located on the premises
- Accessible to fire department personnel at all times
- Located in a weatherproof box
- Use temperature requirements set by the manufacturer
- Situated in a controlled room to prevent access by unauthorized personnel
- Allocated power from a dedicated and separate circuit
- Able to control or disable separate zones within the facilities
- Compliant with local and national regulations and approved by local authorities

Water and Smoke Detectors

In the computer room, water detectors should be placed under raised floors and near drain holes, even if the computer room is on a high floor (because of possible water leaks). Any unattended equipment storage facilities should have water detectors. When activated, the detectors should produce an audible alarm that can be heard by security and control personnel. The location of the water detectors should be marked on the raised computer room floor for easy identification and access. On hearing the alarm, specific individuals should be responsible for investigating the cause and initiating remedial action; other staff should be made aware by security and control personnel that there is a risk of electric shock.

Smoke detectors should be installed above and below the ceiling tiles throughout the facilities and below the raised computer room floor. The detectors should produce an audible alarm when activated and be linked to a monitored station (preferably by the fire department). The location of the smoke detectors above the ceiling tiles and below the raised floor should be marked on the

tiles for easy identification and access. Smoke detectors should supplement, not replace, fire suppression systems.

Visual verification of the presence of water and smoke detectors in the computer room is needed. Whether the power supply to the detectors is sufficient should be determined, especially in instances of battery-operated devices. Also, the locations of the devices should be placed to give early warning of a fire, such as immediately above the computer equipment they are protecting, and should be clearly marked and visible.

Handheld Fire Extinguishers

Fire extinguishers should be in strategic locations throughout the facility. They should be tagged for inspection and inspected at least annually.

Manual Fire Alarms

Manual fire alarms should be placed strategically throughout the facility. They are normally located near exit doors to ensure personnel safety. The resulting audible alarm should be linked to a monitored guard station.

Fire Suppression Systems

Fire suppression systems are designed to automatically activate immediately after detection of high heat, typically generated by fire. Like smoke detectors, they should produce an audible alarm when activated and be linked to a central guard station that is regularly monitored. Fire suppression systems should be inspected and tested annually. Testing intervals should comply with industry and insurance standards and guidelines. Ideally, systems should automatically trigger other mechanisms to localize a fire. This includes closing fire doors, notifying the fire department, closing off ventilation ducts and shutting down nonessential electrical equipment. In addition, systems should be segmented so a fire in one part of a large facility does not activate the entire system.

There are two methods for applying an extinguishing agent, total flooding and local application:

- Systems working under a total flooding principle apply an extinguishing agent to a three-dimensional enclosed space to achieve a concentration of the agent (volume percent of the agent in air) adequate to extinguish the fire. These types of systems may be operated automatically by detection and related controls or manually by the operation of a system actuator.
- Systems working under a local application principle apply an extinguishing agent directly onto a fire (usually a two-dimensional area), or into the three-dimensional region immediately surrounding the substance or object on fire. The main difference between local application and total flooding designs is the absence of physical barriers enclosing the fire space in the local application design. In the context of automatic extinguishing systems, local application does not normally refer to the use of manually operated wheeled or portable fire extinguishers, although the nature of the agent delivery is similar.

Typical fire suppression systems include but are not limited to:

- **Water-based systems (sprinkler systems)**—Water is always present in the system piping, which can potentially leak, causing damage to equipment.
- **Dry-pipe sprinkling systems**—Water does not flow until the fire alarm activates a pump.
- **FM-200, also called heptafluoropropane, HFC-227 or HFC-227ea**—This is often considered the preferred option for fire suppression.
- **Novec 1230, also called perfluoro(2-methyl-3-pentanone)**—This is mostly used as an FM 200 alternative. It is one of the cleanest fire suppression agents and works similar to FM-200.

Because fire suppression systems are expensive to test, IS auditors may need to limit their tests to reviewing documentation to ensure that the system has been inspected and tested within the last year. The exact testing interval should comply with industry and insurance standards and guidelines.

Strategically Locating the Computer Room

To reduce the risk of flooding, the computer room should not be located in the basement or on the top floor. Studies show that in a multistory building the best location for the computer room is on a middle floor (e.g., third, fourth, fifth or sixth floor). Adjacent water or gas pipes should be avoided except in the case of fire suppression systems. Care should be taken to avoid locating computer rooms adjacent to areas used for functions carrying a high risk, such as paper storage. The activity of neighboring organizations should be considered when establishing a computer facility. Locations adjacent to an airport or a chemical plant where explosive gases may be present, for example, should be avoided.

If a data center is already located in an area vulnerable to flooding, such as a basement, an alternative to costly removal is the provision of a plastic sheet or umbrella to

©ISACA. All Rights Reserved.

cover the area and divert any water flow away from the sensitive equipment.

Regular Inspection by Fire Department

To ensure that all fire detection systems comply with building codes, there should be a fire department inspection of the system and facilities annually. Also, the fire department should be notified of the location of the computer room, so it can be prepared with equipment appropriate for electrical fires.

The IS auditor should contact the person responsible for fire equipment maintenance and ask if a local fire department inspector or insurance evaluator has recently been invited to tour and inspect the facilities. If so, a copy of the report should be obtained, and how to address the noted deficiencies should be determined.

Fireproof Walls, Floors and Ceilings of the Computer Room

Walls surrounding the information processing facility (IPF) should contain or block a fire from spreading. The surrounding walls should be from the true floor to the true ceiling and should have at least a two-hour fire resistance rating.

With the assistance of building management, the documentation that identifies the fire rating of the walls surrounding the IPF should be located. The walls should have at least a two-hour fire resistance rating.

Electrical Surge Protectors

Electrical surge protectors reduce the risk of equipment damage due to power spikes. Voltage regulators measure the incoming electrical current and either increase or decrease the charge to ensure a consistent current. Such protectors are typically built into the UPS system.

Uninterruptible Power Supply/Generator

A UPS system consists of a battery or gasoline-powered generator that interfaces with the electrical power entering the facility and the electrical power entering the computer. The system typically cleanses the power to ensure that voltage into the computer is consistent. The UPS continues providing electrical power from the generator to the computer for a defined length of time should a power failure occur. Depending on the sophistication of the UPS, electrical power could continue to flow for days or for just a few minutes to permit an orderly computer shutdown. A UPS system can be built into a computer or can be an external piece of equipment. The most recent test date should be determined, and the test reports should be reviewed.

Emergency Power-Off Switch

There may be a need to immediately shut off power to the computer and peripheral devices, such as during a computer room fire or emergency evacuation. Two emergency power-off switches should serve this purpose —one in the computer room and the other near, but outside, the computer room.

Emergency power-off switches should be clearly labeled and easily accessible, yet they should still be secure from unauthorized people. The switches should be shielded to prevent accidental activation. Furthermore, an IS auditor should assess the need to have them under video surveillance, as a dissuasive control against malicious insiders and a source of information for incident handling.

The presence of electrical surge protectors on sensitive and expensive computer equipment should be visually observed.

Power Leads From Two Substations

Electrical power lines that feed into the facility are exposed to many environmental hazards—water, fire, lightning, cutting due to careless digging, etc. Reducing the risk of a power failure due to this type of exposure is, for the most part, beyond the control of the organization. Redundant power lines should feed into the facility so that the interruption of one power line does not adversely affect the electrical supply. With the assistance of building management, documentation of the use and placement of redundant power lines into the IPF should be located.

Wiring Placed in Electrical Panels and Conduit

To reduce the risk of an electrical fire occurring and spreading, wiring should be placed in fire-resistant panels and conduit, which generally lies under the fire-resistant raised computer room floor.

Inhibited Activities Within the Information Processing Facility

Food, drink and tobacco use can cause fires, the build-up of contaminants or damage to sensitive equipment (especially in the case of liquids). They should be prohibited from the IPF. This prohibition should be overt, such as with a sign on the entrance.

 ©ISACA. All Rights Reserved.

Fire-Resistant Office Materials

Wastebaskets, curtains, desks, cabinets and other general office materials in the IPF should be fire-resistant. Cleaning fluids for desktops, console screens and other office furniture/fixtures should not be flammable.

Documented and Tested Emergency Evacuation Plans

Evacuation plans should emphasize human safety but should not leave IPFs physically unsecured. Procedures should be in place for a controlled shutdown of the computer in an emergency situation, if time permits.

A copy of the emergency evacuation plan should be obtained. It should be examined to determine whether it describes how to leave the IPF in an organized manner that does not leave the facility physically insecure. A sample of IS employees should be interviewed to determine if they are familiar with the documented plan. The emergency evacuation plans should be posted throughout the facility.

Humidity/Temperature Control

The IPF should be visited at regular intervals to determine whether temperature and humidity are adequate.

5.2.2 Physical Access Exposures and Controls

Physical exposures can result in financial loss, legal repercussions, loss of credibility or loss of competitive edge. They primarily originate from natural and human-made hazards and can expose the business to unauthorized access and unavailability of the business information.

Physical Access Exposures

Exposures that exist from accidental or intentional violation of physical access paths include:

- Unauthorized entry
- Vandalism, damage to or theft of equipment or documents
- Copying or viewing of sensitive or copyrighted information
- Alteration of sensitive equipment and information
- Public disclosure of sensitive information
- Abuse of data processing resources
- Blackmail
- Embezzlement
- Wiretapping/eavesdropping

Possible perpetrators include employees with authorized or unauthorized access who are:

- Disgruntled (upset by or concerned about some action by the organization or its management)
- On strike
- Threatened with disciplinary action or dismissal
- Addicted to a substance or gambling
- Experiencing financial or emotional problems
- Notified of termination

Other possible perpetrators include:

- Former employees
- Interested or informed outsiders such as competitors, thieves, organized crime figures and hackers
- Accidental non-malicious actors (e.g., individuals who unknowingly perpetrate violations)

The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.

Other questions and concerns to consider include:

- Are hardware facilities reasonably protected against forced entry?
- Are keys to the computer facilities adequately controlled to reduce the risk of unauthorized access?
- Are computer terminals locked or otherwise secured to prevent removal of boards, chips and the computer itself?
- Are authorized equipment passes required before computer equipment can be removed from its normal secure surroundings?
- Are co-locations and external data centers subject to regular audits?

From an IS perspective, facilities to be protected include:

- Programming areas
- Computer rooms
- Operator consoles and terminals
- Tape libraries, tapes, disks and all magnetic media
- Storage rooms and supplies
- Offsite backup file storage facilities
- Input/output control rooms
- Communications closets
- Telecommunications equipment (including radios, satellites, wiring, modems and external network connections)
- Microcomputers and PCs
- Power sources
- Disposal sites
- Minicomputer establishments
- Dedicated telephones/telephone lines
- Control units and front-end processors

©ISACA. All Rights Reserved.

- Portable equipment (handheld scanners and coding devices, bar code readers, laptop computers, printers, pocket local area network [LAN] adapters and others)
- Onsite and remote printers
- LANs

For safeguards to be effective, they must extend beyond the computer facility to include any vulnerable access points (APs) within the entire organization and at organizational boundaries/interfaces with external organizations. These APs may include remote locations and rented, leased or shared facilities. Additionally, the IS auditor may require assurances that similar controls exist within service providers (SPs) or other third parties if they provide potentially vulnerable APs to sensitive information within the organization.

Physical Access Controls

Physical access controls are designed to protect the organization from unauthorized access. These controls should limit access to individuals specifically authorized by management. The authorization may be explicit (as with a door lock for which management has authorized who has a key) or implicit (as with a job description that implies a need to access sensitive reports and documents). Examples of physical access controls include:

- **Bolting door locks**—Bolting locks require a traditional metal key to gain entry. The key should be stamped "do not duplicate" and should be stored and issued under strict management control.
- **Combination door locks (cipher locks)**—Combination locks use a numeric keypad or dial to permit entry and are often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular intervals or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces the risk of the combination being known by unauthorized people.
- **Electronic door locks**—Electronic door locks require the use of a magnetic or embedded chip-based plastic card key, a token or a biometric measurement entered into a sensor reader to gain access. A special code stored in the card or token is read by the sensor device that activates the door locking mechanism. Electronic door locks have several advantages over bolting and combination locks:
  - Through the special internal code, cards can be assigned to an identifiable individual.
  - Through the special internal code and sensor devices, access can be restricted based on the individual's unique access needs. Restrictions can be assigned to particular doors or to particular hours of the day.
  - They are difficult to duplicate.
  - Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen.
  - Silent or audible alarms can be automatically activated if unauthorized entry is attempted.
- **Biometric door locks**—See section 5.7.16 Biometrics.
- **Manual logging**—All visitors are required to sign a visitor's log indicating their name, the company they are representing, reason for visiting, person to see and date and time of entry and departure. Logging is typically done at the front reception desk and at the entrance to the computer room. Before gaining access, visitors should be required to provide verification of identification, such as a driver's license or vendor identification tag.
- **Electronic logging**—All access can be logged, with unsuccessful attempts being highlighted.
- **Identification badges**—IDs should be worn and displayed by all personnel. Visitor badges should be a different color from employee badges for easy identification. Sophisticated photo IDs can also be used as electronic card keys. Issuing, accounting for and retrieving badges is an administrative process that must be carefully controlled.
- **Video cameras**—All cameras, including motion-activated models, should be located at strategic points and monitored by security guards. The video surveillance recording should be retained for possible future playback, and it should be recorded in sufficient resolution to permit enlarging the image to identify an intruder.
- **Security guards**—Guards are very useful in conjunction with video cameras and locked doors. Guards supplied by an external agency should be bonded to protect the organization from loss.
- **Controlled visitor access**—All visitors should be escorted by a responsible employee. Visitors include friends, maintenance personnel, computer vendors, consultants (unless long-term, in which case special guest access may be provided) and external auditors.
- **Lighting**—Criminals typically favor poorly lit areas. Therefore, ensure that there is adequate lighting around physical premises to deter unauthorized access and improve the effectiveness of video surveillance.

It is critical for the IS auditor to understand that human safety should take precedence in all aspects of information security management. The IS auditor should therefore validate that emergency procedures, disaster

preparedness and proper evacuation procedures are in place.

All service contract personnel, such as cleaning people and offsite storage services, should be bonded personnel. This does not improve physical security but limits the financial exposure of the organization.

A mantrap or airlock entrance (also known as an access control vestibule) uses two doors and is typically found in entries to facilities, such as computer rooms and high-security areas. For the second door to operate, the first entry door must close and lock, with only one person permitted in the holding area. This reduces the risk of piggybacking, when an unauthorized person follows an authorized person through a secured entry. In some installations, this same effect is accomplished by using a full height turnstile. Deadman doors may also be used for delivery and dispatch areas where outer doors open to admit a truck and the inner doors cannot be opened to load or unload until the outer doors are closed and locked.

Computer workstation locks secure the device to the desk, prevent the computer from being turned on or disengage keyboard recognition, thus preventing use. Another available feature is a type of key lock that prevents turning on a PC workstation until unlocked by a turnkey or card key. This is sometimes seen in the case of high-security workstations, such as those that process payroll.

A controlled single-entry point, monitored by a receptionist, should be used by all incoming personnel. Multiple entry points increase the risk of unauthorized entry. Unnecessary or unused entry points, such as doors to outside smoking or break areas, should be eliminated. Emergency exits can be wired to an alarmed panic bar for quick evacuation.

An alarm system should be linked to inactive entry points, motion detectors and the reverse flow of enter-or exit-only doors. Security personnel should be able to hear the alarm when activated.

Secured report/document distribution carts such as mail carts, should be covered and locked and should not be left unattended.

Facilities such as computer rooms should not be visible or identifiable from the outside; there should be no windows or directional signs. The building or department directory should discreetly identify only the general location of the IPF. If windows are present, they should be constructed of reinforced glass and, if on the ground floor of the building, further protected (e.g., with bars).

Auditing Physical Access

Touring the computer site is useful for the auditor to gain an overall understanding and perception of the installation being reviewed. As with environmental controls where the site is owned by a third party, a contractual right of audit may be required. A tour provides the auditor with the opportunity to begin reviewing physical access restrictions (e.g., control over employees, visitors, intruders and vendors).

The computer site (i.e., computer room, developers' area, media storage, printer stations and management offices) and any offsite storage facilities should be included in the tour. Much of the testing of physical safeguards can be achieved by visually observing safeguards. Documents to assist with this effort include emergency evacuation procedures, inspection tags, fire suppression system test results and key lock logs.

Testing should extend beyond the computer room to include the following related facilities:

- Locations of all operator consoles
- Printer rooms
- Computer storage rooms (including equipment, paper and supply rooms)
- UPS/generator
- Locations of all communications equipment identified on the network diagram
- Media storage
- Offsite backup storage facility

To complete a thorough test, the IS auditor should look above the ceiling panels and below the raised floor in the computer operations center, observing smoke and water detectors, general cleanliness and walls that extend all the way to the real ceiling (not just the fake/suspended ceiling). For a ground-floor computer room, the auditor may also consider walking around the outside of the room, viewing the location of any windows, examining emergency exit doors for evidence they are routinely used (such as the presence of cigarette stubs or litter) and examining the air conditioning units. The auditor should also consider whether any additional threats exist close to the room, such as storage of dangerous or flammable material.

The following paths of physical entry should be evaluated for proper security:

- All entry doors
- Emergency exit doors
- Glass windows and walls
- Movable walls and modular cubicles
- Areas above suspended ceilings and beneath raised floors

©ISACA. All Rights Reserved.

- Ventilation systems
- Areas behind curtains or fake walls

5.2.3 Industrial Control Systems Security

Industrial control systems (ICSs) refer to systems that manage and operate infrastructure-supporting functions such as water, power and transportation. Types of ICSs include:

- Supervisory Control and Data Acquisition (SCADA) systems
- Programmable logic controllers (PLCs)
- Remote terminal units (RTUs)

The continued increase in use of smart devices and the Internet of Things (IoT) is significantly transforming ICSs and introducing a wide range of new security risk factors. ICS security focuses on ensuring the security of ICSs, including the hardware and software components of the systems.

ICS Risk

Some of the weaknesses or risk commonly found in ICS environments include:

- **Poor security posture**—Information security planning of ICS-controlled systems in most cases only considers the physical security posture of the system and the implementation of controls to restrict physical access to authorized personnel. The designers give less thought to the physical security of ICS components, applications, networking equipment, telecommunication lines and other infrastructure elements.
- **Improper input validation**—Input validation ensures that content provided to an ICS application does not provide an attacker with access to unintended functionality or privilege escalation. Improper input can affect the control flow or data flow of an ICS application.
- **Improper authentication processes**—Authentication processes are used to determine if the command or client is valid and has permissions for access in an ICS. Most ICS remote elements do not authenticate the commands that are issued to them, leading to the execution of illegitimate commands. Providing authorizations to third parties for remote access to the ICS domain requires the building of trust. Nevertheless, a threat exists that the third party is lax in information security.
- **Poor security configuration and maintenance practices**—Poor patch management, programming flaws, misconfigurations or poor maintenance of ICS platforms, OSs and ICS applications increase risk. Secure authentication applications may be in use, but their configuration may not be correct.
- **Embedded software**—ICSs, such as SCADA systems, typically have embedded Internet-connected controllers that can serve as attack vectors due to their potential security vulnerabilities.
- **Network design weaknesses**—Network infrastructure environments of ICSs are typically developed and modified based on business and operational requirements, with little consideration for potential security risk. They may fail to deploy defense-in-depth strategies, usually lack defined zones and have limited to no port security.
- **Technological depreciation cycle**—Technological aging of ICSs is considered a threat due to the prevalence of technology with limited processing and memory capacities. These technologies are often not able to run with more secure modern ICS applications. ICS components have a long useful life, and their processing and memory capacities may be limited to running newer ICS applications. This affects the implementation of cryptographic security modules that require processor power and memory.
- **Incompatibility with information security standards**—Adhering to a strict implementation of ICT-based security standards, such as International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27001, may be a threat. Such standards were originally developed for the office environment and may not be applicable to ICSs.
- **Weak information security protocols**—ICSs and their protocols were designed in the period of proprietary practices with limited knowledge of ICS technology and few threats. Therefore, ICS protocols do not always protect the content of protocol messages. Most ICSs have weak implementations of cryptography libraries and a high likelihood of inadequate encryption strength, thereby allowing unauthorized access to data in the ICS.
- **Dependencies on other information and communication technology (ICT) systems**—The ICS domain uses systems located in the ICT domain for acquiring information critical to the controlled processes to reduce costs and install the system in the ICS domain. However, upgrades and/or restarts processed by ICT may lead to ICS instability. Emergency generators and batteries may supply power for the continuation of the ICS processes. However, if generators and batteries are not well-maintained, they often fail when power capacity is critical for the ICSs and controlled physical processes.

- **Presence of third parties on site**—Third parties such as ICS maintenance engineers and system integrators occasionally require access to engineering stations, the ICS equipment and components. Often their activities are not monitored, leading to the risk of uncontrolled modifications in the ICS environment.
- **Compliance risk**—The ICS architecture and operations may be noncompliant with specific laws and regulations, which can lead to breaches and attract penalties and fines that are costly to businesses.

ICS Security Best Practices

Best security practices for ICSs include:

- **Conduct an ICS asset inventory**—An asset inventory provides full visibility and understanding of ICS assets and their network connectivity, which are critical for security purposes. After the inventory, an assets classification should be undertaken for the purpose of determining the criticality of the ICS assets.
- **Monitor ICS network baselines**—ICS networks should be monitored on a regular basis for the purpose of establishing network baselines. After the baselines are established, any network performance should be compared to them and anomalies detected and addressed.
- **Segment ICS networks**—ICS networks used to be protected by air gaps, but that practice has been abandoned. Segmentation—typically through the implementation of firewalls that understand ICS protocols—is critical since ICSs were not originally designed to be connected to the Internet. Segmentation prevents general IS attacks from affecting ICSs.
- **Implement the principle of least privilege (POLP)**—The POLP should be implemented in all systems that do not typically have access controls, such as ICSs. This will ensure that even if access to critical areas of the ICS network is provided the damage may be little, as there are restrictions in place as to what users can do if they are given access.
- **Deploy intrusion detection systems (IDSs)/ intrusion prevention systems (IPSs)**—An IDS enhances ICS security by issuing threat alerts, placing it in a position to respond to existing malware infections and other security incidents. An IPS should also be implemented to identify and immediately block any attempted exploitation of known vulnerabilities by malicious actors.
- **Secure remote access**—Remote access is typically required for the purposes of monitoring and managing geographically distributed ICS assets. For example, data should be encrypted while being stored at or transmitted to an ICS site.
- **Secure physical access**—ICSs should always be protected by physical security measures since the systems are basically physical in nature. Physical measures that can be used to secure ICSs include guards and badges.
- **Implement redundancy**—Redundancy should be provided for the most critical ICS components. This reduces the risk of production interruptions because if one line fails or is attacked, another line will be on standby to keep production online. This is especially important in high-risk ICSs such as nuclear power plants.
- **Harden the ICSs and networks**—To increase ICS security, both the systems and the networks should be hardened. For example, unused ports should be blocked and security patches installed.
- **Develop an incident response plan (IRP)**—ICSs often face a plethora of threats from attackers. These threats are quite risky as the security posture of an ICS is typically weak, making incidents inevitable. The organization should have a plan in place to respond to such incidents and enable quick recovery to normal operations.
- **Supply chain security**—Security practices of third-party vendors and SPs involved in the ICS supply chain should be assessed to ensure that their hardware and software components do not contain vulnerabilities, including malicious code. This is to prevent the risk of contaminating the entire ICS operating environment.

5.3 Identity and Access Management

Identification and authentication (I&A) is a critical building block of information security because it is needed for most types of access control and is necessary for establishing user accountability.

For most systems, I&A is the first line of defense because it prevents unauthorized access (or unauthorized processes) to a computer system or an information asset. Logical access can be implemented in various ways. The IS auditor should be aware of the strengths and weaknesses of various architectures along with the risk associated with the different architectures and how it may be addressed.

The identification system is separate from the authentication system. The systems differ with respect to:

- Meaning

- Methods, peripherals and techniques supporting them
- Requirements in terms of secrecy and management
- Attributes

Another key difference is that identity does not normally change, but authentication tokens must be regularly replaced to preserve their reliability.

Some of the common I&A vulnerabilities that may be exploited to gain unauthorized system access include:

- Weak authentication methods (e.g., no enforcement of password minimum length, complexity and change frequency)
- Use of simple or easily guessed passwords
- The potential for users to bypass the authentication mechanism
- The lack of confidentiality and integrity for the stored authentication information
- The lack of encryption for authentication and protection of information transmitted over a network
- The user's lack of knowledge about the risk associated with sharing authentication elements (e.g., passwords and security tokens)

5.3.1 Identity and Access Management

An identity and access management (IAM) framework consists of policies, procedures, processes and technologies that enable the management of identity and access information in an organization. It facilitates and controls user access to critical organizational information, both on-premises and in the cloud environment. Its purpose is to provide the right access to the right people, at the right time, with bare minimum interference. The major elements of IAM can be grouped into four components, as shown in **figure 5.5**.

Figure 5.5—IAM Service Components

Authentication Services • Single sign-on (SSO) • Federated identity management (FIM) • Multifactor authentication (MFA) • Biometric authentication • Adaptive authentication • Session management	**Authorization Services** • Rule-based access control • Role-based access control (RBAC) • Attribute-based access control • Privileged access management • Remote authorization
User Management • Provisioning • Deprovisioning • Self-service • Credential management • Delegated administration	**Central User Repository** • Directory services • Identity providers (IdPs) • Data synchronization • Identity stores • Directory federation • Virtual directory

Benefits of IAM

Some of the benefits of an effective implementation of an IAM program include:

- **Improves regulatory compliance**—Standards may require strict policies around who can access data and for what purposes. IAM systems allow companies to set and enforce formal access control policies that meet those standards. Companies can also track user activity to prove compliance during an audit.
- **Enhances data security**—A key risk of traditional security is that it often has a single point of failure —user passwords. If attackers manage to breach passwords, the organization automatically becomes vulnerable to various types of attacks. IAM services narrow the various points of failure. They can also reduce credential theft by adding extra authentication layers, a form of defense in depth. Threat actors must penetrate multiple layers to reach sensitive data, and IAM can limit the lateral movement of malicious threat actors.
- **Promotes digital transformation**—Organizations need to facilitate secure access for users to spearhead digital transformation activities. IAM systems assist in this process by centralizing IAM and maintaining security without affecting the user experience.
- **Improves productivity**—Once successfully logged on to an IAM portal that supports single sign-on (SSO), employees no longer need to remember

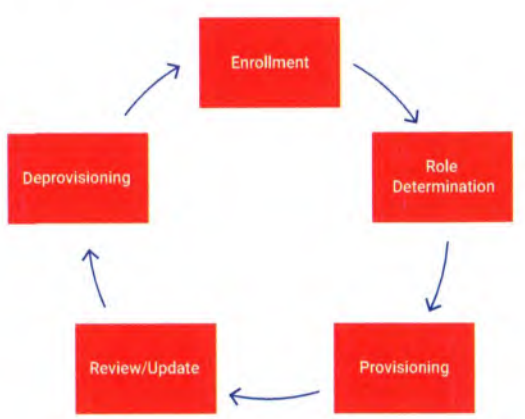
 ©ISACA. All Rights Reserved.

passwords to perform their routine duties. They can access a variety of tools for their roles, reducing IS staff workload.
- **Streamlines access control**—IAM can help the organization streamline the entire process of access control in complex environments like the cloud, which simplifies the provisioning and administration of access control.

IAM Life Cycle Management

Identity life cycle management is the process of creating and maintaining a digital identity for every human or non-human entity on a network. It includes processes for provisioning new users, updating existing accounts and deprovisioning users who no longer need access. **Figure 5.6** shows the stages of the IAM system.

Figure 5.6—The IAM Life Cycle



These phases can be explained as the following:
- **Enrollment**—Enrollment involves the process of creating and/or registering user accounts. An enrolled user is typically an end user who accesses the organization's systems or applications. There are three main methods of user enrollment: automatic enrollment, self-enrollment and manual enrollment. Automatic enrollment is done automatically by the system while self-enrollment involves users enrolling themselves.
- **Role determination**—The next stage in the IAM life cycle involves determining the roles of the enrolled users within an organization. Once the roles have been determined, privileges and access requirements can also be determined. IS auditors should be able to distinguish this stage from the provisioning stage. The key point for the IS auditor to note is that while a role may determine access permissions, the *role itself does not inherently contain permissions*, a name, a description or a scope.
- **Provisioning**—Provisioning specifies access levels to grant a user. For example, some users may be granted permissions to update accounts while others are restricted to viewer status. IAMs enable user provisioning through policies defined based on role-based access control (RBAC). Users are assigned one or more roles and the RBAC IAM system automatically grants them access.
- **Review/Updating**—Account updating involves continuously performing updates based on changes in roles, privileges and access requirements. An example is an employee being promoted to a higher position that entails new roles and responsibilities, requiring an update to the employee's identity information to reflect the new entitlements. IS auditors should be concerned about possible privilege creep at this stage.
- **Deprovisioning**—The purpose of deprovisioning is to avoid security risk presented by the possibility of former users retaining access to organizational systems after they have left the organization. Actions involved in the deprovisioning process include deleting the account, disabling the account and retaining it and disabling it later.

IAM Best Practices

Figure 5.7 identifies the major gaps in IAM and corresponding best practices/recommendations. These are separated based on the key stages of IAM in an organization.

©ISACA. All Rights Reserved.

Figure 5.7—Key Concepts with Corresponding Security Concerns, Good Practices and Recommendations to Help Remediate the Gaps

Key Concepts of IAM	Identified Gaps and Security Concerns	Good Practices/Recommendations
Identify creation and access request	Authorized approval not in place	• The required authority (e.g., the user's manager, the resource owner or the security officer) should authorize the user for access to be granted.
	Privileged access granted without analyzing the need	• To justify its need, privileged access should be provided after approval is issued at two levels—the reporting manager level; and the reporting manager's manager or application, database or server owner level.
	Group shared access	• To justify its need, group shared access should be provided after approval is issued at two levels—the reporting manager level; and the reporting manager's manager or application, database or server owner level. • The principle of least privilege (POLP) should be applied. • The number of servers on which the account can exist should be limited. • The list of users sharing the account should be preapproved. • Account owners should maintain and publish a list of users who have access to the shared account. • The logging activities for shared accounts should be validated. • Passwords should be changed on a regular basis and whenever an employee leaves the organization or changes roles. The frequency should be defined in the process document. • If it is found that someone obtains unauthorized access, the password must be changed immediately.
Transfer request	Authorized approval not in place	• The required authority should give authorized access. • In cases of employee transfers or changes in job roles, access privileges must be reevaluated and adjusted based on the individual's new responsibilities.
Access termination request	User IDs not revoked immediately after termination	• Access termination should be carried out as soon as the access termination request is received.
Password communication	Unsecure means to communicate passwords	• Passwords can be communicated via user email in encrypted format. • Passwords must be stored in a sealed envelope.
Password management	Password parameters not followed	• The minimum password length should depend largely on the threat model being addressed.[34]
	Password complexity not met	

[34] See Appendix A of *https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf* for more information.

 ©ISACA. All Rights Reserved.

Figure 5.7—Key Concepts with Corresponding Security Concerns, Good Practices and Recommendations to Help Remediate the Gaps (cont.)

Key Concepts of IAM	Identified Gaps and Security Concerns	Good Practices/Recommendations
Password management *(cont.)*	Nonexistent password policies, standards and guidelines	• Passwords should contain a mix of lower- and upper-case letters, numbers and punctuation. Passwords should be difficult to guess. Passwords should not consist of: ▪ Words found in the dictionary ▪ Derivatives of the user ID ▪ Common character sequences ▪ Personal details, such as first name, last name, birth date, etc. • An encrypted history file should be maintained and should, at a minimum, retain the last 13 passwords for each user ID. • Users should be educated and made aware of password confidentiality to hinder them from displaying and printing passwords. • Password changes should be enforced: 30 days for privileged access IDs and 90 days for regular access. • At first login, a mandatory password change should be enforced. • At a maximum, five consecutive unsuccessful attempts should lead to suspension of the account until it is reset by the system administrator. • A time-out feature or screensaver should be enabled after 15 minutes of inactivity. • Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over networks. • The password must be changed promptly when disclosure is suspected. • Each user ID should be uniquely identifiable, preferably to the username. • The last login date and time should be displayed for the user at the time of login.
Policy administration	Lack of documented processes, policies and procedures Lack of timely process review	• Document review should be carried out on a regular basis—preferably yearly. The document must have: ▪ The next review date ▪ The name of the process owner ▪ The name of the process approver ▪ The scope of the process ▪ Location of the document ▪ Roles and responsibilities ▪ Measurements (key performance indicators) ▪ Workflows ▪ Templates, forms and formats
Validation	Validation process not in place/not adhered to	• All user accounts should be re-evaluated by user managers at a fixed frequency—preferably

©ISACA. All Rights Reserved.

Figure 5.7—Key Concepts with Corresponding Security Concerns, Good Practices and Recommendations to Help Remediate the Gaps (cont.)

Key Concepts of IAM	Identified Gaps and Security Concerns	Good Practices/Recommendations
Validation *(cont.)*	Timely action not taken for accounts that are not validated in the process	six months for normal user accounts and three months for privileged user accounts. • Validations should be reviewed by user managers or resource, application or data owners.
Reinstatement	Reinstatement without valid authorization	• All requests should be checked for valid granted approvals. User accounts that lack approvals or correct authorization requests should not be reinstated.
Authorization subprocess	Access given without authorization	• All requests should be checked for valid granted approvals. User accounts that lack approvals or correct authorization requests should be blocked at the access request stage. • The required authority should authorize the user for access to be granted.
Separation of duties (SoD)	Lack of SoD	• All requests passing through the IAM process should be validated for SoD policy checking. Requests that fail the SoD check should be blocked at the access request stage. • Automated tools to enforce SoD controls should be used.
Log management	Lack of logging, auditing and reviewing of events	• A log management process should be in place.
Privileged access	Access provided to users without validating the needs of access	• To justify its need, privileged access should be provided after approval is issued at two levels—the reporting manager level; and the reporting manager's manager or application, database or server owner level.
	Periodic revalidation process not in place	• Documented processes must be in place. • Revalidation of privileged accounts must be conducted on a quarterly basis.
	Revalidation process in place although the non-validated accounts are not terminated	• At a minimum, non-validated accounts should be terminated/locked within one working day (at a maximum, five working days).
Dormant/orphan user accounts	Owners or custodians not identified for user accounts	• Accounts not logged in for a denied period should be investigated and removed. • All accounts without an owner or custodian need to be identified and highlighted so they can be assigned or removed.

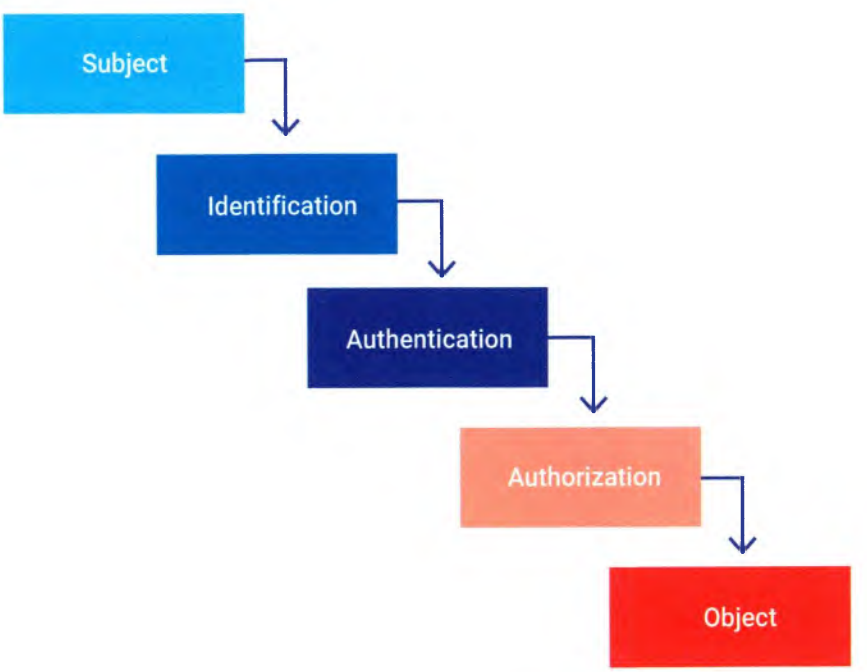
Source: Kaur, H.; "Identity and Access Management—Its Role in Sarbanes-Oxley Compliance," ISACA, 1 November 2011, *https://www.isaca.org/resources/isaca-journal/past-issues/2011/jonline-identity-and-access-management-its-role-in-sarbanes-oxley-compliance*

5.3.2 Authentication, Authorization and Accountability

User accountability requires the linking of activities on a computer system to specific individuals and, therefore, requires the system to identify users. If users are not properly identified and authenticated, particularly in today's open-system networked environments, organizations have a higher exposure to risk of unauthorized access.

Authentication, authorization and accountability are interlinked. The relationship between these concepts in an organization is shown in **figure 5.8**.

Figure 5.8—AAA Relationships



A subject is any entity that has the capability to access and/or manipulate an object (e.g., a human user or a process that is running in memory). On the other hand, an object is an entity that contains information or resources. Subjects are active entities while objects are passive entities. A subject has to be identified first, then authenticated to prove it is who or what it claims to be. After authentication, the subject may be allowed to access and act upon objects, which is authorization. The whole chain works within the context of accountability through tracking user access and the consumption of resources.

Commonly used protocols in implementing authentication, authorization and accountability include the Remote Access Dial-In User Service (RADIUS), Kerberos, Security Assertion Markup Language (SAML) and Open Authentication (OAuth). See section 5.7.18 Federated Identity Management for more information.

Authentication

Authentication is the process of proving that subjects are who or what they claim to be; it verifies a subject's identity. It ensures that the right users and devices can access the right resources for the right reasons at the right time. When users request access to a resource, the IAM system checks their user credentials against the credentials stored in the directory. If they match, access is granted. Various types of authentications are used in IAMs:

- **Password authentication**—Passwords are the most common and simplest methods of authentication (something you know) in use in many organizations. Passwords can come in the form of a string of letters, numbers or special characters or some combination of these items. The IS auditor should be cognizant of the fact that users often use passwords for convenience rather than security and should encourage good password practices.

©ISACA. All Rights Reserved.

- **Multifactor authentication (MFA)**—MFA requires users to provide two or more authentication factors to prove their identities before being granted access to organizational systems. Common factors include knowledge factors, possession factors and biometric factors.
- **Adaptive authentication**—Adaptive authentication, sometimes known as risk-based authentication, is an authentication method that changes its requirements in real time as and when risk changes. When seeking authentication from their usual devices, users typically enter only a username and password. However, when logging in from untrusted devices, users may be required to submit additional authentication factors.
- **Token-based authentication**—Token-based authentication is a typical example of possessive authentication technology (something you have), which requires that users log in their credentials only once to receive unique encrypted strings of random characters known as tokens. The tokens are then used to access the organization's systems instead of requiring that users enter credentials several times. A digital token is enough proof that a user already holds access permissions. Token-based authentication is widely used in RESTful application programming interfaces (APIs), which are accessed by several clients.
- **Certificate-based authentication**—In certificate-based authentication technologies, subjects are authenticated using digital certificates. See section 5.11.1 Digital Certificates.
- **Biometric authentication**—See section 5.7.16 Biometrics.
- **Lightweight Directory Access Protocol (LDAP) authentication**—LDAP is a standards-based protocol that stores information and metadata about users, groups, computers or other objects. Metadata in an LDAP directory can be used for dynamic authentication systems or other automation processes. The most common LDAP system today is Microsoft Active Directory. LDAP authentication is accomplished through a bind operation. To authenticate, the client sends a bind request to the LDAP server together with the user's identifier and password. If the user's submitted credentials match the credentials stored within the LDAP database, the user is authenticated and granted access. If the credentials do not match, the bind fails and access is denied.
- **Smart card authentication**—Smart card authentication technology is similar to token-based authentication, but it offers additional functionalities, such as computer MFA, cashless vending and corporate photo IDs. It is similar to a credit card except that has an embedded microprocessor and an electronic interface. Smart cards have an advantage in that they can be individualized and customized to meet the organization's requirements.

Single Sign-On Authentication

SSO is defined as the process of consolidating all organization platform-based administration, authentication and authorization functions into a single centralized administrative function. SSO is a subset of basic username-password-based authentication. SSO authentication provides advanced security and multiple features with a frictionless experience for end-users. It allows individuals to enter their usernames and passwords once and get access to all configured applications This function provides the appropriate interfaces to the organization's information resources, such as client-server and distributed systems, mainframes, and network security including remote access mechanisms.

SSO allows users to access multiple apps and services with one set of login credentials. The SSO portal authenticates the user and generates a certificate or token that acts as a security key for other resources. Many SSO systems use open protocols, such as SAML, that allow the sharing of keys among SPs. The SSO process begins with the first instance where the user credentials are introduced into the organization's IT computing environment. The information resource or SSO server handling this function is referred to as the primary domain. Every other information resource, application or platform that uses those credentials is called a secondary domain.

The challenges in managing diverse platform through SSO involve overcoming the heterogeneous nature of diverse networks, platforms, databases and applications often found in organizations when establishing a set of credentials acceptable to all of the information resources. To achieve effective integration with the SSO process, SSO administrators need to know how each system manages credentialing information, understand access control list (ACL) authorization rules, and be familiar with audit logs and reports. Requirements developed in this regard should be based on security domain policies and procedures. SSO advantages include:

- Multiple passwords are no longer required; therefore, a user may be more inclined and motivated to select a stronger password.

 ©ISACA. All Rights Reserved.

- SSO improves an administrator's ability to manage users' accounts and authorizations to all associated systems.
- SSO reduces administrative overhead in resetting forgotten passwords over multiple platforms and applications.
- SSO reduces the time users take to log into multiple applications and platforms.

SSO limitations include:

- Support for all major OS environments is difficult. SSO implementations will often require a number of solutions integrated into a total solution for an enterprise's IT architecture.
- The costs associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary.
- The centralized nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information assets. For this reason, strong authentication in the form of complex password requirements and the use of biometrics is frequently implemented.

Authorization

Authorization is the process of granting access to specific types of services or resources based on the authentication process of the user. It helps in providing restricted permissions to users based on physical location, IP address or time of access. Authorization ensures that only authorized users are allowed to access and use organizational resources according to an organization's permissions and privileges. Authorization-related processes enforce least privilege, need-to-know and separation of duties. Authorization is further divided into coarse and fine dimensions:

- **Coarse-grained authorization**—Coarse-grained authorization is an authorization method that makes a high-level determination of whether a subject is authorized to use or access an object. However, it does not determine what the subject can view or how it can act once access is granted. This method typically requires a lower level of specificity in granting or denying access. For example, any user under a particular role in the finance department can access the cloud service.
- **Fine-grained authorization**—Fine-grained authorization starts from coarse-grained authorization and then goes a step further to refine subject access. It grants and/or revokes access to sensitive and critical data based on various conditions. The technology acts as the object itself and enforces the POLP, need-to-know and separation of duties (SoD) restrictions. An example of fine-grained authorization is users under a certain role, such as database administrator, can access the database service only if they have spent at least two months with the organization.

Authorization Issues

The authorization process used for access control requires that the system be able to identify and differentiate among users.

Access rules (authorization) specify who can access what. Access should be on a documented need-to-know and need-to-do basis by type of access.

Computer access can be set for various levels (i.e., files, tables, data items). When IS auditors review computer accessibility, they need to know what can be done with the access and what is restricted. For example, access restrictions at the file level generally include:

- Read, inquiry or copy only
- Write, create, update or delete only
- Execute only
- A combination of the above

The least dangerous type of access is read only, as long as the information being accessed is not sensitive or confidential. This is because the user cannot alter or use the computerized file beyond basic viewing or printing.

Access Control Lists

To provide security authorizations for files and facilities, logical access control mechanisms use access authorization tables, also referred to as ACLs or access control tables. ACLs refer to a register of:

- Users (including groups, machines and processes) who have permission to use a particular system resource
- The types of access permitted

ACLs vary considerably in their capability and flexibility. Some only allow specifications for certain pre-set groups (e.g., owner, group and world), while more advanced ACLs, such as user-defined groups, allow much more flexibility. More advanced ACLs can be used to explicitly deny access to a particular individual or group. With more advanced ACLs, access can be at the discretion of the policy maker (and implemented by the security administrator) or individual user, depending on how the controls are technically implemented. When users change job roles within an organization, often their old access rights are not removed before adding their new

©ISACA. All Rights Reserved.

required accesses. Failure to remove the old access rights could be a potential SoD issue.

Logical Access Security Administration

In a client-server environment, the access I&A and authorization processes can be administered either through a centralized or decentralized environment. The advantages of conducting security in a decentralized environment are:

- The security administration is onsite at the distributed location.
- Security issues are resolved in a timely manner.
- Security controls are monitored on a more frequent basis.

The risk associated with distributed responsibility for security administration includes:

- Local standards might be implemented rather than those required by the organization.
- Levels of security management might be below what can be maintained by a central administration.
- Management checks and audits that are often provided by central administration to ensure that standards are maintained might be unavailable.

There are many ways to control remote and distributed sites:

- Software controls over access to the computer, data files and remote access to the network should be implemented.
- The physical control environment should be as secure as possible, with additions such as lockable terminals and a locked computer room.
- Access to microcomputers from remote locations via modems and laptops should be controlled appropriately.
- Opportunities for unauthorized people to gain knowledge of the system should be limited by implementing controls over access to system documentation and manuals.
- When practical, central monitoring should ensure that all remotely processed data has been received completely and updated accurately.
- If replicated files exist at multiple locations, controls should ensure that all files used are correct and current. If data is used to produce financial information, controls should ensure that no duplication arises.

Accountability

Accountability refers to the tracking of user activity and consumption of resources by users and is sometimes referred to as accounting. Each action, from identity presentation through authentication and authorization, should be logged to ensure accountability. The logs should be stored for audits and/or sent to a log management solution for analysis purposes. Logs provide an audit trail and insight into the effectiveness of access control and how subjects may abuse access. Accountability supports aspects of information security, such as nonrepudiation, deterrence, fault isolation and legal action. IAM tools generate reports to ensure compliance and assessment of security risk throughout the process. To provide assurance that accountability is properly implemented in the organization the IS auditor may evaluate whether:

- Management is committed to ensuring a culture accountability.
- Accountability is addressed in the information security policy.
- There are no shared passwords.
- The default administrator accounts of network devices have been removed.
- Service IDs cannot be used to log in interactively.
- Proximity cards have been installed to control user logins.
- Video recording has been installed to match event log entries to user actions.

5.3.3 Zero-Trust Architecture

Zero-trust architecture (ZTA) is a cybersecurity framework that requires every access request to be authenticated, authorized and validated for security configuration and posture before being granted or allowed to maintain access to the organization's resources. Simply, zero trust adheres to the saying, "Never Trust, Always Verify."

Because ZTA is an emerging field, the IS auditor should be alert to the various interpretations regarding what constitutes ZTA in the marketplace. Basics of zero trust include:[35]

- **Resources include all data and computing services**—All data sources and computing services are considered resources, and a network may be composed of multiple classes of devices. A network may also have some devices that send data to

[35] National Institute of Standards and Technology, *Special Publication 800-207: Zero Trust Architecture*, USA, 2020, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf*

aggregators/storage and software as a service (SaaS) systems.
- **Communication security**—All communication is secured regardless of network location as location alone does not imply trust. Access requests from assets located inside a legacy network perimeter must meet the same security requirements as access requests and communication from any non-enterprise-owned network.
- **Session-based access**—Access to organizational resources is granted on a per-session basis with trust in the requester being evaluated before access is granted. Access should also be granted based on the POLP.
- **Dynamic policy-based access control (PBAC)**—An organization protects resources by defining what resources it has, who its members are, and the level of access to resources those members need. These definitions are clearly stated in the organization's security policies. POLP is applied to restrict both visibility and accessibility.
- **Monitoring and measurement**—The enterprise monitors and measures the integrity and security posture of all owned and associated assets. No asset is inherently trusted. The enterprise evaluates the security posture of the asset when evaluating a resource request.
- **Dynamic authentication and authorization**—Dynamic authentication and strictly enforced authorization are implemented before access is allowed. This is a constant cycle of obtaining access, scanning and assessing threats, adapting and continually reevaluating trust in ongoing communication.
- **Intensive information gathering**—The enterprise collects as much information as possible about the current state of assets, asset security posture, network traffic and access requests. It processes that data and uses any insight gained to improve policy creation and enforcement.

ZTA Best Practices

ZTA is gaining traction mainly due to the weaknesses of other trust models. The IS auditor reviewing the implementation of ZTA in an organization should ensure the organization uses ZTA best practices for the success of the ZTA initiative. Some of the best practices for ZTA include:
- **Monitor network traffic and connected devices**—Visibility is crucial in order for users and machines to be verified and authenticated.
- **Regularly update devices**—Vulnerabilities need to be patched as quickly as possible and access to vulnerable devices restricted.
- **Implement the POLP**—Everyone in the organization should have the least amount of access needed for the performance of duties. This minimizes the damage if an end user account becomes compromised.
- **Segment the network**—Splitting the network into smaller segments helps ensure breaches are identified and contained early, before they can spread to the entire network.
- **Implement security keys for MFA**—Hardware-based security tokens are often more secure than soft tokens such as one-time passcodes.
- **Incorporate threat intelligence**—IS auditors should always keep in mind that attackers are constantly updating and refining their tactics. It is therefore critical to advise the organization to subscribe to the latest threat intelligence data feeds for the timely identification of threats before they spread.
- **Implement good password practices**—Everyone in the organization should abide by strict password requirements.

Implementing IAM Using ZTA

The IAM solution can be implemented using ZTA by:
- **Central management**—A key principle of ZTA is managing access to resources at the identity level; therefore, having centralized management of identities can make this approach much simpler. This could mean migrating users from other systems or synchronizing the IAM with other user directories.
- **Secure access**—Since security at the identity level is key, an IAM should confirm the identities of those logging in. This could mean implementing MFA or a combination of MFA and adaptive authentication to take into consideration the context of the login attempt in terms of location, time and device.
- **Policy-based control**—Users should be given authorization only to perform their required tasks and no more privilege than is necessary. An IAM should be designed to give users access to resources based on their job roles, their departments or any other attributes that seem appropriate.
- **Secured privileged accounts**—Not all accounts in an access management system are created equal and have equal privileges. Accounts with privileged access to sensitive information can be provided with a tier of security and support that suits their status as gatekeepers for the organization.

©ISACA. All Rights Reserved.

5.3.4 Privileged Access Management

Privileged access management (PAM) consists of the information security strategies and technologies for exerting control over the privileged or elevated access levels and permissions for users, accounts, processes and systems across an IS environment. It is a component of an IAM solution with the processes and technologies needed to secure privileged accounts.

In information security, privilege is authority that is given to an account or process in a computer system or network. Privileges typically provide authorization to override or bypass security controls. Permissions enable actions like shutting down systems, configuring networks and configuring accounts. Privileged accounts include:

- **Administrative accounts**—Nonpersonal accounts providing administrative access to the local host or instance only; privileged administrative access across all workstations and servers within the domain
- **Emergency accounts**—Unprivileged users with administrative access to secure systems in case of an emergency; also known as "break glass" accounts
- **Service accounts**—Privileged local or domain accounts used by an application or service to interact with the operating system
- **Application accounts**—Privileged accounts used by applications to access databases, run batch jobs or scripts, or provide access to other applications
- **Secure Socket Shell (SSH) key**—Access control protocols that provide direct root access to critical organizational systems. Root is the username or account that, by default, has access to all commands and files on Linux or other Unix-related OSs.

PAM implementation can have a number of benefits in the organization.

Some of the benefits the IS auditor should be aware of include:

- **Reduction in attack surface**—PAM helps organizations reduce their attack surface across networks, servers and identities, and mitigate risk of attack.
- **Support for least privilege enforcement**—PAM assists in enforcing POLP, preventing incidences of privilege creep in the organization.
- **Streamlining rights provision**—PAM enables users, applications and other system processes with elevated rights to access certain resources and complete work-related tasks.
- **Monitoring of privileged accounts**—PAM provides system administrators with the functionality, automation and reporting they need to manage privileged accounts.
- **Resolve security risk**—A PAM solution can solve security weaknesses, such as multiple users accessing and obtaining knowledge of the same administrative password for a particular service. It also mitigates the risk of long-standing static passwords that system administrators are reluctant to change for fear of causing unplanned disruptions.
- **Secure access control**—PAM controls key aspects of secure access and simplifies the provisioning of administrator user accounts, elevated access rights and configuration for cloud applications.
- **Data breach reduction**—The implementation of PAM in an organization reduces the probability of data breaches due to internal and external cybersecurity threats as the attack surface is also reduced.

PAM Risk

Organizations face several challenges protecting, controlling and monitoring privileged access. The IS auditor should be alert to those challenges and be in a position to provide assurance to management and the board. Some of these challenges include:

- **Challenges in managing account credentials**—PAM requires automation for efficiency in rotating and updating privileged credentials. However, many organizations still rely on manually intensive processes that are prone to errors.
- **Difficulties in tracking privileged activity**—Many organizations may not be in a position to centrally monitor and control privileged sessions, thereby exposing the business to information security threats and regulatory compliance violations.
- **Ineffective threat analysis**—If an organization lacks comprehensive threat analysis tools, it may not be able to proactively identify, monitor and analyze suspicious activities stemming from privileged accounts in order to remediate them.
- **Cloud privileged user access**—Organizations often struggle to effectively control privileged user access in cloud platforms, thereby creating compliance risk and operational complexities.
- **Authentication protocol vulnerabilities**—Information security attackers may exploit vulnerabilities in authentication protocols such as Kerberos and impersonate authorized users to gain privileged access to critical IT resources and confidential data.

 ©ISACA. All Rights Reserved.

PAM Best Practices

The IS auditor should view a PAM solution as only as effective as its implementation. If the solution is not appropriately implemented, its operating effectiveness is likely to be low.

Organizations should consider adopting best practices:

- **Implement the POLP**—It is important for the IS auditor to understand that privileged accounts cannot be managed without first implementing the POLP. Restricting the security environment to allow only privileged accounts to access resources is a requirement for a successful PAM solution implementation.
- **Track all privileged accounts**—It is usually difficult to manage a privileged account if it is not part of the PAM solution. Therefore, all privileged accounts should be tracked and incorporated into PAM.
- **Consider temporary privilege escalation**—Instead of granting a user perpetual privileged access, consider providing access only when needed and then removing it.
- **Implement RBAC**—PAM only works on a system if the organization has differing role-based access levels. For example, in environments where everyone is an administrator, PAM is much more challenging to secure and manage.
- **Automate PAM processes**—Automation reduces the risk of human error and increases the efficiency of operations in the information security environment.
- **Monitor and audit**—Attackers often target privileged accounts, so monitoring and actively logging all privileged account activity is vital to ensure an organization has the insights it needs to protect its environment.
- **Control and secure infrastructure accounts**—It is advisable to place all well-known infrastructure accounts in a central digital vault for greater visibility and ease of management.
- **Limit lateral movement**—Limiting lateral movement helps contain the spread of attacks to other systems. All endpoint users from the local admin groups on workstations should be removed to stop credential theft.
- **Protect credentials for third-party applications**—All privileged accounts used by third-party applications should be placed in a secure vault. This assists in eliminating hardcoded credentials for commercial off-the-shelf applications.
- **Invest in periodic red team exercises**—Red team exercises help validate and improve information security effectiveness against real-world attacks by testing the resilience of the organization's defense capabilities.

5.3.5 Directory Services

A directory service is a database for storing and maintaining information about users and resources. It stores information such as usernames, passwords and user preferences. IT administrators typically use it to onboard users, manage access privileges and monitor and control access to applications and infrastructure resources. For instance, when a user requests access to an application, the application will reference the directory service to ensure the user is legitimate and has the proper privileges. The directory design process typically consists of a set of rules used to determine how network resources are named and identified. Among other requirements, the rules specify that the names be unique and unambiguous.

Domain Name System (DNS) is provided to servers that store the mappings of computer host names and other domain names to IP addresses. A DNS client accesses the DNS server by sending requests about the mappings. Therefore, all of the computing resources (also known as hosts) become clients of the DNS server. The mapping of host names allows users to easily locate computers on a network, using host names rather than complex numerical IP addresses.

Some of the best practices in the administration of directory services are:

- **Implement POLP**—Members of domain administration and other privileged groups have many privileges and typically have access to the entire domain, systems, data and computing devices. The IS auditor should recommend that the organization implement POLP.
- **Remove open access**—Widely used security identifiers—such as Everyone, Authenticated Users and Domain Users—should be removed as they tend to grant inappropriate user privileges to network resources. The use of these security identifiers can allow hackers to exploit the organization's network, as they will have access to a large number of user accounts.
- **Change default passwords**—Default passwords should be changed to reduce the attack surface. The local administrator account is a well-known account among threat actors and often configured with the same password on every computer in the domain and should therefore be disabled.
- **Implement effective password policies**—Having an effective password policy is critical to the security of the directory service. Users change their passwords

©ISACA. All Rights Reserved.

periodically to enhance security. The organization should ideally implement an automated system that controls password generation and maintenance.
- **Implement backup and recovery procedures**—IS auditors should recommend that the organization back up the directory service regularly. The backup procedures should be specified in the disaster recovery/business continuity (DR/BC) plan. At least one domain controller should be backed up. It is advisable to keep backups in several locations.
- **Perform regular monitoring**—The directory service should be regularly monitored for any signs of compromise. Monitoring enables the organization to spot the signs of a breach or compromise. It is a best practice to regularly perform a penetration test to ensure there are no gaps or vulnerabilities in the directory service.
- **Perform regular audits**—It is crucial that the organization audit all changes made to the directory service. All unauthorized changes should be explained. The organization should be in a position to explain the types of changes that were made, identify the personnel who made the changes and provide the time the changes were made, among other audit requests. This information assists in strengthening controls.
- **Educate employees**—Employees pose a serious security risk to the directory service when they unknowingly click on suspicious links. They should be educated to identify phishing attacks and scam emails that trick them into divulging sensitive organizational data.
- **Set up a secure admin workstation (SAW)**—A SAW is a dedicated system that should only be used to perform administrative tasks with privileged accounts. It should not be used for other activities such as checking emails or browsing the Internet.

5.3.6 Identity Governance and Administration

Identity governance is the process of tracking and monitoring user actions on organizational resources. The purpose is to discourage users from abusing their privileges and to find attackers in the network. Identity governance is also important for regulatory compliance, as organizations use user activity data to ensure that their information security policies comply with applicable legal and regulatory frameworks. It is critical for the IS auditor to note that identity governance and administration (IGA) is a subcategory of IAM, making it imperative to include aspects of IGA in the overall IAM audit. However, IGA systems typically provide advanced functionalities beyond standard IAM solutions.

Common IAM challenges addressed by IGA include:
- **Promoting efficient management of user identities**—IGA enables security administrators to efficiently manage user identities and access across the enterprise.
- **Increasing visibility**—IGA improves security administrators' visibility into identities and access privileges and helps them implement the necessary controls to prevent inappropriate or risky access.
- **Streamlining governance and administration**—IGA combines identity governance and identity administration allowing these two aspects to be addressed holistically.
- **Improving user accountability**—With IGA solutions, information security personnel can track, monitor and control user access for both on-premises and cloud-based systems as part of cloud governance efforts.
- **Improving overall security posture**—Information security architects can secure users by ensuring that the right user accounts have the right access to the right systems and detect and prevent inappropriate access.
- **Reducing security risk**—By implementing the right controls with IGA, enterprises can minimize risk and maintain regulatory compliance.
- **Promoting compliance**—Detailed reports and analytics simplify security understanding, allowing security professionals to troubleshoot problems and protect business-critical resources. Data centralization assists in meeting compliance requirements.
- **Improving employee productivity**—With robust IGA solutions, organizations can safely allow and control remote access to maintain business continuity while also preventing breaches. Such flexibility enables employees to work remotely and thus improves their productivity and performance.
- **Enhancing organizational scalability**—IGA solutions support centralized policies and automated workflows that help reduce operational costs, ensure employees can access the resources they need, reduce risk and improve compliance. All these benefits allow the organization to scale effectively.

Elements of IGA

IGA solutions enable organizations to streamline their user identity life cycle management accurately and efficiently. Security administrators can automate the processes of provisioning and deprovisioning user access throughout the entire user access life cycle. To

enable this automation, IGA solutions work with IAM processes. IGA also works with IAM to help information security administrators manage permissions and maintain compliance through accurate reporting. The IS auditor should be able to demarcate elements that constitute identity administration (IA) and elements constituting identity governance (IG) as shown in **figure 5.9**.

Figure 5.9—Elements of Identity Governance Administration

Identity Administration (IA) Elements	Identity Governance (IG) Elements
Connectors: Connectors are implemented to integrate with directories and other enterprise systems that contain user information about users and authorization levels. Connectors create new users and grant them access, leading to identity federation.	**Separation of duties (SoD)**: SoD prevents users from performing two or more duties at a time to reduce collusion. SoD should be implemented within a given application, as well as across multiple systems and IAM applications to enhance security.
Automated workflows: Automated workflows simplify user request processes, allowing security administrators to easily onboard and offboard users, easily determine the levels of access required for particular roles, and approve user access to those roles.	**User access review**: IG solutions can streamline the processes of reviewing and verifying user access to various applications and system resources. They also simplify access revocation when necessary.
Provisioning life cycle management: IA streamlines the process of automated account provisioning, updating and deprovisioning at both the user and application levels.	**Role-based access control (RBAC)**: With RBAC, user access is determined according to user roles. This eliminates unnecessary user access to sensitive data, which in turn increases security and helps prevent breaches.
Entitlement management: With entitlement management, information systems (IS) security administrators can specify the entitlements allowed to users in various applications and systems. For example, some users may be allowed to add or edit data while others are only allowed to view the data.	**Analytics and reporting:** IG solutions provide visibility to user activities and enable IS professionals to identify security issues or risk and respond instantly. The analytics component can also be used to start remediation processes, address security policy violations and generate security compliance reports.

5.3.7 Identity as a Service

Identity as a service (IDaaS) refers to IAM services provided through the cloud on a subscription basis. IDaaS is typically fully on-premises and provided via a set of software and hardware. An identity service stores the information linked with a digital entity in a form that can be managed and queried for further use in electronic transactions. IDaaS solutions, in which a third party delivers cloud-based IAM services and tools, are also gaining popularity. Organizations typically outsource important but time-consuming tasks like creation of new user accounts, authentication of access requests, and identity governance. For greater security effectiveness, an IDaaS solution should support:

- SSO
- MFA
- User identity management
- Access provisioning capabilities
- Cloud directory services

Benefits of IDaaS

The continued growth and popularity of digital services has led to the widespread use of IDaaS solutions. IDaaS offers several benefits to organizations, and it is important for the organization to choose the risk provider for IDaaS. The IS auditor plays an important role in advising the organization's management on the benefits and pitfalls of IDaaS. Some of the benefits of IDaaS implementation in the organization are:

- **Reduced costs**—IDaaS can result in significant cost savings in terms of hardware, software and maintenance expenses.
- **Improved security**—IDaaS provides a more secure environment for managing user identities and access. It offers advanced authentication methods, such as MFA, which can enhance security and reduce the risk of data breaches through compromised credentials, for example.
- **Scalability**—IDaaS is designed to scale easily and accommodate a large number of users and resources. Scalability makes it easier to manage user identities and access as organizations grow and expand.

©ISACA. All Rights Reserved.

- **Flexibility**—IDaaS offers a flexible solution that can be customized to meet the specific needs of an organization and adapt to changing or new user needs. IDaaS flexibility includes providing options for integrating with other cloud-based services and on-premises applications.
- **Simplified identity management**—IDaaS provides a centralized interface that enables organizations to manage user identities and access from a single location. This simplifies the management of user identities and access across different applications and services.

Risk of IDaaS

Some of risk associated with IDaaS includes:

- **Dependence on Internet connectivity**—IDaaS relies on Internet connectivity, which means that organizations may experience disruptions in service if there are issues with the Internet connection or if the SP experiences downtime. Put simply, no Internet connectivity means no account provisioning or deprovisioning takes place.
- **Limited customization**—While IDaaS offers some flexibility, it may not be as customizable as an on-premises solution, which may limit an organization's ability to configure the service to meet specific needs or integrate with certain applications.
- **Security concerns**—IDaaS involves transferring sensitive user identity and access information to a third-party SP. This raises concerns about data security and privacy, as the SP may be a target for information security attacks, or its security practices may not be as stringent as the organization itself.
- **Regulatory compliance**—Organizations may face regulatory compliance issues when using IDaaS, particularly if they operate in industries with strict data privacy regulations. The use of third-party SPs may require additional compliance measures to ensure the security and privacy of sensitive information.
- **Integration challenges**—Integrating IDaaS with existing systems and applications may be challenging, particularly if the systems and applications were not designed with cloud-based IAM in mind.

IDaaS Best Practices

To effectively manage the risk related to IDaaS and ensure satisfaction of their security and compliance risk profiles, organizations should implement IDaaS best practices. Some best practices for IDaaS[36] are:

- **Obtain senior management buy-in**—Before implementing IDaaS solutions in an organization, the IS auditor should ensure that management understands the benefits and risk of IDaaS and is committed to its implementation. IDaaS is a paid subscription service, so funds need to be allocated to continue using it.
- **Conduct due diligence on the IDaaS solution provider**—An organization should conduct due diligence on the IDaaS vendor, covering such aspects as pricing, reputation security options, efficiency in deployment and customer support. The best solution for the organization's objectives should be chosen.
- **Implement strong authentication**—SSO and MFA are typical authentication controls that deliver added layers of protection in an IDaaS solution that can further strengthen the security posture of the organization.
- **Implement log management**—The implementation of logging and log management processes allows for the prompt detection of security incidents. An IDaaS solution can leverage intelligent advanced analytics capabilities for insights on the use of access privileges.
- **Train and develop employees**—Training and development improves the likelihood that employees will follow all precautions required in the management of the IDaaS solution and that they will properly manage user identities and access to the applications and data. Training can include sessions on password management, access control policies and security awareness.
- **Implement DR/BC plans**—In case of any downtime or any disaster, the IDaaS solution should be able to recover and continue operating. A DR/BC plan should be available to provide certainty that data and access controls will continue being operational.

5.3.8 System Access Permission

System access permission is the prerogative to act on a computer resource. This usually refers to a technical privilege, such as the ability to read, create, modify or delete a file or data; execute a program; or open or use an external connection.

[36] Roy, A.; "Identity as a Service Audit Implications and Best Practices," ISACA Now Blog, 23 May 2023, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/identity-as-a-service-audit-implications-and-best-practices*

System access to computerized information resources is established, managed and controlled at the physical and/or logical level. See section 5.2 Physical and Environmental Controls for more information on physical controls.

Logical system access controls restrict the logical resources of the system (e.g., transactions, data, programs, applications, etc.) and are applied when the subject resources are needed. It is possible to determine if requested access is to be allowed by analyzing individual security profiles and resources. Controls may be built into the OS and invoked through separate access control software.

Physical or logical system access to any computerized information should be on a documented need-to-know basis that applies least privilege. Other considerations for granting access are accountability and traceability. These principles should be used by IS auditors when they evaluate the appropriateness of criteria for defining permissions and granting security privileges.

The IT assets under logical security can be grouped into four layers—networks, platforms, databases and applications. The concept of layered security for system access provides greater scope and granularity of control to information resources. For example, network and platform layers provide pervasive general systems control over user authentication into systems, system software and application configurations, data sets, load libraries and any production data set libraries. Database and application controls generally provide a greater degree of control over user activity within a particular business process by controlling access to records, specific data fields and transactions.

To safeguard information resources under their control, information owners or managers responsible for the accurate use and reporting of information should provide written authorization when granting access to users or defined roles. Managers should give this documentation to security administrators to ensure that mishandling or alteration of authorizations does not occur.

Logical access capabilities are implemented by security administrators in a set of access rules that stipulate which users (or groups of users) are authorized to access a resource at a particular level (e.g., read-, update- or execute-only) and under which conditions (e.g., time of the day or a subset of computer terminals). The security administrator invokes the appropriate system access control mechanism upon receipt of a proper authorization request from an information owner or manager to grant a specified user the rights to access or use a protected resource.

Access authorization should be evaluated regularly to ensure that it remains valid. Personnel and departmental changes, malicious efforts and carelessness can result in authorization creep and can impact the effectiveness of access controls. Often, access is not removed when personnel leave an organization, thus increasing the risk of unauthorized access. For this reason, the information asset owner should review access controls periodically with a predetermined authorization matrix that defines the least-privileged access level and authority for an individual/role with reference to job roles and responsibilities. Any access exceeding the access philosophy in the authorized matrix or in the actual access levels granted on a system should be updated and changed accordingly. A good practice is to integrate the review of access rights with human resource processes. When an employee transfers to a different function (e.g., due to promotion, lateral transfer or demotion), access rights are adjusted at the same time. Development of a security-conscious culture increases the effectiveness of access controls.

Nonemployees with access to corporate IS resources should be held responsible for security compliance and be accountable for security breaches. Nonemployees include contract employees, vendor programmers/ analysts, maintenance personnel, clients, auditors, visitors and consultants.

5.3.9 Types of Access Controls

Access control describes a variety of protection mechanisms to prevent unauthorized access to a computer system or network. Access controls can be implemented in several ways and the effectiveness of a control depends on the data regulations set by the company. **Figure 5.10** shows types of access controls.

©ISACA. All Rights Reserved.

Figure 5.10—Types of Access Controls

Access Control	Description
Mandatory access control (MAC)	MACs are logical access control filters used to validate access credentials that cannot be controlled or modified by normal users or data owners; they act by default. MAC can be carried out by comparing the sensitivity of the information resources—such as files, data or storage devices—or a MAC can be kept on a user-unmodifiable tag attached to the security object with the security clearance of the accessing entity, such as a user or an application. With MACs, only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy. MACs are prohibitive; anything that is not expressly permitted is forbidden. Thus, MACs are typically reserved for environments in which particularly sensitive information is used.
Discretionary access control (DAC)	DACs are a protection that may be activated or modified at the discretion of the data owner, such as with data owner-defined sharing of information resources, where the data owner may select who will be permitted to access the resource and determine the security level of the access. DACs cannot override MACs; DACs act as an additional filter, further prohibiting access with the same exclusionary principle. When information systems (IS) enforce MAC policies, the systems must distinguish between MAC and the discretionary policies that offer more flexibility. This distinction must be ensured during object creation, classification downgrading and labeling.
Rule-based access control (RuBAC)	With the RuBAC model, access rules are predefined, typically through an access control list (ACL), and constantly evaluated to determine access permissions. RuBAC defines specific and detailed situations in which a subject can or cannot access an object and specifies what the subject can do once access is granted. The rules are enforced equally for all users, as with firewall rules, for example. RuBAC provides a simple and direct way of managing access control permissions. The challenge is that the approach is a very complex and unproductive control when access is managed at a more granular level.
Role-based access control (RBAC)	RBAC bases access restriction on user roles. Custom roles are usually created, and access is revoked when no longer needed. RBAC is a common access control method. For example, one role might be an IS Auditor. Upon joining the organization, a new IS auditor is added to the role group and given the same access rights immediately. RBAC is generally considered an industry-standard good practice and is in widespread use throughout organizations.
Attribute-based access control (ABAC)	ABAC governs access based on user attributes, resource of object attributes and environmental attributes. Many organizations use attributes to store data about users, such as their department, cost center, manager, location, employee number and date of assumption of duty. These attributes can be used to automate authorization and make it more secure. For example, an authorization might be configured to allow only users who have "Tokyo" as their office location to use the wireless network at the Tokyo office.
Policy-based access control (PBAC)[37]	PBAC is a strategy for managing user systems access that combines users' business roles with policies to determine which access privileges each user role should have. PBAC uses policy guidance to determine which access role each person must have in organizational systems. For instance, the information security policy may state that a user who remotely logs in with the proper credentials can access a specific file folder.

[37] NIST Computer Security Resource Center, "Glossary," *https://csrc.nist.gov/glossary*

5.3.10 Information Security and External Parties

The security of the organization's information and information processing facilities that are accessed, processed, communicated to or managed by external parties should be maintained and should not be reduced by the introduction of external party products or services. Any access to the organization's information processing facilities and processing and communication of information by external parties should be controlled. Controls should be agreed to and defined in an agreement with the external party. Organizations should have the right to audit the implementation and operation of the resulting security controls. Such agreements can help reduce the risk associated with external parties.

Identification of Risk Related to External Parties

The risk to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before access is granted. If there is a need to allow an external party access to the information processing facilities or information of an organization, a risk assessment should be carried out to identify any requirements for specific controls. The identification of risk related to external party access should consider the issues depicted in **figure 5.11**.

Figure 5.11—Risk Related to External Party Access

- The information processing facilities an external party is required to access
- The type of access the external party will have to the information and information processing facilities:
  - Physical access (e.g., to offices, computer rooms and filing cabinets)
  - Logical access (e.g., to an organization's databases and information systems [IS])
  - Network connectivity between the organization and the external party networks (e.g., permanent connection and remote access)
- Whether the access takes place onsite or offsite
- The value and sensitivity of the information involved and its criticality for business operations
- The controls necessary to protect information that is not intended to be accessible by external parties
- The external party personnel involved in handling the organization's information
- How the organization or personnel authorized to have access can be identified, the authorization verified, and how often it needs to be reconfirmed
- The different means and controls employed by the external party when storing, processing, communicating, sharing, exchanging and destroying information
- The impact of access not being available to the external party when required and the external party entering or receiving inaccurate or misleading information
- Practices and procedures to deal with information security incidents and potential damages and the terms and conditions for the continuation of external party access in the case of an information security incident
- Legal and regulatory requirements and other contractual obligations relevant to the external party that should be taken into account
- How the interests of any other stakeholders may be affected by the arrangements

Access by external parties to the organization's information should not be provided until the appropriate controls have been implemented and, when feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. Generally, all security requirements resulting from work with external parties or internal controls should be reflected in the agreement with the external party.

There should be confirmation that the external party is aware of its obligations and accepts the responsibilities and liabilities involved in accessing, processing, communicating or managing the organization's information and information processing facilities.

External parties might put information at risk if their security management is inadequate. Controls should be identified and applied to administer external party access to information processing facilities. For example, if there is a special need for confidentiality, nondisclosure agreements might be used. Organizations may face risk associated with interorganizational processes, management and communication if a high degree of

©ISACA. All Rights Reserved.

outsourcing is applied or if several external parties are involved.

Addressing Security When Dealing With Customers

All identified security requirements should be addressed before giving customers access to the organization's information or assets.

Figure 5.12—Customer Access Security Considerations

- Description of the product or service to be provided
- Reasons, requirements and benefits associated with customer access
- Arrangements for reporting, notification and investigation of information inaccuracies (e.g., of personal details), information security incidents and security breaches
- The target level of service and unacceptable levels of service
- The right to monitor and revoke any activity related to the organization's assets
- The respective liabilities of the organization and the customer
- Responsibilities with respect to legal matters and legal requirements (e.g., data protection legislation); consideration of different national legal systems if the agreement involves cooperation with customers in other countries
- Intellectual property rights, copyright assignment and protection of collaborative work

In addition to asset protection and access control policies, **figure 5.12** describes customer access security considerations.

The security requirements related to customers accessing organizational assets can vary considerably depending on the information processing facilities and information being accessed. Security requirements can be addressed through customer agreements that contain all identified risk and security requirements.

Addressing Security in Third-Party Agreements

Third-party agreements involving accessing, processing, communicating or managing the organization's information or information processing facilities or adding products or services to information processing facilities should cover all relevant security requirements. The agreement should ensure that there is no misunderstanding between the organization and the third party. The organization should ensure that the agreement includes adequate indemnification provisions to protect against potential losses caused by the actions of the third party.

Figure 5.13 describes recommended contract terms to include in third-party agreements.

In general, it is very difficult to ensure the return or destruction of confidential information disclosed to a third party at the end of an agreement. To prevent unauthorized copies or use, printed documents should be consulted on site. Technical controls should be considered to set up the desired constraints, such as the printing or copying of the document, individuals authorized to read it, or requirements for using it after a certain date.

The agreements can vary considerably for different organizations and among different types of third parties. Therefore, care should be taken to include all identified risk and security requirements in agreements. If necessary, the required controls and procedures can be expanded in a security management plan.

Figure 5.13—Recommended Contract Terms for Third-Party Agreements

- Compliance with the organization's information security policy by the third party
- Controls to ensure asset protection, including:
  - Procedures to protect organizational assets, including information, software and hardware
  - Any required physical protection controls and mechanisms
  - Controls to ensure protection against malicious software
  - Procedures to determine whether any compromise of the assets (e.g., loss or modification of information, software and hardware) has occurred
  - Controls to ensure the return or destruction of information and assets at the end of or at an agreed point in time
  - Confidentiality, integrity, availability and any other relevant property of the assets
  - Restrictions on copying and disclosing information and using confidentiality agreements
- User and administrator training in methods, procedures and security
- A means to ensure user awareness of information security responsibilities and issues
- Provision for the transfer of personnel, if appropriate
- Responsibilities regarding hardware and software installation and maintenance
- A clear reporting structure and agreed-upon reporting formats
- A clear and specified process for change management
- An access control policy, covering:
  - The reasons, requirements and benefits that make access by the third party necessary
  - Permitted access methods and the control and use of unique identifiers such as user IDs and passwords
  - An authorization process for user access and privileges
  - A requirement to maintain a list of individuals authorized to use the services made available and to specify their rights and privileges
  - A statement that all access not explicitly authorized is forbidden
  - A process for revoking access rights or interrupting the connection between systems
- Arrangements for the reporting, notification and investigation of any information security incidents and security breaches or violations of the requirements stated in the agreement
- A description of the product or service to be provided and a description of the information to be made available, along with its security classification
- The target level of service and unacceptable levels of service
- The definition and means of monitoring and reporting verifiable performance criteria
- The right to monitor and revoke any activity related to the organization's assets
- The right-to-audit responsibilities defined in the agreement, the right to have those audits carried out by a third party and to enumerate the statutory rights of auditors (and, if appropriate, the provision of a service auditor's report)
- The establishment of an escalation process for problem resolution
- Service continuity requirements, including measures for availability and reliability, in accordance with the organization's business priorities
- The respective liabilities of the parties to the agreement
- Responsibilities for ensuring that legal requirements are met (e.g., data protection legislation), and for considering different national legal systems if the agreement involves cooperation with organizations in other countries
- Intellectual property rights and copyright assignment and protection of any collaborative work
- Involvement of the third party with subcontractors, and the security controls the subcontractors need to implement
- Conditions for renegotiation/termination of agreements, such as:
  - A contingency plan in case either party wishes to terminate the relationship before the agreement ends
  - A provision for renegotiation of the agreement if the security requirements of the organization change
- Current documentation of asset lists, licenses, agreements or rights relating to them
- Non-assignability of the contract

If information security management is outsourced, agreements should address how the third party will guarantee that adequate security, as defined by the risk assessment, will be maintained and how security will be adapted to identify and deal with changes to risk. Some of the differences between outsourcing and the

©ISACA. All Rights Reserved.

other forms of third-party service provision include the question of liability, planning the transition period, planning for potential disruption of operations during the transition period, contingency planning arrangements, due diligence reviews, and collection and management of information on security incidents. Therefore, it is important for the organization to plan and manage the transition to an outsourced arrangement and have suitable processes in place to manage changes and the renegotiation/termination of agreements.

The procedures for continuation of processing if the third party becomes unable to supply its services need to be considered in the agreement to avoid any delay in arranging replacement services. Agreements with third parties may also involve other parties. Agreements granting third-party access should include allowance for designation of other eligible parties and conditions for their access and involvement. A requirement for the third party to have certified compliance with recognized security standards (e.g., International Organization for Standardization (ISO) 27001 and Service Organization Control Type 2 [SOC 2]) may need to be considered.

Generally, agreements are developed primarily by the organization. There may be occasions in some circumstances where an agreement may be developed and imposed upon an organization by a third party. The organization needs to ensure that its own security is not unnecessarily impacted by third-party requirements stipulated in imposed agreements.

Agreements with external parties may also involve other parties. Agreements granting an external party access should include an allowance for designation of other eligible parties and conditions for their access and involvement.

5.3.11 Digital Rights Management

Digital rights management (DRM) consists of a set of hardware and software technologies designed to control how content and information assets are used and to protect copyrights for digital media. DRM includes technologies that limit the copying and use of copyrighted works and proprietary software. DRM allows publishers or authors to control what paying users can do with their works while allowing digital content to be monetized more efficiently. For companies, implementing DRM or related processes can help to prevent users from accessing or using certain assets, allowing the organization to avoid legal issues that arise from unauthorized use and eliminating the risk of third parties not following best practices for data security, leaving partner organizations exposed. DRM solutions can be integrated with data loss prevention (DLP) solutions to assist organizations in protecting sensitive information. With this arrangement, the DLP solution detects any unauthorized access while the DRM denies such access in a seamless fashion. See section 5.5 Data Loss Prevention for more information.

DRM can be implemented on:

- Copyrighted content (e.g., audio, images, over-the-top [OTT] media)
- Copyrighted software (e.g., OSs, applications)
- Confidential documents (e.g., bank statements, company financial statements)
- Intellectual property assets (e.g., product plans, patents)
- Government documents (e.g., policy documents)
- Literature (e.g., online libraries, e-book stores)

DRM Restrictions

The IS auditor should assess DRM processes in the organization and provide necessary assurance. **Figure 5.14** shows the most common DRM restrictions.

 ©ISACA. All Rights Reserved.

Figure 5.14—Digital Rights Management Restrictions

Restriction	Description
Copy restriction	Copy restriction allows users to view content from the primary channel, such as a website or streaming platform, but prevents them from making copies. Users may be allowed to make a certain number of copies under certain conditions. For example, a user might be allowed up to five copies of an e-book. The restriction may further specify the use of the copies, for example, copies may be allowed for educational purposes but not for commercial purposes.
Edit restriction	Edit restriction prevents users from editing or saving content, thereby maintaining the content integrity. It ensures that the author's ideas remain original and are not altered in any way.
Share restriction	Share restriction prevents users from sharing or forwarding content or products without permission from the owner. It controls unintended proliferation of content.
Print restriction	Depending on organizational preferences, print restriction can prevent users from printing whole content or may specify that the content may only be printed up to a limited number of times.
Location restriction	Location restriction locks access to certain Internet Protocol (IP) addresses, locations or devices. For example, if content is only available to residents of Asia, then it will not be accessible to people on other continents.
Expiration data setting	The expiration date setting specifies when access will be revoked, thus encouraging timely consumption of the content.

DRM Technologies

The IS auditor should provide assurance that the correct DRM technologies are used by the organization and help achieve its objectives. Some commonly used DRM technologies include:

- **Password protection**—Password protection is simple and cheap but is a very effective DRM technique. Only the user knows the unique password necessary to access content. This type of DRM is frequently used by financial services providers, such as banks, to keep consumer transactions safe. However, when this technique is preferred, it is crucial to adhere to good password practices.
- **Digital watermarking**—Digital watermarking is a form of steganography that prevents users from reusing visual content as their own. Steganography is a technique used to hide data within an ordinary file such as a picture. Watermarking content is generally used to establish ownership, allowing users to access content libraries without using them for commercial purposes.
- **Device control**—Device control is an advanced DRM solution that prevents users from opening a file if they are not using an approved device. Businesses typically rely on device control DRM. For example, device manufacturers may be compelled to obtain DRM certification from Netflix to run its streaming videos on their devices.
- **Restrictive licensing**—With restrictive licensing, the content provider creates a license that legally prevents the use of content for certain purposes. However, restrictive licensing is not a control. For example, if commercial purpose use were restricted, it might still be possible to use the content for a commercial purpose, but anyone who did so would be legally liable for violating the licensing restriction.
- **Digital trust infrastructure**—Digital trust infrastructure relies on the trust the user and content provider have in the underlying technology. It gives users the autonomy to extensively explore content while the content provider retains control. This is the technique applied in blockchain technology.
- **Hashing**—Hashing is a cryptography technique that prevents content manipulation by taking digital content as the input and generating a final output message for user consumption. If the input content is altered, the output message will change, proving that the content is not authentic. This technique is used to verify that digital content is genuine and free from tampering.
- **Secure communication protocols**—Secure communication protocols such as Transport Layer Security (TLS) maintain the security of information flowing through the Internet. They act as DRM staples and should form a part of DRM technology. Many organizations embed encryption technologies into digital content to restrict access or use.
- **Timebound decryption keys**—Timebound decryption keys can be used to protect digital rights. The decryption will be set to only allow users to decrypt content for a specific period. For example,

©ISACA. All Rights Reserved.

if an organization buys a commercial video, it might be granted only one month of access, beyond which further access will require payment of a fee.

Best Practices for DRM

Some best practices for DRM include:

- **Perform a DRM content inventory**—An inventory of all content, clearly specifying the type of content that is rights-managed and free, is critical. The organization should specify and understand the origins of the content rights.
- **Adopt a risk-based approach**—An organization should select content for DRM based on risk levels, as not all content requires DRM. If not carefully planned, some DRM measures can prevent content from achieving the desired reach and engagement level.
- **Maximize utilization of DRM tools**—Numerous free DRM tools are available for an organization to use before determining if premium tools are appropriate.
- **Obtain employee buy-in**—It should be clear to employees that the implementation of DRM is more about securing data than restricting access. That way it is easier to obtain their buy-in and active support for DRM implementations.
- **Integration with other data management infrastructure**—DRM typically works best when integrated with associated solutions. For example, the DRM can be integrated with a DLP tool; a DLP tool will restrict data sharing to prevent leakage while a DRM enforces protocols when sharing data within the confines of the DLP territory.
- **Minimize Shadow IT**—Shadow IT and unmapped distribution channels make the process of data sharing and utilization difficult by hiding data. Reducing shadow IT can help reduce the burden of implementing a DRM in the organization.
- **Automate the DRM process**—A manual DRM is not scalable and adaptable to the changing needs of the digital content environment. The IS auditor should advise on the need for the organization to automate the DRM process.

5.3.12 Logical Access

Logical access is the ability to interact with computer resources granted using identification, authentication and authorization. Logical access controls are the primary means used to manage and protect information assets. They enact and substantiate management-designed policies and procedures intended to protect assets. The controls are designed to reduce risk to a level acceptable to an organization. IS auditors who understand this relationship should be able to analyze and evaluate the effectiveness of a logical access control in accomplishing information security objectives and avoiding negative consequences resulting from exposures, which can range from minor inconveniences to a total shutdown of computer functions with associated losses.

Logical Access Exposures

Technical exposures exist due to accidental or intentional exploitation of logical access control weaknesses. Intentional exploitation of technical exposures might lead to computer crime. However, not all computer crimes exploit technical exposures. Technical exposures are the unauthorized activities interfering with normal processing, such as implementation of software or modification of data, locking or misusing user services, destroying data, compromising system usability, distracting processing resources or spying on data flow or user activities at either the network, platform (OS), database or application level. Technical exposures include:

- **Data leakage**—Siphoning or leaking information out of the computer. This can involve dumping files to paper or can be as simple as stealing computer reports and tapes. Unlike product leakage, data leakage leaves the original copy, so it may go undetected.
- **Computer shutdown**—Initiated through terminals or personal computers connected directly (online) or remotely (via the Internet) to the computer. Usually, only individuals who know a high-level logon ID can initiate the shutdown process, but this security measure is effective only if proper security access controls are in place for the high-level logon ID and the telecommunications connections into the computer. Some systems have proven to be vulnerable to shutting themselves down under certain conditions of overload.

Familiarization With the Enterprise's IT Environment

To effectively assess logical access controls within their organization, IS auditors first need to gain a technical and organizational understanding of the IT environment. The purpose is to determine, from a risk standpoint, which areas warrant IS auditing attention in planning current and future work. This includes reviewing the network, OS platform, database and application security layers associated with the organization's IT information systems architecture.

 ©ISACA. All Rights Reserved.

Paths of Logical Access

Access to an organization's IS infrastructure can be gained through several points of entry. Each avenue is subject to appropriate levels of access security. A direct path of access (such as a PC terminal user tying directly to a mainframe) is available when the IS environment is under direct control of the main system and when the users are locally known individuals with well-defined access profiles. Direct access related to a LAN is more complex, given that many specific IS resources are tied to a common linking structure. These resources may have different access paths/levels that normally are mediated through LAN connectivity, and the network itself is considered an important IS resource at a higher access level.

A combination of direct, local network and remote access paths is the most common configuration. Complexity is increased by several intermediate devices that act as security doors among the various environments. The need to cross low-security or totally open IT spaces, such as the Internet, also necessitates increased complexity. An example of an access path through common nodes is a back-end or front-end interconnected network of systems for internally or externally based users. Front-end systems are network-based systems connecting an organization to outside, untrusted networks, such as corporate websites, where a customer can access the website externally to initiate transactions that connect to a proxy server application. The proxy server application connects to a back-end database system to update a customer database. Front-end systems can also be internally based to automate paperless business processes that tie into back-end systems in a similar manner.

General Points of Entry

General points of entry to either front-end or back-end systems control access from an organization's networking or telecommunications infrastructure to its information resources (e.g., applications, databases, facilities and networks). The approach followed is based on a client-server model. A large organization can have thousands of interconnected network servers. Connectivity in a large enterprise environment needs to be controlled through a smaller set of primary domain controllers (servers), which enable users to obtain access to specific secondary points of entry (e.g., application servers and databases).

General modes of access into this type of infrastructure occur through:

- **Network connectivity**—Access is gained by linking a PC to a segment of an organization's network infrastructure, either through a physical or a wireless connection. At a minimum, such access requires user I&A to a domain-controlling server. More specific access to a particular application or database may require that users identify and authenticate themselves to that particular server (secondary point of entry). Other modes of access to the infrastructure can occur through network management devices, such as routers and firewalls, which should be strictly controlled.
- **Remote access**—Users connect remotely to an organization's server, which generally requires users to identify and authenticate themselves to the server for access to specific functions that can be performed remotely (e.g., email, File Transfer Protocol [FTP] or some application-specific function). Complete access to view all network resources usually requires a virtual private network (VPN), which allows secure authentication and connection to resources if privileges have been granted. Remote APs of entry can be extensive and should be centrally controlled when possible.

From a security standpoint, it is incumbent upon the organization to know all the points of entry into its information resource infrastructure, which, in many organizations, will not be a trivial task (e.g., thousands of remote access users). This is significant because any point of entry that is not appropriately controlled can potentially compromise the security of an organization's sensitive and critical information resources. When performing detailed network assessments and access control reviews, IS auditors should determine whether all points of entry are known, and they should support management's effort in obtaining the resources to identify and manage all access paths.

5.3.13 Access Control Software

IT has made it possible for computer systems to store and contain large quantities of sensitive data, increase the capability of sharing resources from one system to another and permit many users to access systems through Internet/intranet technologies. All these factors have made organizations' IS resources more widely and promptly accessible and available.

The purpose of access control software is to prevent unauthorized access and modification to an organization's sensitive data and misuse of system-critical functions.

©ISACA. All Rights Reserved.

To achieve this goal, access controls should be applied across all layers of an organization's IS architecture, including networks, platforms or OSs, databases and application systems. Each of them layer usually features some form of I&A, access authorization, checking of specific information resources and logging and reporting of user activities.

The greatest degree of protection in applying access control software against internal and external users' unauthorized access is at the network and platform/OS levels. These systems, also referred to as general support systems, make up the primary infrastructure on which applications and database systems reside.

OS access control software is typically restricted to privileged users. It interfaces with network access control software and usually resides on network layer devices (e.g., routers and firewalls) that manage and control external access to organizations' networks. Additionally, OS access control software interfaces with database and/or application system access controls to protect system libraries and user data sets.

General operating and/or application system access control functions include:

- Create or change user profiles.
- Assign user I&A.
- Apply user logon limitation rules.
- Ensure user access is commensurate with job responsibilities.
- Ensure notification concerning proper use and access prior to initial login.
- Create individual accountability and auditability by logging user activities.
- Establish rules for access to specific information resources (e.g., system-level application resources and data).
- Log events.
- Report capabilities.

Database and/or application-level access control functions include:

- Create or change data files and database profiles.
- Verify user authorization at the application and transaction level.
- Verify user authorization within the application.
- Verify user authorization at the field level for changes within a database.
- Verify subsystem user authorization at the file level.
- Log database/data communications access activities for monitoring access violations.

Access control software is provided at different levels within an IS architecture, with each level providing a certain degree of security. Properties of such relationships are that upper layers (applications and databases) are dependent on lower, infrastructure-type layers to protect general system resources. Upper layers provide the granularity needed at the application level in separating duties by function.

5.3.14 Logon IDs and Passwords

Logon IDs and passwords are the components of a user I&A process, where the authentication is based on something you know. The computer can maintain an internal list of valid logon IDs and a corresponding set of access rules for each logon ID. These access rules are related to computer resources. As a minimum requirement, access rules are usually specified at the OS level (controlling access to files) or within individual application systems (controlling access to menu functions and types of data or transactions).

The logon ID should be restricted to providing individual but not group identification. If a group of users is to be formed for interchangeability, the system usually offers the ability to attach a logon ID to a named group with common rights. Each user gets a unique logon ID that can be identified by the system. The format of logon IDs is typically standardized.

Features of Passwords

A password provides individual authentication. It should be easy for the user to remember but difficult for an intruder to determine. The minimum password length largely depends on the threat model being addressed.[38] For example, passwords in online environments that are too short are prone to brute force and dictionary attacks.

Initial passwords may be allocated by the security administrator or generated by the system itself. When the user logs on for the first time, the system should force a password change to improve confidentiality. Initial password assignments should be randomly generated. The ID and password should be communicated in a controlled manner to ensure that only the appropriate user receives the information. New accounts without an initial password assignment should be suspended.

If the wrong password is entered a predefined number of times, the logon ID should be automatically locked out. Locking-out may be made permanent (only the administrator may unlock the ID) or temporary (the

[38] See Appendix A of *https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf* for more information.

system automatically unlocks the ID after a system-specified time period).

Users who have forgotten their password must notify a security administrator—the only person with sufficient privileges to reset the password and/or unlock the logon ID. The security administrator should reactivate the logon ID only after verifying the user's identification (challenge/response system). To verify, the security administrator should return the user's call after verifying the extension or calling the user's supervisor for verification.

Passwords should be hashed (a type of one-way encryption) and stored using a sufficiently strong algorithm. This allows checking passwords without the need to record them explicitly. To reduce the risk of an intruder gaining access to other users' logon IDs, passwords should not be displayed in any form. Passwords are normally masked on a computer screen, and they are not shown on computer reports. Passwords should not be kept on index or card files or written on pieces of paper taped somewhere near the computer or inside a person's desk.

Passwords should be changed on a regular basis (e.g., every 30 days). The frequency depends on many factors, including the criticality of the information access level, the nature of the organization, the IS architecture and the technologies used. Users, not administrators, should change their passwords at their computers, rather than at any location where the new password might be observed. The best method is to force the change by notifying the user prior to the password expiration date. The risk of allowing voluntary password changes is that users will not change their passwords unless forced to do so. Password management is stronger if a history of previously used passwords is maintained by the system and their reuse prohibited for a period—such as no reuse of the last 12 passwords is permitted.

A password for a logon ID should only be known by the individual user; if a password is known to more than one person, the accountability of the user for all activity within the account cannot be enforced.

Special treatment should be applied to supervisor or administrator accounts. These accounts frequently allow full access to the system. Normally there is a limited number of such accounts per system/authentication level. For accountability, the administrator password should be known only by one individual. On the other hand, the organization should be able to access the system in an emergency when the administrator is not available. To enable this, special backup practices should be implemented, such as keeping the administrator password in a sealed envelope in a locked cabinet available only to senior management. This is sometimes referred to as a firecall ID.

All of these guidelines should be formalized in a password policy, and reading and acknowledging the policy should be mandatory. An acceptable use policy should include the requirement to follow the policy.

Password Attacks

Passwords are a popular access verification solution for most organizations so figuring out a target's password is an attractive proposition to most attackers. Attackers can carry out password attacks in various ways. **Figure 5.15** provides an overview of the common password attacks IS auditors should be aware of.

Figure 5.15—Common Password Attacks

Type of Attack	Description of Attack
Password sniffing	This is a passive form of password attack in which an attacker attempts to intercept network transmissions to obtain passwords that are not encrypted by the network security technologies. Attackers can also use social engineering techniques to trick victims into providing their passwords, ostensibly to solve a critical problem. Attackers can also simply guess users' passwords, particularly default passwords. This is why default passwords should always be changed.
Phishing	Attackers can use social engineering techniques to trick victims into providing their passwords, ostensibly to solve critical problems. Attackers can also simply guess users' passwords, particularly default passwords. This is why default passwords should always be changed.

©ISACA. All Rights Reserved.

Figure 5.15—Common Password Attacks (cont.)

Type of Attack	Description of Attack
Brute-force attack	A brute-force password attack uses basic information about individuals or their job titles to guess passwords. For example, usernames, birthdates, anniversary dates or other personal but easy-to-discover details can be used in different combinations to decipher passwords. This information is mostly obtained from social media platforms. Humans are the weakest link in the security chain. In many cases an individual's hobbies, names of children or other relatives are used to create passwords, making it easy for attackers to guess them.
Dictionary attack	A dictionary attack is a technique in which the attacker uses common words and phrases, such as those listed in a dictionary, to guess a target's password. An effective method of preventing brute-force and dictionary password attacks is to set up a lockout policy. This automatically prohibits access to organizational systems after a certain number of failed attempts. Thus, the attacker can only make a few attempts before getting locked out.
Keylogger attack	Keylogger or keystroke logger attacks are very risky, as even the strongest passwords fail to provide adequate protection against them. They arise when attackers spy on targets and record their passwords as they type them. They are usually successful in that they are very accurate and there is no need to guess passwords. The information systems (IS) auditor should be aware that once keyloggers have infected a system, detection is difficult. For this reason, IS audit should advise on prevention as the best defense against keylogger attacks.
Rainbow attack	A rainbow table looks for matches in a pre-computed list of hash functions that are stored alongside their hashed values. An attacker compares values against this table and decrypts the hashed passwords in the organization's database. It is crucial for the IS auditor to note that rainbow tables containing the solutions to common hashing algorithms are widely available on the dark web. Salting can help mitigate rainbow attacks.
Credential stuffing attack	Credential stuffing is a form of attack that exploits the human tendency to reuse passwords. An attacker attempts various combinations of stolen usernames and passwords with the hope of gaining access to an account owned by the target who has reused a compromised password. These stolen passwords are usually available from the dark web. Attackers can also reuse passwords stolen by any other means to carry out credential stuffing attacks. To mitigate this type of attack, users should be educated on the dangers of reusing passwords.
Password spraying attack	Password spraying attacks are similar to dictionary attacks and brute force attacks except that password spraying typically targets several users (even millions) at once, hence the use of "spraying" in the name. This attack usually targets single sign-on (SSO) and cloud-based IS platforms. Distributing login attempts across multiple users lessens the risk of an attacker being caught when repeated failed login attempts trigger account lockout policies.

Login ID and Password Good Practices

Logon ID requirements include:

- Logon ID syntax should follow an internal naming rule; however, this rule should be kept as confidential as the IDs themselves.
- Default system accounts—such as Guest, Administrator and Admin—should be renamed or disabled whenever technically possible.
- Logon IDs not used after a predetermined period of time should be deactivated to prevent possible misuse. This can be done automatically by the system or manually by the security administrator.
- The system should automatically disconnect or lock a logon session if no activity has occurred for a period of time. This reduces the risk of misuse of an active logon session left unattended because the user went to lunch, left for home, went to a meeting or otherwise forgot to log off. This is often referred to as a session timeout. Regaining access should require the re-entry of the authentication method, password, token, etc.

At a minimum, these rules should be applied to individuals with privileged system account authority (e.g., system administrators, security administrators) versus general users. Users with privileged authority need access to establish and manage appropriate system configurations. However, such privileges enable the user to bypass any access control software restrictions that may exist on the system. The general rule to apply is that the greater the degree of sensitivity of the access rights, the stricter the access controls should be.

 ©ISACA. All Rights Reserved.

5.3.15 Remote Access Security

Many organizations require remote access connectivity for different types of users, such as employees, vendors, consultants, business partners and customer representatives. A variety of methods and procedures are available to satisfy an organization's business need for this level of access.

Remote access users can connect to their organization's networks with the same level of functionality that exists within their office. The remote access design enables connectivity using the same network standards and protocols applicable to the systems users are accessing. Transmission Control Protocol/Internet Protocol (TCP/IP)-based systems and systems network architecture (SNA) systems are used for the mainframe, with users connecting to a mainframe-based legacy application via terminal emulation software. Support for these connections includes asynchronous point-to-point modem connectivity, integrated services digital network (ISDN) dial-on-demand connectivity, and dedicated lines (e.g., frame relay and digital subscriber lines [DSL]).

Remote Access Risk

Remote access is vulnerable to many risk factors that would not ordinarily be found in the traditional environment. The IS auditor should ensure that remote access is given priority in the security architecture of the organization. Common types of risk associated with remote access include:

- **Denial of service (DoS)**—Remote users may not be able to gain access to data or applications that are vital to carry out their day-to-day business.
- **Malicious third parties**—Intruders may gain access to critical applications or sensitive data by exploiting weaknesses in communications software and network protocols.
- **Misconfigured communications software**—Communications misconfigurations may result in unauthorized access or modification of an organization's information resources.
- **Misconfiguration**—Misconfigured devices may compromise the corporate computing infrastructure.
- **Unsecured hosts**—Host systems that are not secured appropriately can be exploited by an intruder gaining access remotely.
- **Physical security weaknesses**—Physical security issues associated with remote users' computers are a major risk.

Remote access controls include:

- Policy and standards
- Proper authorizations
- Strong I&A mechanisms
- Encryption tools and techniques, such as use of a VPN, TLS, etc.
- Robust system and network management
- Continuous network monitoring, such as the use of IDS/IPS, DLP, etc.

5.3.16 Biometrics

Biometric access controls are the best means of authenticating a user's identity based on a unique, measurable attribute or trait for verifying the identity of a human being. A biometric control restricts computer access based on a physical or behavioral characteristic of the user. Due to advances in hardware and storage, biometric systems are becoming a more viable option for use as access control mechanisms.

Using a biometric generally involves use of a reader device that interprets the individual's biometric features before access is authorized. However, this is not a flawless process because changes can affect certain biometric features (e.g., fingerprint scars, signature irregularities, voice changes). For this reason, biometric access control systems are not all equally effective and easy to use.

Adding a user's biometric information to a system occurs through an enrollment process that involves storing a user's particular biometric feature data. This occurs through an iterative averaging process of acquiring a physical or behavioral sample, extracting unique data from the sample (converted into a mathematical code), creating an initial template, comparing new samples with what has been stored, and developing a final template that can be used to authenticate the user. Subsequent samples will be used in determining whether a match or non-match condition exists for granting access.

Management of Biometrics

Management of biometrics should address effective security for the collection, distribution and processing of biometric data, encompassing:

- Data integrity, authenticity and nonrepudiation
- Management of biometric data across its life cycle—comprised of the enrollment, transmission, storage, verification, identification and termination processes
- Use of biometric technology, including one-to-one and one-to-many matching, for the I&A of users
- Application of biometric technology for internal and external, as well as logical and physical, access control

©ISACA. All Rights Reserved.

- Encapsulation of biometric data
- Techniques for the secure transmission and storage of biometric data
- Security of the physical hardware used throughout the biometric data life cycle
- Techniques for integrity and privacy protection of biometric data

Management should develop and approve a biometric information management and security policy. The auditor should use the policy to gain a better understanding of the biometric systems in use. With respect to testing, the auditor should make sure a biometric policy has been developed and that biometric information is being secured appropriately.

With any critical information system, logical and physical controls, including business continuity plans (BCPs), should address this area.

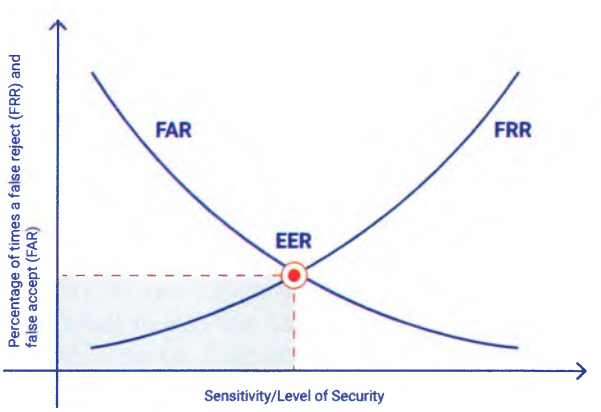
Life cycle controls for the development of biometric solutions should be in place to cover the enrollment request, the template creation and storage, and the verification and identification procedures. The I&A procedures for individual enrollment and template creation should be specified in the biometric identity management system (BIMS) policy. Management needs to have controls in place to ensure that these procedures are being followed in accordance with this policy. If the biometric device malfunctions or is inoperable, backup authentication methods should be developed. Controls should be in place to protect the sample data as well as the template from modification during transmission.

Biometric Performance Metrics

The most common metrics that are used to measure biometric performance are:

- **Failure to enroll rate (FER)**—FER refers to the proportion of people who fail to be enrolled successfully in a biometric system. The IS auditor reviewing the performance of a biometric system needs to determine the causes of FER. Some of the reasons users fail to enroll include physical differences, lack of knowledge, inadequate training and environmental conditions prevailing at the time of enrollment.
- **False rejection rate (FRR)**—A false rejection occurs when an authorized subject is rejected as unauthorized. FRR is calculated by dividing the total number of identification attempts by the number of false-negative recognitions. The false rejections are also known as Type 1 errors. Though they are normally a source of frustration for the authorized users who are falsely denied access, they are not really security issues. However, this issue raises the overhead of revalidating authorized users and making up valuable lost time to complete the users' assigned tasks.
- **False acceptance rate (FAR)**—A false acceptance occurs when an unauthorized subject is falsely accepted as valid and authorized. The formula for FAR is the total number of identification attempts divided by the number of false-positive recognitions. False acceptances are also known as Type 2 errors. A Type 2 error is very undesirable in terms of information security due to the risk that impostors may gain unauthorized access.
- **Crossover error rate (CER)**—The CER describes the point where the FRR and the FAR meet. At that point, the FRR and the FAR are equal, so CER is sometimes referred to as the equal error rate (EER). The CER measures the overall accuracy of a biometric system. **Figure 5.16** depicts the mechanics underlying the CER.

Figure 5.16—The Crossover Error Rate



If an organization's biometric control is producing a lot of false rejections, this can be addressed by reducing the amount of data the system collects while authenticating subjects to lower the system's accuracy. However, lowering the FRR data points may result in an increase in the FAR. Put simply, as the sensitivity of a biometric system increases, FRRs will rise and FARs will drop and vice versa, and the intersection of both lines results in the CER. The CER should be zero at the intersection. Ideally, this should be the case with any effective biometric system, but it is largely unattainable in practice.

 ©ISACA. All Rights Reserved.

Physically Oriented Biometrics

Generally, the ordering of biometric devices with the best response times and lowest CERs are palm, hand, iris, retina, fingerprint and voice, respectively.

Palm-based biometric devices analyze physical characteristics associated with the palm, such as ridges and valleys. This biometric involves placing the hand on a scanner that captures physical characteristics.

As one of the oldest biometric techniques, hand geometry measures the physical characteristics of the users' hands and fingers from a three-dimensional perspective. The user's hand is placed palm-down on a metal surface with five guidance pegs to ensure that fingers are placed properly and in the correct hand position. The template is built from measurements of physical geometric characteristics of a person's hand (usually 90 measurements)—for example, length, width, thickness and surface area.

Advantages of hand geometry systems are the social acceptance that they have received and the very minimal computer storage space that is required for a template, generally 10 to 20 bytes. The main disadvantage compared to other biometric methods is the lack of uniqueness of hand geometry data. Moreover, an injury to the hand may cause the measurements to change, resulting in recognition problems.

Patterns associated with the iris, the colored portion of the eye surrounding the pupil, are unique for every individual and thus a viable method for user identification. To capture this information, the user's eye is centered on a device that displays a reflection of the iris. After the user's eye is aligned, a camera takes a picture of the iris and compares it with a stored image. The iris is stable over time, having over 400 characteristics, although only approximately 260 of these are used to generate the template. As is the case with fingerprint scanning, the template carries less information than a high-quality image.

The key advantage to iris identification is that contact with the device is not needed, which contrasts with other forms of identification, such as fingerprint and retinal scans. Disadvantages of iris recognition are the high cost of the system, compared to other biometric technologies, and the high amount of storage required to uniquely identify a user.

Fingerprint access control involves users placing a finger on an optical device or silicon surface for scanning. The template generated for the fingerprint measures bifurcations, divergences, enclosures, endings and valleys in the ridge pattern. It contains only specific data about the fingerprint, not the whole image of the fingerprint itself. Additionally, the full fingerprint cannot be reconstructed from the template. Depending on the provider, the fingerprint template may use between 250 bytes and 1,000 bytes or more. More storage space implies lower error rates. Fingerprint characteristics are described by a set of numeric values. While the user's finger is in place for between two and three seconds, a typical image containing between 30 and 40 finger details is obtained and used for an automated comparison with the user's template.

Advantages of fingerprint scanning are its low cost, the small size of the device, ability to physically interface with existing client-server-based systems and ease of integration with existing access control methods. Disadvantages include the need for physical contact with the device and the possibility of poor-quality images due to residues, such as dirt and body oils, on the finger. Additionally, fingerprint biometrics are not as effective as other techniques.

With face-recognition biometric devices, the biometric reader processes an image captured by a video camera, which is usually within 24 inches (60 cm) of the human face, isolating it from the other objects captured within the image. The reader analyzes images captured for general facial characteristics. The template created is based on generating either two- or three-dimensional mapping arrays or by combining facial-metric measurements of the distance between specific facial features, such as the eyes, nose and mouth. Some vendors include thermal imaging in the template. The face is considered one of the most natural and "friendly" biometrics, and it is acceptable to users because it is fast and easy to use. The main disadvantage of face recognition is the lack of uniqueness, which means that people who look alike may fool the device. Moreover, some systems cannot maintain high levels of performance as the database grows in size.

Behavior-Oriented Biometrics

With signature recognition, also referred to as signature dynamics, information from a reader is used to analyze two different areas of an individual's signature: the specific features of the signature and the specific features of the signing process. It includes speed, pen pressure, directions, stroke length and the points in time when the pen is lifted from the paper.

Advantages of this method are that it is fast, easy to use and has a low implementation cost. Other advantages are that even though a person might be able to duplicate the

©ISACA. All Rights Reserved.

visual image of someone else's signature, it is difficult if not impossible to duplicate the dynamics (e.g., time duration in signing, pen-pressure, how often pen leaves signing block, etc.).

The main disadvantage is capturing the uniqueness of a signature, particularly for users who do not sign their names in a consistent manner, which may occur due to illness/disease or use of initials versus a complete signature, for example. Additionally, users' signing behavior may change when they sign onto signature I&A "tablets" versus writing their signature in ink on a piece of paper.

Voice recognition involves taking the acoustic signal of a person's voice, saying a passphrase, and converting it to a unique digital code that can then be stored in a template (approximately 1,500-3,000 bytes). Voice recognition incorporates several variables or parameters to recognize a voice/speech pattern, including pitch, dynamics and waveform.

The main attraction of this method is that it can be deployed in telephone applications with no additional user hardware costs. It also has a high rate of acceptance among users.

Disadvantages of this method include:
- The large volume of storage requirements
- Changes to people's voices
- The possibility of misspoken phrases
- The possibility of using a clandestine recording of the user saying the passphrase to gain access
- Background noise interference

Biometric Audit Considerations

Organizations should consider many factors when choosing and implementing a biometric system including:
- **Privacy concerns**—The success of a biometric system deployment may depend on how acceptable it is to users. This is mainly due to privacy concerns, as some systems are viewed as intrusive to a user's personal space. Cultural and religious considerations are often related to privacy objections.
- **Personal health**—Some health complications may affect the use of a biometric system. For example, chronic conditions such as diabetes may affect the flow of blood. Another concern is that organizations may improperly obtain health information that could be used to the detriment of the system user. There are also concerns over the spread of contagious diseases by contact with contaminated surfaces.
- **Expertise**—Certain users in the organization may not have the required level of literacy and educational skills to use a biometric system. Moreover, the organization may lack in-house skills to enroll users on the biometric platforms. The IS auditor should evaluate the skill levels of both the security architects implementing the biometric system and the users.
- **Robustness of the system**—To be effective, a biometric system must be robust and able to withstand challenges related to reliability and resilience. This can help reduce the impact of FRR and FAR readings, as well as system tampering and sabotage by threat actors.
- **Cost**—The cost of a biometric deployment is a key consideration in the selection of a biometric system for an organization. Some biometric systems are expensive and consume huge amounts of resources. The IS auditor reviewing biometric systems in the organization should ascertain whether the one selected provides an ROI for the organization.
- **Accuracy**—The accuracy of a biometric system is determined by the FAR, which influences the probability of unauthorized users gaining access. It is one of the most critical factors to be assessed when selecting a modality of a biometric system to deploy in an organization. The organization should consider biometric systems that have lower FARs.
- **Security**—Security is an important consideration in the choice of which biometric system to implement in an organization. Biometric systems such as iris and vein patterns, which are difficult to replicate, are generally considered the most secure. The IS auditor should not consider security as the only important consideration in the review process—other factors are also important. Yet security is generally given more weight.
- **Compliance requirements**—All biometric systems should be compliant with applicable laws and regulations. This is especially true when dealing with sensitive data such as health and privacy information. Compliance with such requirements assists the organization with avoiding fines and penalties associated with noncompliance.

5.3.17 Naming Conventions for Logical Access Controls

Access capabilities are implemented by security administration in a set of access rules that stipulate which users (or groups of users) are authorized to access a resource (such as a dataset or file) and at what level (such as read or update). The access control mechanism applies

 ©ISACA. All Rights Reserved.

these rules whenever a user attempts to access or use a protected resource.

Access control naming conventions are structures used to govern user access to a system and user authority to access/use computer resources such as files, programs and terminals. General naming conventions and associated files are required in a computer environment to establish and maintain personal accountability and SoD in the access of data. The owners of the data or application, with the help of the security officer, usually set up naming conventions. The need for sophisticated naming conventions over access controls depends on the importance and level of security needed to ensure that unauthorized access has not been granted. It is important to establish naming conventions that both promote the implementation of efficient access rules and simplify security administration.

Naming conventions for system resources (e.g., datasets, volumes, programs and employee workstations) are an important prerequisite for efficient administration of security controls. Naming conventions can be structured so that resources beginning with the same high-level qualifier can be governed by generic rules. This reduces the number of rules required to adequately protect resources, which facilitates security administration and maintenance efforts.

5.3.18 Federated Identity Management

Federated identity management (FIM)—also known as identity federation—is an arrangement between multiple enterprises to use common identification data of users within a group to provide access to organization systems. A corporate entity may initiate such federation for all group enterprises within corporate control. The main objective of implementing FIM is to make access easier for users.

Identity federation links a user's identity across multiple security domains, each supporting its own identity management system. When two domains are federated, the user can authenticate to the home domain and then access resources in the other domain without having to perform a separate login process. Identity federation offers economic advantages and convenience to enterprises and their network subscribers. For example, multiple corporations can share a single application, resulting in cost savings and consolidation of resources.

For FIM to be effective, the partners must have a sense of mutual trust, generally established through contracts. Identity authorization message transmission between partners in an FIM system must be through a secure channel.

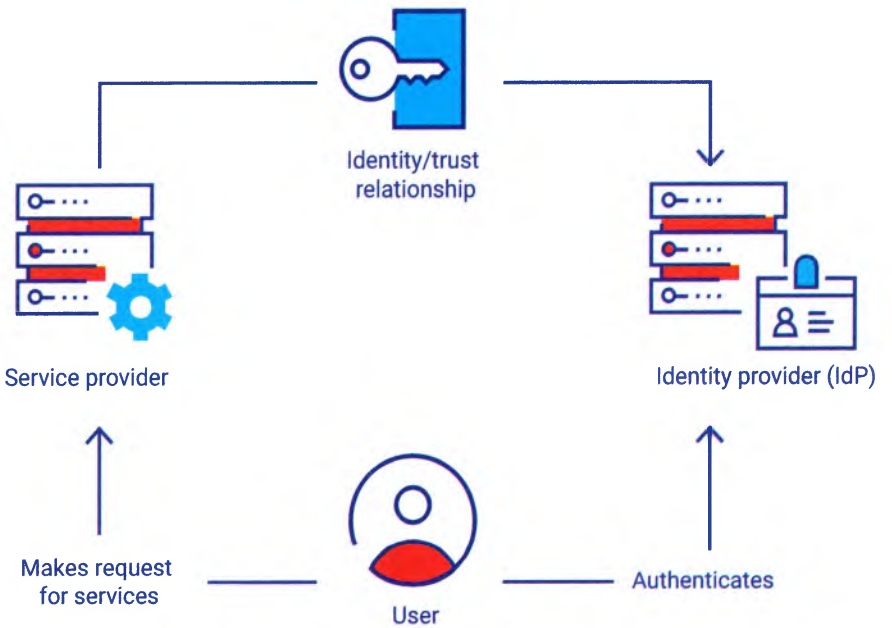
To implement effective FIM, partnering organizations must have policies that adhere to the security requirements of all members, which can sometimes be complicated due to enterprises setting different security requirements and rules. Also, when an organization is a member of multiple federations, ensuring that polices accurately reflect the rules of each member can be time-consuming, costly and complex.

An IS auditor should review the business case that establishes the need for identity federation. Next is reviewing policies and monitoring mechanisms to ensure unauthorized access is prevented or detected and corrected. Federated identity works on the basis of mutual trust relationships between a SP, such as an application vendor, and an external party known as the identity provider (IdP). The IdP creates and manages user credentials while the SP and the IdP agree on an authentication process. Multiple SPs can participate in a federated identity agreement with a single IdP with the IdP maintaining mutual trust agreements with all the organizations. Users requesting access to a domain or service will not be required to provide their login credentials every time, as their credentials are already stored in the IdP's database. The IdP confirms a user's digital identity in its database, authenticates the user and sends the identity information to the SP. This enables the user to access multiple applications, systems, portals, websites and similar facilities. **Figure 5.17** details the FIM process.

As shown in **figure 5.17**, a user first makes a request for services to the SP. The SP requests user authentication by the IdP. Through the identity/trust relationship in place, the SP verifies whether the user is currently authenticated by the IdP. The SP directs any user who is not authenticated to the login page of the IdP for authentication. The user authenticates with the IdP by entering login credentials. If the login credentials are properly validated, the user is authenticated and provided with an access token. Finally, the access token is used to access the application.

©ISACA. All Rights Reserved.

Figure 5.17—The Federated Identity Management Process



FIM Technologies

It should be clear to the IS auditor that FIM leverages certain standard protocols in its operations that may also be found in implementations such as SSO. **Figure 5.18** shows typical standards used to support FIM.

Figure 5.18—Federated Identity Management Protocols

Protocol	Description
Security Assertion Markup Language (SAML)	SAML is an open Extensible Markup Language (XML) standard data format used for exchanging authentication and authorization information between an IdP and applications or services. It simplifies password management and user authentication in a federated system. SAML authorization authenticates a user and tells the SP the type of access to be granted. This facilitates access to multiple domains using a single set of credentials. It is important for the IS auditor to be aware that SSO also uses the SAML.
Open Authentication (OAuth)	OAuth allows third-party services like websites and applications to exchange user information without the need for the user to provide credentials such as passwords to access the services. The various services trust each other, allowing them to share information while also protecting the user. For instance, users can allow YouTube to access their Facebook profiles without having to share their Facebook passwords. It is important to note that OAuth will not share user credentials across services but simply uses authorization tokens to prove a user's identity.

 ©ISACA. All Rights Reserved.

Figure 5.18—Federated Identity Management Protocols (cont.)

Protocol	Description
OpenID Connect (OIDC)	OIDC adds an identity layer on top of the OAuth 2.0 protocol to allow third-party applications to verify a user's identity and provide the user with one login facility for multiple applications. The IS auditor should understand that the login flow for OIDC and SAML is basically the same. The major difference is that SAML is a self-contained authentication and authorization protocol, while OIDC adds an authentication layer on top of SAML. Another notable difference is that OIDC is built on the OAuth 2.0 standards and uses JSON to transmit the data while SAML uses XML.
System for Cross-Domain Identity Management (SCIM)	SCIM is a standard for automatically exchanging identity information between two systems. While SAML and OIDC pass identity information to an application during the authentication process, SCIM keeps the user information updated as events change, such as when new users are assigned to the service or application or deleted from the system. SCIM is a key component of user provisioning in the IAM space.

Benefits of FIM

A FIM architecture offers numerous advantages over traditional authentication systems. Some of the advantages include:

- **Enhanced security**—In non-federated systems, a user typically logs into several individual systems, each with its own set of credentials. This means that each log in is a potential point of vulnerability. This increases the risk of attack from unauthorized users. FIM, in contrast, securely authenticates a user to grant access to applications in many domains, thus reducing the number of logins and lowering attack risk.
- **Enhanced user experience**—Users only provide their credentials once to access multiple applications across federated domains. Users need to remember only one set of credentials for one account. That can be much easier than keeping track of multiple credentials for different sites and services. This increases user convenience and efficiency and improves user experiences.
- **Single-point provisioning**—FIM enables single-point provisioning, making it easier to provide access to users outside the traditional organizational perimeter. With FIM, a user needs to remember credentials for only one account. This also makes it easier to monitor multiple credentials for a variety of sites and services.
- **Secure resource-sharing**—Federated organizations can effectively share information and resources without risking user credentials or security.
- **Easier information management**—Organizations store user information with an IdP, which simplifies data management processes.
- **Reduced costs**—Implementing a federated login system can be less expensive than setting up and maintaining a SSO solution. Organizations do not need to build and deploy a custom SSO solution.
- **Increased productivity**—Multiple logins reduce organizational productivity as users spend considerable time entering and re-entering passwords and requesting assistance from the helpdesk. FIM improves organizational productivity by addressing these challenges.

Limitations of FIM

Some limitations associated with FIM include:

- **Increased dependency**—When using federated login, an organization relies on the IdP to keep its credentials safe and secure. If the IdP experiences an outage or security breach, users may be unable to log in to the websites and services they ordinarily use.
- **Reduced control**—With FIM, an organization loses some control. For example, all password changes on websites will go through the IdP, which the organization does not control. If the IdP security environment is weak, the organization will be exposed.
- **Reduced flexibility**—Federated login systems can be less flexible than SSO solutions because they typically only work with a few specific types of accounts. The FIM technology may therefore not be compatible with the existing systems in the organization.
- **Increased costs**—The cost of setting up a FIM is generally high and beyond the reach of many small to medium enterprises. Moreover, adoption of FIM normally comes with major modifications to the organization's existing IS infrastructure, which is costly and time-consuming.

©ISACA. All Rights Reserved.

FIM Versus SSO

FIM and SSO enable organizations to minimize password-related risk, secure their data and improve user experiences. Both kinds of solutions require a single set of credentials to grant user access to multiple applications. These two technologies often confuse business leaders. The IS auditor should be alert to such confusion and advise management accordingly. **Figure 5.19** provides a comparison between FIM and SSO technologies.

Figure 5.19—Comparison of Federated Identity Management and Single-Sign On

	Federated Identity Management (FIM)	Single-Sign On (SSO)
Extent of access	FIM enables users to access applications or platforms across multiple enterprise domains that are part of the federated configuration. FIM supports SSO and extends SSO to multiple domains.	With SSO, users can access multiple applications within the same organization or domain using a single set of credentials.
Level of centralization	FIM is a decentralized approach to authentication that allows users to access multiple online services with a single set of credentials. It is more scalable and easier to manage than SSO.	SSO is centralized, requiring users to authenticate with a single provider to access multiple online services
Areas of application	FIM is prevalent on consumer-facing websites and applications.	SSO is typically used in business environments where employees need to access various resources, such as email and shared files.
Level of security	FIM is less secure since there is a possibility of using compromised credentials to access accounts at multiple entities.	SSO is more secure as there is virtually no possibility of using compromised credentials to access accounts at multiple entities.

5.3.19 Auditing Logical Access

When evaluating logical access controls, the IS auditor should:

- Obtain a general understanding of the security risk facing information processing through a review of relevant documentation, inquiry, observation, risk assessment and evaluation techniques.
- Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness by reviewing appropriate hardware and software security features and identifying any deficiencies or redundancies.
- Test controls over access paths to determine whether they are functioning and effective by applying appropriate audit techniques.
- Evaluate the access control environment to determine if the control objectives are achieved by analyzing test results and other audit evidence.
- Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standards or practices and procedures used by other organizations.

Familiarization With the IT Environment

Familiarization is the first step of the audit. It involves obtaining a clear understanding of the technical, managerial and security environment of the IS processing facility, typically through interviews, physical walk-throughs, review of documents and risk assessments.

Assessing and Documenting the Access Paths

The access path is the logical route an end user takes to access computerized information. This starts with a terminal/workstation and typically ends with the data being accessed. Along the way, numerous hardware and software components are encountered. The IS auditor should evaluate each component for proper implementation and physical and logical access security.

Special consideration should be given to the:

- Origination and authorization of the data
- Validity and correctness of the input data
- Maintenance of the affected OSs (patching, hardening and closing the unnecessarily open ports)

 ©ISACA. All Rights Reserved.

Note

The IS auditor should evaluate the control objectives, referring to the origination and authorization of the application data, and should evaluate the control measures used in data input and processing. Omitting control objectives and measures makes the applications vulnerable to attacks either from within or from the outside, especially from the Internet. Firewalls do not protect applications against the types of attacks that come with the Hypertext Transfer Protocol (HTTP) communication that is usually permitted on the applications.

Interviewing Systems Personnel

Technical experts are often required to control and maintain the various components of the access path, as well as the OS and computer mainframe. These experts can be a valuable source of information to the IS auditor who is developing an understanding of the security environment. To determine who the technical experts are, the IS auditor should meet with the IS manager and review organizational charts and job descriptions. Key roles include the security administrator, network control manager and systems software manager.

The security administrator should be asked to identify the responsibilities and functions of the position. If the answers provided do not support sound control practices or do not adhere to the written job description, the IS auditor should compensate by expanding the scope of the testing of access controls. Also, the IS auditor should determine whether the security administrator is aware of the logical accesses that must be protected, has the motivation and means to actively monitor logons to account for employee changes, and is knowledgeable about how to maintain and monitor access.

A sample of end users should be interviewed to assess their awareness of management policies regarding logical security and confidentiality.

Reviewing Reports From Access Control Software

The reporting features of access control software provide the security administrator with the opportunity to monitor adherence to security policies. By reviewing a sample of security reports, the IS auditor can determine whether enough information is provided to support an investigation and if the security administrator is performing an effective review of the report.

Unsuccessful access attempts should be reported and should identify the time, terminal, logon and file or data element for which access was attempted.

Reviewing Application Systems Operations Manual

An application systems manual should contain documentation of the programs that generally are used throughout a data processing installation to support the development, implementation, operation and use of application systems. The manual should include information about the platform the application can run on, database management systems (DBMSs), compilers, interpreters, telecommunication monitors and other applications that can run with the application.

5.4 Network and Endpoint Security

Enterprises can effectively prevent and detect most attacks on their networks by employing perimeter security controls. Firewalls and IDSs provide protection and critical alert information at borders between trusted and untrusted networks. The proper implementation and maintenance of firewalls and IDSs is critical to a successful, in-depth security program. The security landscape is filled with technologies and solutions to address a myriad of needs. Understanding the solution's function and its application to the underlying infrastructure requires knowledge of the infrastructure itself and the protocols in use.

5.4.1 IS Network Infrastructure

IS networks were developed from the need to share information resources residing on different computer devices, which enabled organizations to improve business processes and realize substantial productivity gains.

Generally, digital telecommunication links or lines are used for networks and classified according to the type of provider or the type of technology. Typically, they can be divided into dedicated circuit (also known as leased lines) and switched circuit.

With packet switching technology, users share common carrier resources. Because it allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much lower than with leased lines. In a packet switching setup, networks have connections with the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between customers' sites to deliver packets of data from one to the other through the network.

©ISACA. All Rights Reserved.

The section of the carrier's network that is shared is often referred to as a cloud. Some examples of packet-switching networks include asynchronous transfer mode (ATM) and Switched Multimegabit Data Services (SMDS).

Methods for transmitting signals over analog telecommunication links or lines are either baseband or broadband:

- **Baseband**—The signals are directly injected on the communication link (no modulation or shift in the range of frequencies of the signal). Generally, only one communication channel is available at any a time (half-duplex), although full-duplex modems are now available.
- **Broadband network**—Different carrier frequencies defined within the available band can carry analog signals, such as those generated by image processors or a data modem, as if they were placed on separate baseband channels. Interference is avoided by separating adjacent carrier frequencies with a gap that depends on the band requirements of the carried signals. The possibility of vectoring multiple independent channels on single-carrier media enhances considerably the effectiveness of remote connections. Simultaneous data or control transmission/reception taking place between two stations is called a full-duplex connection.

5.4.2 Enterprise Network Architectures

Modern networks are part of a large, centrally managed, internetworked architecture solution of high-speed local- and wide-area computer networks serving organizations' client server-based environments. Such architectures include clustering common types of IT functions in network segments, each uniquely identifiable and specialized for a particular task. For example, network segments or blocks may include web-based front-end application servers (public or private), application and database servers, and mainframe servers using terminal emulation software to allow end users to access these back-end legacy-based systems. In turn, end users can be clustered together within their own network LANs, but with rapid access capabilities to incorporate information resources.

Some organizations implement service-oriented architectures (SOAs) in which web software components, using Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML), interoperate in a loosely connected and distributed fashion across the network. Within this environment, information is highly accessible, available anytime and anywhere, and centrally managed for highly effective and efficient troubleshooting and performance management to achieve optimum use of network resources.

To understand the network architecture solutions offered from a business, performance and security design standpoint, an IS auditor must understand information technologies associated with the design and development of a telecommunications infrastructure (e.g., LAN and WAN specifications).

5.4.3 Types of Networks

The types of networks common to organizations include:

- **Personal area networks (PANs)**—Generally, a PAN is a microcomputer network used for communications among computer devices (including telephones, tablets, printers, cameras, scanners, etc.) being used by an individual person. The extent of a PAN is typically within a range of 33 feet (about 10 meters). PANs can be used for communication among the personal devices themselves or to connect to a higher-level network and the Internet. PANs may be wired with computer buses, such as universal serial bus (USB). Wireless PANs (WPANs) can be set up using network technologies, such as infrared data association (IrDA) and Bluetooth (piconet). A piconet is composed of up to eight active devices in a master-slave relationship. A piconet typically has a range of 32.8 feet (10 meters), although ranges of up to 328 feet (100 meters) can be reached under ideal circumstances.
- **LANs**—LANs are computer networks that cover a limited area, such as a home, office or campus. Characteristics of LANs are higher data transfer rates and smaller geographic range. Ethernet and Wi-Fi (wireless local area networks [WLANs]) are the two most common technologies currently used.
- **Storage area networks (SANs)**—SANs are a variation of LANs and are dedicated to connecting storage devices to servers and other computing devices. SANs centralize the process for the storage and administration of data. Basically, a SAN is an independent dedicated network that provides access to consolidated data storage in block-level format. The main difference between SAN and network attached storage (NAS) is that SAN provides block level storage while NAS provides file level storage. Also, NAS is a single device made up of redundant array of independent disks (RAID) while SAN uses a network of devices including solid-state drives (SSDs), cloud storage and flash storage. The IS auditor should be aware of the security risk associated

with SAN architectures. For example, in a SAN, along with applications and networks, there are physical threats to data that need to be secured. Network and configuration protocol vulnerabilities are also widespread because SANs typically do not enforce strict authentication and users require authorization. Therefore, attacks that exploit a lack of appropriate authentication protocols are easy to carry out in SANs. SANs are used to access large storage solutions, making them a target for attackers who laterally move through the network, possibly using stolen credentials or taking advantage of insufficient access controls. An IS auditor reviewing the operation can recommend that management adequately protect SANs from attacks though implementing strong frequent authentication to protect the data storage and help organizations better track who is allowed access to each individual application or database. An organization-wide security approach should be in place so that any department in the organization that stores sensitive business data on its SAN is responsible for protecting its own data.

- **Wide area networks (WANs)**—WANs are computer networks that cover a broad area, such as a city, region, nation or international link. The Internet is the largest example of a WAN. WANs are used to connect LANs and other types of networks so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers (ISPs), provide connections from an organization's LAN to the Internet. WANs may also be wireless (WWANs). A WAN that is limited to a city or region is called a metropolitan area network and is characterized by relatively higher data transfer rates than would be typical over a wide area.

5.4.4 Network Services

Network services are functional features made possible by appropriate OS applications. They allow orderly utilization of the resources on the network. Instead of having a single OS that controls its own resources and shares them with the requesting programs, the network relies on standards and on a specific protocol or set of rules, enacted and operated through the basic system software of the various network devices capable of supporting the individual network services. Users and business applications can request network services through specific calls/interfaces. Some common network application services are:

- **Network file system**—Allows users to share files, printers and other resources in a network
- **Email services**—Provide the ability, via a terminal or PC connected to a communication network, to send an unstructured message to another individual or group of people
- **Print services**—Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network
- **Remote access services**—Provide remote access capabilities that allow a computing device to appear as if directly attached to the remote host
- **Directory services**—Store information about the various resources on a network and help network devices locate services, much like a conventional telephone directory
  - Directory services also help network administrators manage user access to network resources.
- **Network management**—Provides a set of functions to control and maintain the network
  - Network management provides detailed information about the status of all components in the network, such as line status, active terminals, length of message queues, error rate on a line and traffic over a line. It enables computers to share information and resources within a network and provides network reliability. It provides the operator with an early warning signal of network problems before they affect network reliability, allowing the operator to take timely preventive or remedial actions.
- **Dynamic Host Configuration Protocol (DHCP)**—Used by networked computers (clients) to obtain IP addresses and other parameters, such as the default gateway, subnet mask and IP addresses of DNSs from a DHCP server:
  - The DHCP server ensures that all IP addresses are unique (e.g., no IP address is assigned to a second client while the first client's assignment is valid [its lease has not expired]). Thus, IP address pool management is performed by the server and not by a human network administrator.
- **DNS**—Translates the names of network nodes into network (IP) addresses

©ISACA. All Rights Reserved.

5.4.5 Network Standards and Protocols

Network architecture standards facilitate the process of creating an integrated environment that applications can work within by providing a reference model that organizations can use for structuring intercomputer and network communication processes.

Besides the convenience of using compatible architectures, one major advantage of network standards is that they help organizations meet the challenge of designing and implementing an integrated, efficient, reliable, scalable and secure network of LANs and WANs with external connectivity (public Internet). This is a major challenge due to the requirements of the following:

- **Interoperability**—Occurs when connecting various systems to support communication among disparate technologies with different sites using different types of media that may operate at differing speeds
- **Availability**—Means end users have continuous, reliable and secure service (24/7 access)
- **Flexibility**—Needed for network scalability to accommodate network expansion and requirements for new applications and services
- **Maintainability**—Means an organization provides centralized support and troubleshooting over heterogeneous but highly integrated systems

Organizations need to have the ability to define specifications for the types of networks to be established (e.g., LANs/WANs) when creating an integrated environment that their applications can work within. Organizations must also provide centralized support and troubleshooting over heterogeneous but highly integrated systems.

5.4.6 Virtual Private Networks

A VPN extends the corporate network securely with encrypted packets sent out via virtual connections over the public Internet to remote offices and workers, salespeople and business partners. Rather than using expensive dedicated leased lines, VPNs use public worldwide IP infrastructure, enabling remote users to make a local call (versus dialing-in at long distance rates) or use an Internet cable modem or DSL connection for inexpensive public network connectivity.

VPNs are platform independent. Any computer system that is configured to run on an IP network can be connected through a VPN with no modifications except for the installation of remote software.

There are three types of VPNs:

1. **Remote-access VPN**—Connects telecommuters and mobile users to the enterprise WAN in a secure manner; lowers the barrier to telecommuting by ensuring that information is reasonably protected on the open Internet
2. **Intranet VPN**—Connects branch offices within an enterprise WAN
3. **Extranet VPN**—Gives business partners limited access to each other's corporate networks, (e.g., an automotive manufacturer and its suppliers)

The only difference between a traditional, intracompany VPN (intranet) and an intercompany VPN (extranet) is the way the VPN is managed. With an intranet VPN, all network and VPN resources are managed by a single organization. When an organization's VPN is used for an extranet, management control becomes weak. Therefore, it is recommended that with an extranet VPN, each constituent company manage its own VPN and maintain control over it.

VPNs allow:

- Network managers to cost-efficiently increase the span of the corporate network
- Remote network users to securely and easily access their corporate enterprise
- Corporations to securely communicate with business partners
- Supply chain management to be efficient and effective
- SPs to grow their businesses by providing substantial incremental bandwidth with value-added services

Determining which network resources should be linked via a VPN depends on the applications used on the various systems. Requirements often used to determine network connectivity include security policies, business models, intranet server access, application requirements, data sharing and application server access.

Independent of the type of connectivity, the primary issues related to VPNs are:

- Security of transmissions, including preventing hijacking of transmissions and preventing malware from entering the network
- Managing the technology
- Configuration management
- Ensuring information is unaltered and maintains accuracy and reliability

The impact on the business transmitting data through public networks and the accompanying risk are significant. Depending on the industry, enterprises may experience outages and intrusion attempts for financial

gain, to obtain intellectual property, to create business disruption, to obtain sensitive private information or to compromise national security. The perpetrators of an intrusion can be external or internal, private or government-sponsored. This activity may increase the enterprise's risk of:

- Public relations issues with the customers or the public (reputational risk)
- Inability to comply with regulatory processing requirements (regulatory and financial risk)
- Inability to perform critical business functions (operational and financial risk)
- Inability to maintain payroll and employee privacy (regulatory and reputational risk)
- Loss of physical or informational assets (reputational and financial risk)
- Inability to meet contractual service level agreements (SLAs) with third parties or customers (contractual risk)

VPN Protocols

Figure 5.20 provides an overview of the most common types of VPN protocols.

Figure 5.20—Virtual Private Network (VPN) Protocols

Type of Protocol	Protocol Description
Internet Protocol Security (IPSec)	IPSec is implemented in two modes. The IPSec tunnel mode encrypts the entire packet, including the header. The IPSec transport mode encrypts only the data portion of the packet. IPSec is commonly used for securing Internet communications and often for site-to-site VPNs.
Internet Key Exchange version 2 (IKEv2)	This protocol is useful and mostly implemented to re-establish a connection that was temporarily lost. It is considered one of the most secure and robust protocols and is generally most effective for mobile devices that switch between Wi-Fi and mobile data.
Point to Point Tunneling Protocol (PPTP)	PPTP allows multiprotocol traffic to be encrypted and then wrapped in a header to be sent across an IP network. It is typically used for remote access and site-to-site VPN connections. When using the Internet, the PPTP server is a PPTP-enabled VPN server with one interface on the Internet and a second interface on the corporate intranet. PPTP uses a transmission control protocol connection for tunnel management and generic routing encapsulation to wrap PPP frames for tunneled data. Due to security vulnerabilities, PPTP should be pared with compensating controls.
Secure Socket Tunneling Protocol (SSTP)	SSTP uses the Hypertext Transfer Protocol Secure (HTTPS) to pass traffic through firewalls and web proxies that might block other protocols. SSTP provides a mechanism to wrap Point-to-Point Protocol (PPP) traffic over the Secure Sockets Layer (SSL) channel. The use of PPP allows support for strong authentication methods, and SSL provides transport-level security with enhanced key negotiation, encryption and integrity checking.
Layer 2 Tunneling Protocol (L2TP)	L2TP enables multiprotocol traffic to be encrypted and sent over any transmission medium that supports PPP data delivery, such as IP or ATM. It is a combination of PPTP and Layer 2 Forwarding (L2F). L2TP represents the best features of PPTP and L2F. Unlike PPTP, L2TP relies on IPSec in transport mode for encryption services. The combination of L2TP and IPsec is known as L2TP/IPsec. Both L2TP and IPsec must be supported by both the VPN client and the VPN server. L2TP/IPsec is also capable of implementing perfect forward secrecy.

©ISACA. All Rights Reserved.

Figure 5.20—Virtual Private Network (VPN) Protocols (cont.)

Type of Protocol	Protocol Description
OpenVPN	OpenVPN is an open-source software application that implements VPN techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol with SSL/Transport Layer Security (TLS) for key exchange and is capable of traversing network address translators and firewalls. OpenVPN allows peers to authenticate each other using a secret key, certificate or username and password. Most VPN providers using OpenVPN employ perfect forward secrecy.

VPN Best Practices

There are various best practices the IS auditor can recommend to management to enhance the security of VPN technologies. Some of the recommendations for securing VPN infrastructures are:

- **Establish a VPN policy**—A VPN policy should be developed to establish the minimum security requirements and behavior expectations for users accessing the network through a VPN. It should also be reviewed and updated regularly to ensure it remains current. The policy should incorporate guidelines for creating secure passwords, enforcing strong authentication, using strong encryption, controlling access, monitoring and logging activities, and other best security practices.
- **Select a standards-based VPN**—VPNs that use accepted standards, such as Internet Key Exchange/ Internet Protocol Security (IKE/IPSec), are generally considered less risky and more secure than the Secure Sockets Layer (SSL)/TLS VPNs that use custom code to send traffic over TLS. If a VPN is designed to use a custom SSL/TLS tunnel as a fallback, it is advisable to disable this functionality.
- **Implement a VPN with strong cryptography**—Organizations should use VPNs with strong and up-to-date encryption technology. The encryption algorithms should also be validated by Federal Information Processing Standards (FIPS). Strong cryptography technologies include the TLS 1.3 protocol and encryption algorithms such as the AES 256-bit encryption algorithm. Strong cryptography ensures the confidentiality and integrity of data transmitted over the VPN.
- **Implement strong authentication**—VPNs should be configured using MFA, and passwords should be replaced with client authentication through digital certificates. Authentication tokens are another form of strong authentication. This reduces the risk of unauthorized access to VPN resources.
- **Practice effective patch management**—Security attackers often exploit VPN software vulnerabilities. Therefore, a continuous patch management process for VPN resources is needed. If the VPN is managed by a third-party vendor, the organization should confirm that the third-party code is current and secure. After the deployment of the VPN, it is advisable to regularly check for and promptly apply software updates.
- **Implement strict VPN access control measures**—VPNs should be protected using strong access control measures. Access to and from a VPN should be tightly controlled. Firewall rules should be created to allow only User Datagram Protocol (UDP) ports 500 and 4500 for IKE/IPsec VPNs or TCP port 433 (or custom port) for SSL/TLS VPNs. Access to the VPN endpoint based on an IP address allowlist should be limited. Access to the management interfaces through the VPN should be blocked to prevent compromise of administrator credentials and allow access to management interfaces.
- **Secure VPN traffic**—An IS auditor providing assurance over an organization's VPN architecture should be aware that while a VPN is designed to provide an encrypted channel between two locations, it does not perform any security inspection or filter the traffic passing through the tunnel. All VPN traffic should pass through a full security stack, including a web application firewall (WAF) and an IDS/IPS. It is crucial to ensure that the VPN is configured with all web application security settings enabled, such as replay attacks using previous users' session data.
- **Ensure the VPN is properly configured**—The VPN should be properly configured and hardened to reduce its attack surface. A secure VPN should support strong authentication, digital certificates, logging and auditing and an IPS.
- **Protect against zero-day vulnerabilities and malware**—VPNs are very useful security tools to prevent man-in-the-middle attacks and general

 ©ISACA. All Rights Reserved.

eavesdropping, but they cannot prevent, detect or eliminate malware traversing the network. Organizations should ensure that VPNs only use company hardware and incorporate antivirus and antimalware capabilities.
- **Test the VPN's capabilities**—Before the final deployment of a VPN to the organization, it is critical to understand the first test's capabilities and how it will handle user traffic. The IS auditor should be aware that while security remains the top priority in a VPN's configuration, additional security features can lead to more latency.
- **Monitor and log VPN usage**—It is important to regularly monitor and log VPN activity to detect and respond to any suspicious or malicious activities happening on the VPN. Logging VPN activities typically helps in identifying unauthorized access attempts and other malicious activities, enabling organizations to respond quickly to VPN security incidents.

5.4.7 Network Attached Storage

NAS consists of a centralized file server that enables multiple users to store and share files over communication networks. NAS security refers to the measures an organization implements to protect critical data within NAS environments from threats. NAS security helps organizations manage their NAS rather than passively allowing incidents to occur. Securing NAS environments is critical for all enterprises because it enables them to stay compliant with data protection and privacy laws, to protect proprietary information and to provide the best experience for customers. Some key benefits of maintaining a secure NAS environment include increased accountability and security awareness among all employees, improving an enterprise's overall data protection activities, decreasing data theft, and achieving cost savings through decreasing outages and maintaining a positive reputation with customers.

The IS auditor should be aware that NASs are subject to vulnerabilities such as:
- **Unsecure network configurations**—If the network to which the NAS storage devices are connected is an open network without secure configurations, all NAS devices are automatically vulnerable to threats on that public network. Unencrypted network sessions also make NAS systems vulnerable to attacks.
- **Unsecure passwords**—Network access passwords, storage management passwords and any other credentials that are left out in the open and are not encrypted or are shared unsafely are at risk of unauthorized use. An attacker could read or steal credentials and get unauthorized access.
- **Insufficient authentication**—If users on the network are not required to prove their identity and their right to access the system, malicious attackers can gain unauthorized access to the storage system. Once attackers gain access, they can launch more attacks within the system.
- **Leakage from other network devices**—NAS devices are typically connected to other devices on the same network and to IoT devices. IoT devices can leak malware into the NAS infrastructure, infecting NAS-connected devices.
- **Exposure to malware**—NAS can be exposed to malware, including worms and viruses. Some NAS devices have been victims of ransomware attacks. These attacks typically use poorly secured NAS and IoT-enabled devices as attack vectors.
- **Command injection**—NAS is susceptible to command injection attacks that allow attackers to take control of NAS storage drives and sometimes gain root access, which is a preserve of system administrators.

To secure an enterprise's NAS, the IS auditor should advise management to follow a few key practices including:
- **Train all employees**—All employees should be trained in how to recognize social engineering attacks, such as phishing attacks. Even employees who are not members of any storage or technical teams should be encouraged to adopt security practices, such as restricting visitors to a location where the NAS is located.
- **Update all OSs and firmware**—All system software should be updated regularly, including patches for known vulnerabilities. IS security teams and system administrators should continually check with the NAS vendor for available updates and immediately update their systems.
- **Secure Internet connections and ports**—The IS security team should ensure secure storage while networking teams should secure all connections to the public Internet. Examples include strict IP address allowlists, Hypertext Transfer Protocol Secure (HTTPS) connections and encryption of data in transit.
- **Manage passwords securely**—All passwords for storage devices or the network should be stored securely and never shared over email or business communication channels or written down in any public setting. Put simply, the organization should enforce good password practices.

©ISACA. All Rights Reserved.

- **Enable MFA**—MFA prevents many of the techniques and tactics used by attackers to gain unauthorized access to a NAS. Without all the required factors, an attacker cannot log on to the NAS account. This enhances the security of the NAS.
- **Use HTTPS**—HTTPS is a secure channel since it is encrypted—unlike HTTP, which is unencrypted. Users are given a choice of either HTTP or HTTPS in the settings page when connecting to a NAS remotely. HTTPS encrypts all the data to and from the NAS.
- **Implement firewall technology**—Most NAS drives incorporate built-in firewall technologies in their architectures. A firewall in a NAS device should always be turned on and configured in such a way that it only allows traffic from trusted sources. This strengthens the security defense posture of the NAS.
- **Use VPN to connect**—A VPN should be used to connect to the NAS. VPNs are very secure as they incorporate encryption in their functionalities. This is especially important in organizations where the NAS servers are accessed remotely.

5.4.8 Content Delivery Networks

A content delivery network (CDN) consists of interconnected servers that are strategically located to minimize the distance between the user and the nearest server. It works by directing each incoming request for a file or service to the nearest service location. If the CDN server has a recent copy of the requested content stored in its cache, it responds directly to the request. If it does not have it, it forwards the request onto the origin server, which fulfills the request while caching a copy of the response to support future requests. This provides some form of geographical and logical load balancing. For example, if a company is located in the United States and a request comes from South Africa, a local repository in Africa, rather than one in the United States, would provide the file access. The IS auditor should view CDNs as a collection of resource services deployed in numerous data centers across the Internet to provide low latency, high performance with less bandwidth, high quality and high availability of the hosted content.

There are three primary types of content delivered through CDN:

- **Dynamic content**—Dynamic content is generated on the fly by the web server. The content is created by web programming languages such as Hypertext Preprocessor (PHP) and Java.
- **Static content**—Static content does not typically change and does not require generation. It includes images, Cascading Style Sheets (CSS), JavaScript, etc.
- **Streaming content**—Streaming content includes videos or audio files that are played through a web browser control technology.

Benefits of CDNs

Some of the benefits of adopting CDN technology are:

- **Improved user experience**—In content distribution, load time equals high bouncing rates. The bounce rate applies to users who visit a website and then leave immediately. It is considered one of the most important measures of effectiveness for a website. CDNs help reduce bounce rates, thereby increasing Internet traffic. There are also fewer delays as the end users are closer to point of presences (PoPs).
- **Global accessibility**—CDNs help make content globally available and accessible, bypassing the problem of content source and destination by having multiple PoPs.
- **Scattered PoPs**—If the main server of a network is a whole continent away from a customer located in Asia, content delivery in response to customer queries will be slow. For this reason, CDNs use servers that are located as close as possible to the geographical location of the end users. This significantly speeds up content delivery, facilitates online business and eliminates disturbances in the form of slow or unsuccessful transactions.
- **Automatic data analytics**—Usually, CDN providers base their charges on data volume. This includes data analytics: most-used search queries, times, locations, etc. Data analytics permit organizations to improve their business models and evaluate working practices.
- **Lower rates of network congestion**—CDN implementation leads to lower network congestion rates and, hence, better performance. Network congestion occurs when multiple users want to access a website at the same time. A CDN can redirect users to less congested sections of the network leading to superior performance overall and an improved user experience.
- **Increased content quality**—There is a very high probability the content delivered through CDNs will maintain optimal quality in comparison to content delivered through other means. This makes the information shared more trustworthy, which has a positive effect on customer satisfaction.
- **Lower overhead costs**—CDNs eliminate payments for foreign services and for multiple providers. Content distributed through CDNs is available globally and can be accessed through a single

provider. This reduces the overhead for most organizations.

CDN Security Risk

In terms of risk assessment and subsequent auditing processes, the IS auditor needs to have heightened awareness. A breach or security vulnerability in a CDN is a serious event with serious consequences as it impacts several third-party partners causing drastic productivity losses.

Some of the security threats common to CDN environments include:

- **Session hijacking**—Unlike firewalls, CDNs cannot block undesirable traffic from infecting a website. CDN servers containing cached information can be hijacked and exploited in various ways.
- **Credential theft**—If a hacker gains access to cached information on a CDN that multiple businesses use, for example, the information of each organization's customers becomes vulnerable. Cybercriminals can steal passwords, email addresses and other sensitive information through a CDN.
- **Distributed DoS attacks**—Most CDNs are vulnerable to exploits that causes servers to run the same command repeatedly, leading to overloading and taking the content offline.
- **Security risk**—CDNs cache content on servers on a global basis, making it more vulnerable to attack. A threat actor who manages to compromise a CDN server could potentially access or modify all cached content.
- **Performance risk**—While CDNs can improve the performance of most websites or applications, they can introduce performance issues if they are not configured correctly. For example, if a CDN server goes offline or is overloaded, it can cause a website or application to become unavailable.
- **Increased cost profile**—A CDN is typically expensive to build and maintain and is often limited to well-resourced organizations with large websites or high traffic volumes.
- **Loss of control**—By using the services of a CDN, an organization becomes reliant on the CDN provider for content delivery. This can lead to loss of control and business continuity challenges, especially if the CDN provider encounters operational issues or goes out of business.

CDN Security Best Practices

Measures that help ensure CDN usage does not compromise organizational security include:

- **Perform a careful CDN evaluation**—There are multiple CDN providers on the market, and it is critical for organizations to consider all options available before committing. It is critical to understand how data is cached and how often penetration testing is completed to ensure the server is secure and understand what happens when the server fails. The CDN provider should be able to address security concerns.
- **Implement a WAF**—CDNs are vulnerable on their own and need to be combined with a WAF that already has CDN capabilities built into its infrastructure. A WAF serves as a barrier between the content and the broader Internet and blocks traffic that is suspect while allowing good traffic through.
- **Ensure compatibility with SSL certificates**—If the organization processes credit card payments, an SSL certificate should be compatible with the SSL certificate. This ensures that information being submitted on the organization's website remains encrypted as it travels through the CDN.
- **Ensure proper content routing**—It is critical that the organization use the proper CDN with the correct content routing procedures. The CDN should be capable of restricting access based on country or region as requested.
- **Implement content deletion and caching controls**—Controls to make information unavailable from the CDN, like deleting the content from the server of origin, should be implemented. Caching should be managed properly by implementing global rules or providing caching options.
- **Implement DR/BC procedures**—DR/BC procedures provide a fallback and business continuity perspective. CDNs should provide near-constant availability and fallback facilities even in cases of extreme widespread system failure.

5.4.9 Network Time Protocol

Network Time Protocol (NTP) is used to synchronize system clocks over packet-switched data networks. It is a built-on UDP and operates at the application layer of the Open Systems Interconnection (OSI) model. NTP is particularly useful when the organization needs to implement a security solution that relies on consistent

©ISACA. All Rights Reserved.

time keeping across the network such as with Kerberos. Some of the benefits of NTP are:

- **Improves security**—NTP reduces the susceptibility of organizational systems to virus attacks and intrusions from malicious actors. This is because a crucial consideration for effective security is accurate timing. Computer systems typically read time in an increasingly progressive linear fashion. Therefore, clock synchronization is necessary when slow and faster systems communicate.
- **Reduces spoofing attacks**—Protocols and servers with synchronization processes using the UDP protocol are prone to spoofing. Attackers typically slow down the Internet clock of a computer to assist in the spoofing process. However, NTP servers can instantly detect such attempts allowing security teams to deal with them before they cause damage to computer systems.
- **Improved accuracy**—NTP synchronizes time more accurately than manual methods by enabling symmetrical network communication between clients. In other words, the length of time it would take for one client's information to reach the server is the same length of time taken for the data to move from the server to the receiving client.
- **Easy configuration**—NTP can be configured by individuals with limited security knowledge.
- **Improved availability**—NTP improves availability by preventing errors or vulnerabilities from disrupting information exchange processes between the server and its clients. It also ensures continuous and consistent timekeeping for the servers.
- **Improved reliability**—Protocols can be made reliable by installing multiple redundant NTP servers. This is because the redundant NTP servers typically stand in for others if there is a hardware failure in the computer environment. Another advantage is that the servers do not need an Internet connection to synchronize time accurately.
- **Improved network management**—In cases of unstable or poor network connections, the NTP is critical as it works differently from Internet time servers. Internet time servers can log users out of a site when there is a poor or lost connection. Unlike Internet time servers whose actions cannot be monitored or traced, NTP ensures continuous monitoring for all servers. Also, NTP servers store working information logs that can be analyzed and traced to the precise time source.
- **Improved compliance**—In some organizations, it is legally compulsory to maintain the synchronization of systems that can be traceable to a source of precise time. Since Internet time servers are untraceable, the only option is NTP. Organizations or industries that must meet these legal standards are groups that deal with sensitive information such as many in the healthcare and financial services industries.

NTP Risk

Although NTP has numerous benefits, it also has a number of weaknesses, some of which are lesser in terms of impact and have alternative options. Some weaknesses do not have solutions at all while others barely have a solution, which makes the protocol untenable in some cases. The IS auditor should be conversant with the risk of NTP to be able to provide assurance regarding its operation and to give advice during implementation and continuous operation. NTP risk includes:

- **Inefficient security options**—The security architectures of symmetric and asymmetric encryption technologies are rarely used with NTP, which makes it less secure. Symmetrical encryption is not commonly used as it operates on the message-digest algorithm (MD5), which has little or no security. The Secure Hash Algorithm 1 (SHA-1) may also be used as a replacement for the MD5 algorithm, but it is less secure. Asymmetric authentication for NTP is based on Autokey, which is another insecure protocol that should not be used.
- **Continues possibility of spoofing attacks**—NTP servers typically prevent spoofing attacks on the server but do not protect all clients at all stages. Clients remain susceptible to spoofing attacks as there are no security controls against time skimming actions. Only clients that are well-built are protected.
- **Addition of UDP fragments**—Adding fake fragments into the stream of fragmented UDP sent by attackers to the receiving client does not alter the timestamp on the communication packet but only changes the time of delivery. Its detection is difficult because a checksum is unnecessary and can also be easily set to zero. This makes the NTP vulnerable to attacks.
- **Vulnerability to kiss-of-death (KoD) attacks**—A KoD attack stops the system's upstream NTP server and enables a DoS attack on the NTP servers. It is a necessary functionality on NTP servers involved in query slow control over short periods of time. However, the functionality is often abused by attackers and used to stop clients from sending queries over an extended period of time. This attack is usually effective as the receiving client rarely matches timestamps.

 ©ISACA. All Rights Reserved.

- **Dependent security protocols**—When NTP is implemented, security protocols become time dependent. An attacker can execute a DoS attack or flush the cache by expiring the time to live record prematurely. This premature expiration is implemented through advancing the system time on a validating resolver. However, if the system time is out back, it makes the servers susceptible to replay attacks.

Best Practices for Using NTP

If not properly configured and secured, NTP can be used to manipulate logs and change the time on the system, thereby changing the sequence of events, making it harder to discover attack attempts. When clocks are not synchronized properly, it is difficult to perform operations such as log correlation across various systems. The IS auditor should ensure that the NTP is properly configured and secured by following best practices such as:

- **Use public NTP for external hosts**—If the organization develops services or other platforms for deployment outside the organization, it is best practice to use a public NTP. This is very important as most public NTPs specify their respective rules of engagement.
- **Ensure hierarchical configuration**—The organization should ensure a hierarchical service is configured for its networks. Stratum 1 or Stratum 0 NTP appliances should be acquired. Setting up a private NTP server is also recommended, which is cost-effective.
- **Standardize coordinated universal time (UTC)**—The best approach is to homogenize all systems within an organization to UTC. This simplifies the correlation of logs within the organization and external groups irrespective of the time zone location where the synchronized device is located.
- **Evaluate the need for cryptography**—Although it is advisable to use encrypted communications and authentications, cryptography has its own challenges, including complex key management processes and increased systems management costs. An evaluation should be made before its implementation.
- **Use at least two servers**—Using at least two servers enables the organization to maintain redundancy in case one server fails. Most NTP software allows minimum fail-over capabilities to a second server should the first one experiences any issues. More servers can be added but the minimum recommendation is a pair of servers.
- **Limit strata levels**—The organization may have in place stratum levels, depending on the complexity of the NTP device network, with each stratum adding a risk of loss of accuracy. It is therefore advisable to limit the levels as much as possible to help mitigate the risk.
- **Monitor server functionality**—It is important to monitor the function of NTP servers on a continuous basis to get real-time status information about the time server. Such information includes circumstances and times when the Global Positioning System (GPS) signal is lost, for example. If Simple Network Management Protocol (SNMP) is already configured, monitoring is easier.

5.4.10 Applications in a Networked Environment

There are different types of applications used in networked architecture.

Client-Server Technology

Client-server is a network architecture in which each computer or process on the network is either a server (a source of services and data) or a client (a user that relies on servers to obtain services and data). With client-server technology, the available computing power can be distributed and shared among the client workstations. Use of client-server technology is one of the most popular trends in building applications aimed at networked environments. Often, in a client-server network environment, the server provides data distribution and security functions to other computers that are independently running various applications.

Client-server architecture has a number of advantages, such as distributing the work among servers and performing as much computational work as possible on the client workstation to save bandwidth and server computing power. Important tasks, such as manipulating and changing data, may be performed locally and without the need for controlling resources on the main processing unit. In this way, applications may run more efficiently.

To achieve these advantages, client-server application systems are split so that processing may take place on different machines (e.g., servers and clients). Each processing component is mutually dependent on the others. The fact that tasks are performed on both client and server is the main difference between client-server processing and traditional mainframe/distributed processing.

©ISACA. All Rights Reserved.

The typical client is a single PC or workstation. Presentation usually is provided by a graphical user interface (GUI). Clients may be thick or thin. A thin client (sometimes called a lean client) is a client computer or software that depends primarily on the central server for processing activities and mainly focuses on conveying input and output between the user and the remote server. Many thin client devices run only web browsers or remote desktop software, meaning that all significant processing occurs on the server. In contrast, a thick, or fat, client does as much processing as possible and passes only data for communications and storage to the server.

The server is one or more multiuser computers. Server functions include any centrally supported role, such as file-sharing, printer-sharing, database access and management, communication services, email services and processing application logic. Multiple functions may be supported by a single server.

Client-server architecture can be composed of two tiers:
- A thick client, focused on GUI tasks and running the application logic
- A group (one or more) of database servers

The main disadvantages of this model are the requirement to keep the programs on the clients synchronized (ensuring that they are running the same logic) and limited scalability.

Client-server architecture is normally based on (at least) three levels of computing tasks (i.e., three-tier architectures). A three-tier architecture is composed of:
- A thin client, focused on GUI tasks (most often but not always via web browsers)
- A group (one or more) of application servers, focused on running the application logic
- A group (one or more) of database servers

This architecture does not have the limitations of two-tier applications and has other advantages, such as:
- Thin clients are less complex and less costly to buy and maintain.
- There is more scalability (up to several thousands of concurrent users) because the load is balanced among different servers. This, in turn, improves overall system performance and reliability since more of the processing load can be accommodated simultaneously.
- It can be implemented in applications for internal usage only or in e-business applications (in this case, there could be another tier represented by the web server).
- All of the program logic is separated from the rest of the code (via application servers).

Designs that contain more than two tiers are referred to as multi-tiered or n-tiered. N-tiered architecture applications are more complex to build and more difficult to maintain.

In an n-tiered environment, each instance of the client software can send data requests to one or more connected servers. In turn, the servers can accept the requests, process them and return the requested information to the client. This concept can be applied to many different kinds of applications with the architecture remaining fundamentally the same. The interaction between client and server is often described using sequence diagrams. Sequence diagrams are standardized in the Unified Modeling Language.

Note

Implicit in n-tiered architectures is the presence of middleware that supports not just communications between clients and servers, but more advanced features such as load balancing and fail over, dynamic location of components, and establishing synchronous connections or asynchronous queue-based messages.

Client-Server Security

The security of a client-server environment is dependent on the security of its component parts. This includes the security of the:
- LAN
- Client
- OS
- Database
- Middleware

In a client-server environment, several access routes exist because application data may exist on the server or on the client. Therefore, each of these routes must be examined individually and in relation to each other to ensure that no exposures are left unchecked.

An additional risk to consider with the client-server model is the potential gaps among the components. In other words, how do the components connect to each other?

For example, in a two-tiered environment, the thick client must connect to the database. To achieve this, either (1) all users have database accounts, in which case they may be able to bypass the client application (and hence the application controls) and connect directly to the database or (2) a proxy user (i.e., a single account that connects

to the database on behalf of all others) is used, in which case the database password must be stored somewhere, and it might be stored insecurely or unencrypted.

In a client-server environment the IS auditor should ensure that:
- Application controls cannot be bypassed.
- Passwords are always encrypted.
- Access to configuration or initialization files is kept to a minimum.
- Access to configuration or initialization files is audited.

Middleware

Middleware is a client-server specific term used to describe a unique class of software employed by client-server applications. Middleware serves as the glue between two otherwise distinct applications and provides services such as identification, authentication, authorization, directories and security. This software resides between an application and the network and manages the interaction between the GUI on the front end and data servers on the back end. Middleware facilitates the client-server connections over the network and allows client applications to access and update remote databases and mainframe files.

Middleware is commonly used for:
- **Transaction processing (TP) monitors**—Programs that handle and monitor database transactions and are used primarily for load balancing
- **Remote procedure calls (RPC)**—A protocol that enables a program on the client computer to execute another program on a remote computer (usually a server)
- **Object request broker (ORB) technology**—The use of shared, reusable business objects in a distributed computing environment. This technology enables support for interoperability across languages and platforms and enhances maintainability and adaptability of the system. Examples are Common Object Request Broker Architecture (CORBA) and Microsoft's Component Object Model/Distributed Component Object Model (COM/DCOM).
- **Messaging servers**—Programs that asynchronously prioritize, queue and/or process messages using a dedicated server

Risk and controls associated with middleware in a client-server environment are:
- **Risk**—System integrity may be adversely affected because of the very purpose of middleware, which is to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in a loss of data or program integrity.
- **Controls**—Management should implement compensating controls to ensure the integrity of the client-server networks. Management should ensure that systems are properly tested and approved, modifications are adequately authorized and implemented, and appropriate version control procedures are followed.

On-Demand Computing

On-demand computing (ODC), also referred to as utility computing, is a computing model in which IS resources are allocated to users according to their current needs. The resources could be available within an organization or supplied by a third-party SP. At any moment, a user (or organization) may need more bandwidth, central processing unit (CPU) cycles, memory, application availability or other resource to a greater degree than another user. When that situation occurs, the resource can be made available to the user with the immediate need and taken away from the user with the lesser need.

A benefit of ODC is that an organization that is outsourcing its computing needs does not have to pay for excess computing capacity. A concern is the confidentiality of information maintained by the third-party provider.

5.4.11 Network Infrastructure Security

Communication networks (i.e., WANs or LANs) generally include devices connected to the network as well as programs and files supporting the network operations. Control is accomplished through a network control terminal and specialized communications software.

Controls over the communication network include:
- Network control functions should be performed by individuals possessing adequate training and experience.
- Network control functions should be separated, and the duties should be rotated on a regular basis, if possible.
- Network control software must restrict operator access from performing certain functions (e.g., the ability to amend/delete operator activity logs).
- Network control software should maintain an audit trail of all operator activities.

©ISACA. All Rights Reserved.

- Audit trails should be periodically reviewed by operations management to detect any unauthorized network operation activities.
- Network operation standards and protocols should be documented and made available to the operators and should be reviewed periodically to ensure compliance.
- Network access by the system engineers should be monitored and reviewed closely to detect unauthorized access to the network.
- Analysis should be performed to ensure workload balance, fast response time and system efficiency.
- A terminal identification file should be maintained by the communications software to check the authentication of a terminal when it tries to send or receive messages.
- Data encryption should be used, when appropriate, to protect messages from disclosure during transmission.
- Restrictions should be placed on remote printing facilities to ensure sensitive documents cannot be read by unauthorized personnel.
- Device hardening should be used to keep devices up to date. That means upgrading firmware, patching, and installing updates to fix any security gaps.

To improve the control and maintenance of the infrastructure and its use, besides the direct management of the network devices, consolidate the logs of the devices with the firewall's logs and the client-server OS's logs.

In recent years, the management of large capacity storage units is frequently based on FC connections.

System security is improved when a dynamic inventory of devices is possible. In the case of an incident, it is important to know which computer is used by whom.

Another important security improvement is the ability to identify users at every step of their activity. Some application packages use predefined names (e.g., SYSTEM). New monitoring tools have been developed to resolve this problem.

Adopting an IT governance practice enables an organization to comply with network security requirements effectively. For example, the Information Technology Infrastructure Library (ITIL) is a framework of practice guidance in information technology service management that can be used in setting up SLAs, specifically for enterprise network operations, to maintain the uninterrupted operation of the network through controls, incident handling and auditing.

Internet Security Controls

To establish effective Internet security, an organization must develop controls within an IS security framework from which Internet security controls can be implemented and supported. Generally, the process for establishing such a framework entails defining, through corporate policies and procedures, the rules the organization will follow to control Internet use. For example, one set of rules should address appropriate use of Internet resources with rules that might reserve Internet privileges for those with a business need, define what information resources should be available for outside users, and define trusted and untrusted networks within and outside the organization. Another set of rules should address the classification of the sensitivity or criticality of corporate information resources. This will help to determine what information will be available for use on the Internet and the level of security to be used for corporate resources of a sensitive or critical nature on the Internet.

From an evaluation of these issues, an organization will be able to develop guidelines specific to its situations for defining the level of security controls related to the CIA of information resources (i.e., business applications) on the Internet. For example, OS security hardening guidelines can be developed that define how the OS should be configured, detail which Internet services should be blocked from use or could be exploited by external untrusted users and define how the system will be protected by firewalls. Additionally, supporting processes over controls should be defined, including:

- Risk assessments performed periodically over the development and redesign of Internet-based web applications
- Security awareness and training for employees, tailored to their levels of responsibilities
- Firewall standards and security to develop and implement firewall architectures
- Intrusion detection standards and security to develop and implement IDS architectures
- Remote access for coordinating and centrally controlling dial-up access on the Internet via corporate resources
- Incident handling and response for detection, response, containment and recovery
- Configuration management for controlling the security baseline when changes occur
- Encryption techniques applied to protect information assets passing over the Internet

 ©ISACA. All Rights Reserved.

- A common desktop environment to control, in an automated fashion, what is displayed on a user's desktop
- Monitoring Internet activities for unauthorized use and notification to end users of security incidents via computer emergency response team (CERT) bulletins or alerts

5.4.12 Firewalls

Every time a corporation connects its internal computer network to the Internet, it faces potential danger. Because of the Internet's openness, every corporate network connected to it is vulnerable to attack. Hackers on the Internet could theoretically break into the corporate network and do harm in several ways. Companies should build firewalls as one means of perimeter security for their networks. Likewise, this principle holds true for sensitive or critical systems that need to be protected from untrusted users inside the corporate network (internal hackers). A firewall is defined as a device installed at the point where network connections enter a site. Firewalls apply rules to control the type of networking traffic flowing in and out. Most commercial firewalls are built to handle the most used Internet protocols.

To be effective, firewalls should allow individuals on the corporate network to access the Internet and, at the same time, stop hackers or others on the Internet from gaining access to the corporate network to cause damage. Generally, most organizations will follow a deny-all philosophy, which means that access to a given resource will be denied unless a user can provide a specific business reason or need for access to the information resource. The converse of this access philosophy, not widely adopted, is the accept-all philosophy, which means everyone is allowed access unless someone can provide a reason for denying access.

Firewall General Features

Firewalls are hardware and software combinations that are built using routers, servers and a variety of software. They separate networks from each other and screen the traffic between them. Thus, along with other types of security, they control the most vulnerable point between a corporate network and the Internet, and they can be as simple or complex as the corporate information security policy demands. There are many different types of firewalls, but most enable organizations to:

- Block access to particular sites on the Internet
- Limit traffic on an organization's public services segment to relevant addresses and ports
- Prevent certain users from accessing certain servers or services
- Monitor communications and record communications between an internal and an external network
- Monitor and record all communications between an internal network and the outside world to investigate network penetrations or detect internal subversion
- Encrypt packets that are sent between different physical locations within an organization by creating a VPN over the Internet (i.e., IPSec, VPN tunnels)

The capabilities of some firewalls can be extended so they can also provide protection against viruses and attacks directed to exploit known OS vulnerabilities.

Firewall Types

Generally, firewalls are classified into three categories:

- Packet filtering
- Application firewall systems
- Stateful inspection

Packet Filtering Firewalls

The simplest and earliest kinds of firewalls (i.e., first generation of firewalls) are packet filtering-based firewalls deployed between the private network and the Internet. In packet filtering, a screening router examines the header of every packet of data traveling between the Internet and the corporate network. Information contained in packet headers includes the IP address of the sender and receiver and the authorized port numbers (application or service) allowed to use the information transmitted. Based on that information, the router knows what kind of Internet service, such as web-based or FTP, is being used to send the data, as well as the identities of the sender and receiver of the data. Using that information, the router can prevent certain packets from being sent between the Internet and the corporate network. For example, the router could block any traffic except for email or block traffic to and from suspicious destinations.

The advantages of this type of firewall are its simplicity and generally stable performance, as the filtering rules are performed at the network layer. Its simplicity is also a disadvantage, because it is vulnerable to attacks from improperly configured filters and attacks tunneled over permitted services. Because the direct exchange of packets is permitted between outside systems and inside systems, the potential for an attack is determined by the total number of hosts and services to which the packet filtering router permits traffic. Also, if a single packet filtering router is compromised, every system on the private network may be compromised, and organizations

©ISACA. All Rights Reserved.

with many routers may face difficulties in designing, coding and maintaining the rule base. This means that each host directly accessible from the Internet needs to support sophisticated user authentication and needs to be regularly examined by the network administrator for signs of attack.

Some of the more common attacks against packet filter firewalls are:

- **IP spoofing**—The attacker fakes the IP address of either an internal network host or a trusted network host so that the packet being sent will pass the rule base of the firewall. This allows for penetration of the system perimeter. If the spoofing uses an internal IP address, the firewall can be configured to drop the packet based on packet flow direction analysis. However, if the attacker has access to a secure or trusted external IP address and spoofs that address, the firewall architecture is defenseless.
- **Source routing specification**—It is possible to define the routing that an IP packet must take when it traverses from the source host to the destination host across the Internet. With this process, it is possible to define the route so it bypasses the firewall. Only those who know the IP address, subnet mask and default gateway settings at the firewall routing station can do this. A clear defense against this attack is to examine each packet and, if the source routing specification is enabled, drop that packet. However, if the topology permits a route, skipping the choke point, this countermeasure will not be effective.
- **Miniature fragment attack**—Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall in the hope that only the first of the sequence of fragmented packets will be examined and the others will pass without review. This can occur if the default setting is to pass residual packets. This can be countered by configuring the firewall to drop all packets where IP fragmentation is enabled.

Application Firewall Systems

There are two types of application firewall systems —application-level and circuit-level firewall systems. They provide greater protection capabilities than packet filtering routers. Packet filtering routers allow the direct flow of packets between internal and external systems. Application and circuit gateway firewall systems allow information to flow between systems but do not allow the direct exchange of packets. The primary risk of allowing packet exchange between internal and external systems is that the host applications residing on the protected network's systems must be secure against any threat posed by the allowed packets.

Application firewall systems can be an appliance or sit atop hardened (tightly secured) OSs, such as Windows or Unix. They work at the application level of the OSI model. The application-level gateway firewall is a system that analyzes packets through a set of proxies—one for each service (e.g., HTTP proxy for web traffic, FTP proxy). An HTTP proxy is known as a WAF. This applies rules to HTTP conversations that cover known attacks, such as cross-site scripting (XSS) and Structured Query Language (SQL) injection, which could reduce network performance. Circuit-level firewalls are more efficient and also operate at the application level—where TCP and UDP sessions are validated, typically through a single general-purpose proxy before opening a connection. Commercially, circuit-level firewalls are quite rare.

Both application firewall systems employ the concept of bastion hosting in that they handle all incoming requests from the Internet to the corporate network, such as FTP or web requests. Bastion hosts are heavily fortified against attack. By having only a single host handling incoming requests, it is easier to maintain security and track attacks. Therefore, in the event of a break-in, only the firewall system is compromised, not the entire network. In this way, none of the computers or hosts on the corporate network can be contacted directly for requests from the Internet, providing an effective level or layer of security.

Additionally, application-based firewall systems are set up as proxy servers to act on behalf of someone inside an organization's private network. Rather than relying on a generic packet filtering tool to manage the flow of Internet services through the firewall, a special-purpose code called a proxy server is incorporated into the firewall system. For example, when someone inside the corporate network wants to access a server on the Internet, a request from the computer is sent to the proxy server, the proxy server contacts the server on the Internet, and the proxy server then sends the information from the Internet server to the computer inside the corporate network. By acting as a go-between, proxy servers can maintain security by examining a service's (e.g., FTP, Telnet) program code and modifying and securing it to eliminate known vulnerabilities. The proxy server can also log all traffic between the Internet and the network.

The application-level firewall implementation of proxy server functions is based on providing a separate proxy for each application service (e.g., FTP, Telnet and

HTTP). This differs from circuit-level firewalls, which do not need a special proxy for each application-level service. In other words, one proxy server is used for all services.

Advantages of these types of firewalls are that they provide security for commonly used protocols and generally hide the internal network from outside untrusted networks. For example, a feature available on these types of firewall systems is the network address translation (NAT) capability. This capability takes private internal network addresses (unusable on the Internet) and maps them to a table of public IP addresses, assigned to the organization, which can be used across the Internet.

Disadvantages are poor performance and scalability as Internet usage grows. To offset this problem, the concept of load balancing is applicable when a redundant fail-over firewall system may be used.

Stateful Inspection Firewalls

A stateful inspection firewall keeps track of the destination IP address of each packet that leaves the organization's internal network. Whenever the response to a packet is received, its record is referenced to ascertain and ensure that the incoming message is in response to the request that went out from the organization. This is done by mapping the source IP address of an incoming packet with the list of destination IP addresses that is maintained and updated. This approach prevents any attack initiated and originated by an outsider.

The advantage of this approach over application firewall systems is that stateful inspection firewalls control the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets at the transport layer against a set of rules specified by the firewall administrator. This provides a greater degree of efficiency when compared to typical CPU-intensive, full-time application firewall systems' proxy servers, which may perform extensive processing on each data packet at the application level.

A disadvantage of stateful inspection firewalls is that they can be relatively complex to administer, compared to the other two types of firewalls.

Next Generation Firewalls

A next generation firewall (NGFW) combines traditional firewall capabilities like packet filtering and stateful inspection with newer technologies to make better decisions regarding allowing or denying traffic to pass through. It can filter packets based on applications and inspect the data contained in packets and operate at layers up to layer 7 of the OSI model. NGFWs can also block modern threats such as advanced malware and application-layer attacks. From an IS audit perspective, NGFWs are more advanced versions of traditional firewalls. Except for the ability to filter traffic based on applications, they are similar in that they both use static and dynamic packet filtering and VPN support. However, there are significant differences. NGFWs typically have extensive control and visibility of applications and can identify attacks using analysis and signature matching. They also employ allowlists or signature-based IPSs to distinguish between safe applications and risky ones. Also, unlike regular firewalls, NGFWs include a path through which future updates are received.

While NGWF specifications vary by provider, they generally include some combination of:

- **Application awareness**—NGFWs can filter traffic and apply complex rules based on applications rather than only based on specific ports. They can block traffic from certain applications and maintain greater control over individual applications.
- **Deep packet inspection (DPI)**—DPI inspects the data contained in packets and is an improvement over traditional firewall technology, which only inspected a packet's IP header to determine its source and destination.
- **IDS/IPS**—NGFWs incorporate IDS/IPS solutions to monitor the network for malicious activity and block traffic where malicious activities occur. This monitoring can be signature-based, policy-based or anomaly-based.
- **High performance**—NGFWs have high performance, which allows the firewall to monitor large amounts of network traffic without slowing down. They include a number of security features that require processing time, so high performance is critical to avoid disrupting business operations.
- **Threat intelligence**—NGFWs have threat intelligence features and communicate with a threat intelligence network to ensure that threat information is up to date and to help identify bad actors.
- **Antimalware**—NGFWs may provide additional features such as antivirus and malware protection. These help in preventing malicious software from infecting the organization's systems.
- **Firewall as a Service (FWaaS)**—This is a cloud-based service that provides scalability and ease of maintenance. With FWaaS the firewall software is maintained by the SP, and resources scale automatically to meet processing demands, freeing

©ISACA. All Rights Reserved.

enterprise IT teams from dealing with the burden of handling patches, upgrades and sizing.

Benefits of NGFWs

The IS auditor should view NGFWs as an improvement to the traditional firewall, with more benefits. It is therefore crucial for the IS auditor to validate that an NGFW accomplishes its stated functions prior to advising management on its implementation. Some of the benefits of NGFWs include:

- **Robust security**—NGFWs provide more robust security than a traditional firewall due to their context-awareness nature. They can also receive updates from external threat intelligence networks, thus enabling protection against various threats. This increases the overall security posture of the organization.
- **Intelligent automation**—Intelligent automation is typically incorporated in NGFWs to update security policies and respond to security events without intervention from the IS security teams. NGFWs can recognize many aspects of organizational systems such as applications independent of ports, protocols and evasive tactics. Upon recognizing applications, they can provide real-time protection by limiting or restricting the use of functionalities.
- **Streamlined security architecture**—A streamlined security architecture is recommended, as makes it easier and cheaper to manage the security infrastructure. The process involves combining several security features into one solution and reporting identified incidents through a single reporting system.

Web Application Firewall

A WAF is a type of firewall that protects web applications by filtering, monitoring and blocking malicious traffic traveling to web applications and preventing unauthorized data from leaving the applications. It operates similarly to a reverse proxy as an intermediary that protects the web app server from a potentially malicious client. There is a need to update policies when using WAFs; however, some have the capability to update themselves using artificial intelligence (AI). WAFs require the regular updating of policies to address new vulnerabilities. However, advances in machine learning (ML) now enable some WAFs to update automatically. The major difference between proxies and WAFs is that while proxies generally protect clients, WAFs protect servers and are deployed to protect a specific web application or set of web applications. The IS auditor should be aware of the following functions of WAFs:

- **Protection of inbound traffic**—This functionality enables the inspection of application traffic from the outside world. It is critical for the WAF to be able to identify dangerous activity patterns, suspicious payloads and vulnerabilities.
- **Protection of outbound traffic**—This is concerned with the protection of data leakage. Inline WAFs can intercept outbound data and/or block sensitive data from leaking due to accidental or malicious activities.

WAFs can be distinguished by how they work as well as by their deployment. In terms of how they work, they can be categorized into blocklist and whitelist WAFs. In terms of deployment, they are classified as network-based, host-based and cloud-based. Brief descriptions of these classifications are provided in **figure 5.21**.

 ©ISACA. All Rights Reserved.

Figure 5.21—Types of Web-Application Firewalls (WAFs)

Type of WAF	Description
Blocklist	Blocklist WAFs are designed to block certain traffic identified as threats while allowing all other traffic to pass through. They are based on the negative security model in which certain inputs or requests are rejected according to the blocklist. The WAF, on a blocklist basis, protects against known security attacks. Its downside is that it requires continuous monitoring and updating of the blocklist to be effective.
Allowlist	Allowlist WAFs block all traffic by default and allow only explicitly preapproved traffic to pass through. They are based on the positive security model and are generally considered more secure as they minimize the risk of malicious traffic evading defenses due to improperly configured firewall rules. The IS auditor should note that most WAFs operate under the hybrid security model, thus benefiting from the advantages of both the positive security model and the negative security model.
Network-based	A network-based WAF is a hardware appliance that has to be licensed and maintained and operates on network infrastructure, such as a switch. It sits between applications and the Internet and is installed locally to minimize latency. However, it is very expensive and requires the storage and maintenance of physical equipment.
Host-based WAF	Host-based WAFs are co-located with web applications on servers. They are normally deployed as a part of the operating system (OS) of the application, and they are easy to scale. This solution is cheaper and more customizable than network-based WAFs. The drawbacks are that they are complex to implement and very expensive to maintain. The machine used to run a host-based WAF also requires hardening and customization, which is time-consuming.
Cloud-based WAF	A cloud-based WAF integrates with cloud virtual networking services or load balancers to filter web traffic. It requires minimal effort to deploy but does not offer clear visibility into threats. It leads to significant cost savings because it can be updated regularly at no further cost or effort on the part of the user.

NGFWs and WAFs Compared

It is not uncommon for IS auditors to confuse NGFW with WAF or use the terms interchangeably. This is because there are only slight differences between the two security technologies. NGFW can be thought of as the entrance to an office complex and the WAF as the key to the manager's office. **Figure 5.22** shows the major differences between the NGFW and the WAF.

Figure 5.22—Comparison of Next Generation Firewall and Web-Application Firewall

Key Aspect	Next Generation Firewall (NGFW)	Web-Application Firewall (WAF)
Location of operation	The NGFW operates close to the organization on the network (Layers 3-4).	The WAF's area of operation is close to the applications (Layer 7).
Operating methodology	The NGFW operates as a filter to protect the network against network access.	The WAF regularly inspects the web applications for unusual behavior and sends alerts.
Purpose	The NGF protects the internal network and its users and separates the network into secure and non-secure zones.	The WAF protects the data moving across web-facing applications.
Capabilities	The NGFW protects against attacks on protocols such as Domain Name System (DNS), File Transfer Protocol (FTP) and Secure Socket Shell (SSH). It can add further security features such as antimalware and antivirus solutions.	The WAF is capable of detecting web application attacks such as cross-site scripting (XSS), cross-site request forgery (CSRF), L7 distributed denial of service (DDoS), injection and broken authentication.

©ISACA. All Rights Reserved.

Examples of Firewall Implementations

Firewall implementations can take advantage of the functionality available in a variety of firewall designs to provide a robust layered approach in protecting an organization's information assets. Commonly used implementations include:

- **Screened-host firewall**—Using a packet-filtering router and a bastion host, this approach implements basic network layer security (packet filtering) and application server security (proxy services). An intruder in this configuration has to penetrate two separate systems before the security of the private network can be compromised. This firewall system is configured with the bastion host connected to the private network with a packet filtering router between the Internet and the bastion host. Router filtering rules allow inbound traffic to access only the bastion host, which blocks access to internal systems. Because the inside hosts reside on the same network as the bastion host, the security policy of the organization determines whether inside systems are permitted direct access to the Internet or whether they are required to use the proxy services on the bastion host.
- **Dual-homed firewall**—This is a firewall system that has two or more network interfaces, each of which is connected to a different network. In a firewall configuration, a dual-homed firewall usually acts to block or filter some or all of the traffic trying to pass between the networks. A dual-homed firewall system is a more restrictive form of a screened-host firewall system, in which a dual-homed bastion host is configured with one interface established for information servers and another for private network host computers.
- **Demilitarized zone (DMZ) or screened-subnet firewall**—Using two packet-filtering routers and a bastion host, this approach creates the most secure firewall system because it supports network- and application-level security while defining a separate DMZ network. The DMZ functions as a small, isolated network for an organization's public servers, bastion host information servers and modem pools. Typically, DMZs are configured to limit access from the Internet and the organization's private network. Incoming traffic access is restricted to the DMZ network by the outside router and protects the organization against certain attacks by limiting the services available for use. Consequently, external systems can access only the bastion host (and its proxying service capabilities to internal systems) and possibly information servers in the DMZ. The inside router provides a second line of defense, managing DMZ access to the private network, while accepting only traffic originating from the bastion host. For outbound traffic, the inside router manages private network access to the DMZ network. It permits internal systems to access only the bastion host and information servers in the DMZ. The filtering rules on the outside router require the use of proxy services by accepting only outbound traffic on the bastion host. The key benefits of this system are that an intruder must penetrate three separate devices, private network addresses are not disclosed to the Internet, and internal systems do not have direct access to the Internet.

Firewall Issues

Issues related to implementing firewalls include:

- A false sense of security may exist if management feels that no further security checks and controls are needed on the internal network (e.g., most incidents are caused by insiders who are not controlled by firewalls).
- The circumvention of firewalls using modems may connect users directly to ISPs. Management should provide assurance that the use of modems when a firewall exists is strictly controlled or prohibited altogether.
- Misconfigured firewalls may allow unknown and dangerous services to pass through freely.
- What constitutes a firewall may be misunderstood (e.g., companies claiming to have a firewall merely have a screening router).
- Monitoring activities may not occur on a regular basis (e.g., log settings are not appropriately applied and reviewed).
- Firewall policies may not be maintained regularly.
- Most firewalls operate at the network layer; therefore, they do not stop any application-based or input-based attacks. Examples of such attacks include SQL injection and buffer-overflow attacks. Newer-generation firewalls are able to inspect traffic at the application layer and stop some of those attacks.

Firewall Platforms

Firewalls may be implemented using hardware or software platforms. When implemented in hardware, a firewall will provide good performance with minimal system overhead. Although hardware-based firewall platforms are faster, they are not as flexible or scalable as software-based firewalls. Software-based firewalls are generally slower with significant systems overhead; however, they are flexible with additional services. They

 ©ISACA. All Rights Reserved.

may include content and virus checking before traffic is passed to users. It is generally better to use appliances, rather than normal servers, for a firewall. Appliances are normally installed with hardened OSs. When server-based firewalls are used, OSs in servers are often vulnerable to attacks. When the attacks on OSs succeed, the firewall is compromised. Appliance-type firewalls are generally significantly faster to set up and recover.

5.4.13 Unified Threat Management (UTM)

Unified threat management (UTM) refers to a solution in which multiple security features or services are combined into a single device within the organizational network.

Using UTM, a network's users are protected with several different features, including antivirus, content filtering, email and web filtering and anti-spam. Common features that an ideal UTM solution must possess are shown in **figure 5.23**.

Figure 5.23—Unified Threat Management (UTM) Components

UTM Component	Description
Antivirus	A UTM solution should be equipped with antivirus software that can monitor network activity and detect and stop viruses from damaging the system or any of its connected devices. The antivirus leverages data contained in signature databases to check if there are any active viruses attempting to gain access. Some of the threats the antivirus software within a UTM can mitigate include infected files, Trojans, worms and spyware.
Antimalware	A UTM protects networks against malware by detection and response. It can be configured to detect known malware, filter it from the organization's data streams and block it from penetrating the system. The UTM can also be configured to detect even novel threats of malware. It leverages techniques such as heuristics, which involve rules that analyze the behavior and characteristics of files.
Sandboxing	A UTM can deploy a sandboxing solution to prevent malware. Sandboxing involves confining a cell inside the system to a sandbox that captures the suspicious file. If the malware is allowed to run, the sandbox prevents it from interacting with other programs in the computer.
Firewall	A UTM should come with a firewall configured to scan incoming and outgoing traffic for attack attempts on the network. Firewalls also prevent all forms of devices from acting as attack vectors for malware.
Intrusion detection system (IDS)/Intrusion prevention system (IPS)	An IDS/IPS included as part of UTM has the advantage of detecting and preventing attacks at the same time.
Virtual private network (VPN)	A VPN is typically incorporated into UTM to create a private network that tunnels through a public network, enabling users to send and receive encrypted data through the public network. If an attacker were to intercept the data it would be useless, as it would be encrypted.
Data loss prevention (DLP)	The DLP solution is attached to a UTM appliance to enable the user to detect and prevent data breaches and exfiltration attempts. It typically monitors sensitive data, and when it identifies any threats by an attacker, it blocks such threats, thereby protecting the data.
Web filtering	A UTM's web filtering feature can prevent users from seeing specific websites or URLs. This is done by stopping users' browsers from loading the pages from those sites onto their devices. Web filters can be configured to target certain sites according to organizational objectives.

©ISACA. All Rights Reserved.

Benefits of Using a UTM

UTM is critical to the improvement of the organization's security posture and has many advantages that IS auditors can provide assurance on. Some advantages of a UTM:

- **Improves security flexibility**—With a UTM network, an organization can use a set of flexible solutions from the available pool of security tools to handle its security requirements. This saves both time and money involved in searching for individual security solutions.
- **Promotes security adaptability**—A UTM can be used to adapt the organization's security architecture to suit its business model. It comes with automatic updates that keep the system prepared to deal with the latest threats in the security landscape.
- **Enhances security visibility**—The centralized nature of a UTM allows security professionals to monitor several threats simultaneously as they impact multiple components of the organizational network. In a network without a centralized structure, it is often difficult to prevent multi-module attacks.
- **Reduces costs**—Because of its centralized setup, a UTM reduces the number of devices an organization needs to adequately protect its network. In addition, because fewer staff are required to monitor the system the organization can save on employment costs.
- **Increases security risk awareness**—The combination of a UTM's centralization and faster operation results in increased awareness of network security threats, enabling organizations to implement advanced persistent threat (APT) protection mechanisms. The IT team will be better equipped to manage APTs and other modern risk factors in the threat landscape.
- **Encourages faster security solutions**—With a UTM, it is possible to streamline the way data is processed and use fewer resources simultaneously. The UTM does not require as many resources as several components operating independent of each other. This higher efficiency in the use of UTM solutions allows organizations to free up resources to better manage other essential network-dependent processes.
- **Reduces security complexities**—With a UTM, an organization transitions from multiple standalone security products to a single solution. This single tool is easier to configure, update and manage than an array of independent solutions.
- **Simplifies security monitoring and compliance**—UTM solutions with identity-based security policies simplify the process of implementing access controls based on least privilege. This makes it easier to meet the access control requirements of regulations.

5.4.14 Network Segmentation

Network segmentation is splitting a network into smaller parts to improve network performance and security. It is sometimes known as network partitioning or network isolation. Network segmentation results in multiple network zones, each with its own specific security requirements. By separating the network into smaller networks, the organization's IS infrastructure is isolated from the entire network.

Network segmentation is often confused with micro-segmentation. While the two concepts have many similarities, such as reducing an organization's network attack surface, there are some marked differences. For example, network segmentation typically refers to segmentation as applied on the physical level and is typically hardware based, while micro-segmentation is virtual and typically software based. Another distinction is that micro-segmentation is a generally a more granular form of network segmentation and involves placing each device or application within its own virtual segment, providing greater network control than network segmentation. Network segmentation breaks down the network based on north-south traffic (i.e., traffic flowing clients and servers and across the security perimeter). In contrast, micro-segmentation focuses on east-west traffic (i.e., traffic flowing laterally across and within the network). Despite these differences, the IS auditor should treat network segmentation and micro-segmentation as related concepts with virtually similar benefits, challenges and best practices.

Methods of Network Segmentation

Some of the ways an organization can segment its network include:

- **VLAN segmentation**—Networks can be segmented using VLANs or subnets to create smaller segments to connect to hosts virtually. The created subnets use IP addresses to segment the network and are connected by network devices. The major limitation of creating network segments using VLANs is that the approach is complex requiring regular re-architecting.
- **Firewall segmentation**—Various types of firewalls can be used to enforce network segmentation. When firewalls are deployed inside the network, they can create internal network zones. In this way functional areas of an organization are separated from each other.

 ©ISACA. All Rights Reserved.

- **Software-Defined Networking (SDN) segmentation**—SDN segmentation is a more modern approach to network segmentation and is typically applied in micro-segmentation. The approach applies an SDN-automated network overlay to created network segments. The challenges with SDN segmentation are that it is complex and difficult to manage and control.
- **Host-based segmentation**—Host segmentation relies on special dedicated software that is installed on network endpoints for the purpose of reporting data to a central location. It uses technologies such as workload telemetry and visualization to map multi-cloud environments that can be easily managed from a central dashboard. This approach provides visibility into the overall network segmentation process.

Benefits of Network Segmentation

Network segmentation offers several benefits to an organization when implemented properly. Some of the benefits of network segmentation include:

- **Improves operational performance**—One of the major advantages of network segmentation is that it reduces network congestion. Generally, as a network grows, congestion increases and performance decreases considerably. Network segmentation solves this challenge by creating smaller network segments that perform better. Reduced congestion leads to better load balancing and limited traffic channeled to specific zones according to needs.
- **Limits attack damage**—Network segmentation improves the security posture of an organization by limiting the extent an attack can spread once it is launched. By reducing the attack surface, the extent of damage is also reduced as it is contained in a specific zone. For instance, network segmentation can keep a malware outbreak in a single zone and prevent it from spreading to other zones.
- **Protects vulnerable devices**—Effective network segmentation can prevent malicious traffic from reaching network devices that are vulnerable to attacks by threat actors. In an organization, some devices may not be secure enough or appropriately hardened to withstand attacks.
- **Improves compliance**—Network segmentation minimizes compliance costs by limiting the number of systems within the compliance scope. A typical example is network segmentation separating systems that process payments from those that do not. This means that the costly, often time-consuming, and mandatory compliance and audit requirements only apply to in-scope systems.
- **Enhances security**—Network segmentation creates multi-layer security perimeters and effectively implements the principle of defense-in-depth. The creation of network boundaries between various sub-segments hinders lateral movement by attackers and makes it easier to detect them. Another way security is enhanced is through localization of security rules to segments.
- **Improves network monitoring**—Monitoring of network segments is enhanced through greater visibility of the segments by IS security personnel. IS security professionals can easily detect threats and vulnerabilities in a network segment due to its smaller size and scope. The segments also make it easier to quickly isolate threats before they propagate throughout the entire network.

Network Segmentation Best Practices

Best practices to consider in network segmentation include:

- **Avoid under or over segmentation**—The organization should guard against under segmentation and over segmentation and aim for optimal segmentation.
- **Perform regular network audits**—Regular network audits, which include vulnerability assessments and penetration tests, should be carried out to identify any security gaps in the network segmentation and whether the existing network segmentation plan is still current and relevant.
- **Control third-party access**—The maintenance of specific APs for third parties is one of the core tenets of best network segmentation practices. Controlling third-party access to the organization's critical systems and sensitive information should be prioritized. One of the controls that can be implemented to restrict third-party access is to create separate portals to serve each third party, isolating and limiting damages in the event of an attack.
- **Combine similar network resources**—Effective network segmentation is achieved when similar network resources are combined into separate zones.
- **Define access rights**—Defining access rights properly and clearly allows the organization to ensure against the risk that unauthorized access could lead to revision of the network segmentation design resulting in exposure of sensitive data.
- **Implement POLP**—In network segmentation, it is critical to minimize the number users who can have access as well as what they can do with that access. This is implemented through the POLP.

©ISACA. All Rights Reserved.

5.4.15 Endpoint Security

An endpoint refers to any a device that enables an employee to connect to the organizational network. Endpoint security refers to the security measures implemented on each endpoint of the organization's network. An important aspect of effective endpoint security is auditing. IS auditors should regularly carry out audits of endpoints to ensure that the security measures implemented are working effectively. The growth of Bring Your Own Device (BYOD) and the IoT has exponentially increased the number of devices that could potentially connect to a network. Common devices that can be considered endpoints include:

- Automated teller machines
- IoT-enabled smart devices
- Industrial machines
- Laptop computers
- Medical devices
- Mobile phones
- Printers
- Servers
- Tablets
- Smartwatches

IS auditors should understand that endpoints are key entry points to business networks and systems for hackers. Therefore, organizations should ensure that every device that is or could be connected to their network is protected. As endpoints evolve and increase in sophistication, so too should the security solutions that protect them from exploitation. Some of the benefits of implementing endpoint security are:

- **Keeps connected devices secure**—Endpoint security helps organizations keep the devices that connect to a network secure. Organizations that make endpoints their network perimeter can reduce risk and detect suspicious activity no matter where employees are located.
- **Promotes data security**—Data is the most valuable asset of an organization. To lose data or to lose access to it can put the entire business at risk of insolvency.
- **Facilitates secure remote working**—Remote work and BYOD policies make perimeter security increasingly insufficient and create vulnerabilities.

Endpoint Detection and Response

Endpoint detection and response (EDR) refers to the application of various tools and technologies to continuously monitor the organization's endpoints for the purposes of detecting suspicious behavior and triggering automatic responses. EDR performs data collection, which is critical for threat analysis and the prevention of attacks. The IS auditor should be familiar with the EDR components shown in **figure 5.24**.

Figure 5.24—Components of Endpoint Detection and Response (EDR)

Component	Component Description
Endpoint data collection agents	These are software agents that monitor and collect data about the status of endpoints. The collected data is transmitted to a central database for storage pending further actions. Typical data collected includes processes running on endpoints, the volume of activity at each endpoint and the status of endpoint connections.
Automated response	The automated response component has preconfigured rules that can recognize data representing a known security attack or breach. Once detected, an automated response is triggered. The responses include alerting the responsible personnel and logging off the user.
Analysis and forensics	This component consists of real-time analytics for the speedy resolution of incidents that cannot be resolved through automated responses. It uses sophisticated algorithms for the correlation and analysis of large data volumes searching for specific patterns. The EDR analysis and forensics component incorporates forensic tools that help in investigating past attacks and breaches and perform actions such as threat intelligence and threat hunting. Forensics also includes post-mortem analysis of an attack.

Some of the major advantages of implementing endpoint security solutions are:

- **Improved monitoring**—The main advantage of endpoint security is that it protects the data on the device itself, enabling the organization to centrally monitor the activities and status of its employees' devices at all times. This assists in containing security incidents at their source before they spread to other systems.
- **Improved database security**—EDR works by examining files as they enter the network. It can use the cloud to store the latest threat information databases, freeing endpoints from the bloat associated

 ©ISACA. All Rights Reserved.

with storing and maintaining information databases locally.
- **Provides fast access to security data**—With endpoint security in place, the organization can access actionable data relevant to security and quickly and accurately respond to security incidents. An EDR can isolate the affected endpoint and allow the organization to swiftly act on the attack. Using the data obtained, security teams can also effectively track attacks and uncover security incidents.
- **Centralized visibility**—The EDR provides information security administrators with a centralized management console, which enhances real-time security visibility in the organization. Adversary activities can be contained as early as the period they begin initiating the attacks.
- **Application control**—EDRs secure endpoints through application control, which blocks the use of applications that are unsafe or unauthorized, and through encryption, which helps prevent data loss.
- **Malware detection**—The organization can devise malware-containment strategies and remediate damage when EDR technology is established.

EDR can be implemented through an on-location, cloud or hybrid approach as specified below:
- **On-location**—An on-location, or on-premises, approach involves a locally hosted data center that acts as a hub for the management console, providing endpoint security via an agent. This approach is seen as a legacy model and has drawbacks. For example, it can create security silos since administrators can only manage endpoints within their perimeter.
- **Cloud**—This approach enables administrators to monitor and manage endpoints through a centralized management console in the cloud, which devices connect to remotely. Cloud solutions use the advantages of the cloud to ensure security behind the traditional perimeter, removing silos and enhancing administrator reach.
- **Hybrid**—A hybrid approach mixes both on-location and cloud solutions. This approach has become more prevalent with the increase in remote working. Many organizations have adapted elements of legacy infrastructures to leverage on cloud capabilities.

Some of the desired features of highly effective EDR solutions are:
- Advanced antimalware and antivirus protection to prevent, detect and contain malware and viruses
- ML capabilities to detect zero-day threats in real time
- Proactive web security to ensure safe browsing on the web
- DLP to prevent data loss and exfiltration
- Firewalls to block undesirable network traffic
- Email gateways to block social engineering attack attempts
- Computer forensics capabilities to enable security administrators to quickly isolate infections
- Centralized management console to improve visibility and simplify operations

Extended Detection and Response

Extended detection and response (XDR) security takes a broader view of information security than EDR by integrating security across endpoints, cloud computing, email and other solutions. XDR provides extended visibility, analysis and response across endpoints, workloads, users and networks. It uses the latest technologies to provide higher visibility and collect and correlate threat information, while employing analytics and automation to assist in detecting current and future attacks. There are three parts to XDR:
- **Data analysis**—XDR monitors and collects data across multiple security layers, including endpoints. It leverages data analysis to correlate context from several alerts and integrate them into a few high-priority alerts. This helps avoid overwhelming security teams with huge amounts of data and allows them to concentrate on the most significant alerts.
- **Detection**—XDR's superior visibility allows it to search through all the alerts and report on those that require immediate responses. Its visibility allows the XDR to create baselines of normal behavior within an environment; to detect security threats that leverage software, ports and protocols; and to investigate the origins of the threats. All these activities help in preventing threats from affecting other parts of the system.
- **Response**—XDR can contain and eliminate threats that have been detected, and update security policies to prevent similar threats in the future. The major difference between EDR and XDR in terms of response is that EDR performs response activities on endpoints and workloads, but XDR goes further. XDR addresses everything from protecting endpoints to responding to threats across all security control points, such as servers and networks.

XDR benefits include:
- **Provides granular visibility**—Unlike EDR, XDR provides full visibility into the security environment. It allows security analysts to view hidden threats, and it provides information regarding how an attack was

©ISACA. All Rights Reserved.

carried out, including its entry point and its victims, origins and spread.

- **Encourages prioritization of security threats**—IT and security teams often struggle to keep up with thousands of alerts generated by their security services. XDR's data analysis and correlation capabilities allow it to group related alerts across the MITRE ATT&CK[39] framework, prioritize them and surface only the most important ones.
- **Improves speed in detection and response**—XDR's use of automation speeds up detection and response by eliminating the manual steps from the security processes. This allows IT security teams to handle a large volume of security data and carry out complex processes several times. Automated analysis also enables security teams to address threats more effectively.
- **Improves operational efficiency**—Instead of offering a fragmented collection of security tools, XDR enables a holistic view of threats affecting the entire security posture of an organization. It provides a centralized data collection and response solution that is closely integrated into the environment and broader security ecosystem. It can detect threat actors employing authorized software to infiltrate the system.
- **Provides more sophisticated responses**—XDR's more sophisticated capabilities allow it to tailor the response to the specific system. It can also leverage other control points to minimize the overall impact and can incorporate lateral movement, anomalous connections, beacons and data exfiltration.
- **Improves prevention capabilities**—Solutions that protect against various attacks can be developed when threat intelligence and adaptive ML technologies are included in XDR. Continuous monitoring paired with automated response capabilities assist in instantly blocking threats upon detection.
- **Improves control processes**—XDR technologies can both allow and deny traffic and processes, ensuring that only authorized actions and users can access the organization's systems. The centralization feature reduces the number of alerts and increases their accuracy, leading to fewer false positives. Another advantage of XDR is that it is a unified platform and not an aggregation of endpoint solutions. This makes the XDR easy to maintain and manage by reducing the number of interfaces to be navigated during a response.

5.5 Data Loss Prevention

DLP is a set of tools and processes that are implemented to prevent the loss or misuse of sensitive data or access by unauthorized users, especially those outside the organization. It is sometimes referred to as data leakage prevention. DLP software classifies regulated, confidential and business-critical data and identifies violations defined by organizations' DLP policies. Once those violations are identified, DLP enforces remediation with alerts for protective actions to prevent end users from accidentally or maliciously sharing data that could create organizational risk. DLP is very critical in the day-to-day operation of an organization because when data is lost, several negative consequences may result, including:

- Reduced productivity as employees who should be working with the data become idle
- Increased costs to replace or regain control of the data
- Exposure to various legal actions resulting from loss of sensitive data
- Loss of business due to customers losing trust in the organization, contributing to lower revenue and profitability levels
- Risk of business closure if organizations fail to raise funds for data recovery

5.5.1 Types of DLPs

Figure 5.25 shows the common types of DLP systems.

[39] MITRE ATT&CK, *https://attack.mitre.org/*

 ©ISACA. All Rights Reserved.

Figure 5.25—Types of Data Loss Prevention (DLP) Software

Type of DLP	Description
Network-based DLP	A network-based DLP scans all outgoing data looking for specific data. If a user sends out a file containing restricted data and/or to an unauthorized destination, the DLP system detects and prevents it from leaving the organization in real time. It then sends an alert, such as an email, to the security administrator. Depending on the rule set, it may also quarantine or encrypt the data. It uses DPI technology to extend beyond reading the header information of a packet to reading the contents of the packet's payload.
Endpoint-based DLP	An endpoint-based DLP can scan files stored on a system as well as files sent to external devices, such as printers. For example, an organization endpoint-based DLP can prevent users from copying sensitive data to flash drives or sending sensitive data to a printer. Security administrators normally configure the DLP to scan the files composed of appropriate keywords. When it detects files with such keywords, it blocks the copy or print job. Endpoint-based DLP solutions typically accomplish this by using a software program known as an agent, which is centrally managed.
Cloud DLP	Due to increases in remote working, IS security administrators leverage the cloud service to provide DLP solutions. A cloud DLP solution ensures the data stored in the cloud is monitored and protected. It uses a library of predefined data types to identify sensitive data and blocks potential exposures to cloud data infrastructure or prevents data loss from happening. For instance, a cloud-based DLP can remove a sensitive attachment from an email.

5.5.2 Data Loss Risk

Risk of data loss is pervasive in most IS environments and can cause serious consequences to organizations.[40] When data leaks, the potential consequences include its corruption or destruction, exposure of confidential information and theft of IP. **Figure 5.26** shows some of the causes of data leakage in an organization.

Figure 5.26—Data Leakage Risk

Area of Risk	Causes of Data Loss
Technology	• Loss or theft of devices • Unencrypted data storage • Inheriting data from another system • Software vulnerabilities • Exploitation of vulnerabilities in a database development environment • Exploitation of unnecessary technology installed on the computer • Processing production data in the development environment • Failure to install patches and updates • Unsecure remote access tools • Faults in vendor products (software and/or hardware) • Insecure communication platforms • Inappropriate access rights to applications with sensitive data • Insecure transmission links between the organization and a third party • Poor system programming and/or design

[40] Wlosinski, L.; "Data Loss Prevention–Next Steps," *ISACA Journal*, vol. 1, 16 February 2018, *https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/data-loss-preventionnext-steps*

©ISACA. All Rights Reserved.

Figure 5.26—Data Leakage Risk (cont.)

Area of Risk	Causes of Data Loss
Process	• Poor data governance oversight • Absence of data retention policy • Non-performance of risk assessments • Keeping or transmitting unencrypted data • Not assessing data sensitivity • Not enforcing principle of least privilege (POLP) and need to know • Poor incident response practices • Software setting misconfigurations • Poor data monitoring systems • Failure to close expired accounts
People	• Negligence • Unintentional data transmission • Lack of training and awareness; inadequate awareness • Poor accountability systems • Accidental deletion of files • Leaving sensitive data exposed • Emailing sensitive data without encryption • Sharing work devices • Poor employee supervisory systems • Data theft (selling corporate information) • Exposure of data due to blackmail via social engineering • Printing and copying sensitive data • Insider threats with malicious intent (hacking, fraud, sabotage) mainly due to discontent • Breach of trust among systems developers • Misuse or sharing of passwords • Copying data to remote systems (to support work effort)
Threat actors	• Malware propagation • Software corruption • Sabotage (mainly by malicious insiders)
Natural disasters	• Data loss due to fires, earthquakes and tornados • Liquid spillages • Power outages • High temperatures (overheating) and low humidity levels (overcooling/freezing)

Some of the use cases for DLP include:

- **Compliance**—A DLP can identify, classify and tag sensitive data in an organization. It can also monitor activities and events surrounding data and the necessary information typically required for compliance purposes.
- **Intellectual protection**—DLP solutions can classify intellectual property in both structured and unstructured forms thus offering protection against unwanted exfiltration of data.
- **Data visibility**—A DLP can track data on endpoints, networks and the cloud. This tracking provides greater visibility into how users interact with organizational data.
- **Pervasiveness**—DLP solutions can span multiple environments, including cloud environments and complicated supply chain networks, providing visibility and preventing sensitive data breaches.
- **Frequent data breaches**—Adversaries from nation states, cybercriminals and malicious insiders often target sensitive data. DLP solutions can protect against all kinds of adversaries, malicious or not.
- **Value of stolen data**—Stolen data is often sold on the dark web, where individuals and groups can purchase it for future use. There is an important financial

 ©ISACA. All Rights Reserved.

incentive for data theft, particularly of financial information like credit card or banking information.

5.5.3 DLP Solutions and Data States

There are three primary states of information:
1. Data at rest
2. Data in motion
3. Data in use

Each of these three states of data is addressed by a specific set of technologies provided by DLP solutions.

Data at Rest

A basic function of DLP solutions is the ability to identify and log where specific types of information (e.g., credit card or social security numbers) are stored throughout the enterprise. To accomplish this, most DLP systems use crawlers, which are applications that are deployed remotely to log onto each end system and "crawl" through data stores, searching for and logging the location of specific information sets based on a set of rules entered into the DLP management console.

Data in Transit

To monitor data movement on enterprise networks, DLP solutions use specific network appliances or embedded technology to selectively capture and analyze network traffic. When files are sent across a network they are typically broken into packets. To inspect the information being sent across the network, the DLP solution must be able to passively monitor the network traffic, recognize the correct data streams to capture, assemble the collected packets, reconstruct the files carried in the data stream and perform the same analysis that is done on the data at rest to determine whether any portion of the file content is restricted by its rule set. At the core of this ability is the DPI process. If sensitive data are detected flowing to an unauthorized destination, the DLP solution has the capability to alert and optionally block the data flows in real or near real time, again based on the rule set defined within its central management component. Based on the rule set, the solution may also quarantine or encrypt the data in question.

Data in Use

Data in use primarily refers to monitoring data movement stemming from actions taken by end users at their workstations, whether that entails copying data to a flash drive, sending information to a printer or even cutting and pasting between applications. DLP solutions typically accomplish this through the use of a software program known as an agent, which is ideally controlled by the same central management capabilities of the overall DLP solution.

5.5.4 DLP Controls

IS auditors should undertake regular audits to provide assurance to management of the efficiency and effectiveness of controls put in place to reduce data loss in the organizations. They should also advise on the improvement of controls and the amount of data leakage. **Figure 5.27** provides brief explanations on the DLP controls that can be implemented in an organization.

Figure 5.27—Data Loss Prevention (DLP) Controls

Area	Control
Governance	• Craft DLP policy, procedures and guidelines. • Classify data and assign sensitivity levels. • Perform data loss risk assessment regularly. • Regularly update data risk profiles to identify new threats. • Standardize the endpoints to make deployment more manageable. • Document all data loss incidents. • Periodically audit the organization for compliance with data protection requirements.
People	• Do not leave sensitive data exposed and unattended. • Prohibit copying sensitive data onto removable media. • Provide read-only access to sensitive information. • Incorporate data protection clauses in employment contracts. • Require data owner authorization prior to data exportation. • Train and develop employees in data protection.

©ISACA. All Rights Reserved.

Figure 5.27—Data Loss Prevention (DLP) Controls (cont.)

Area	Control
DLP Solution Deployment	• Deploy DLP using a risk-based approach. • Fine-tune DLP policies to the organization's requirements. • Test the DLP implementation. • Encrypt data in transit and at rest.
IT Controls	• Closely monitor all sensitive data channels. • Prohibit unauthorized devices in the network. • Block files containing personal identity information. • Ensure all removable storage devices are configured for read-only. • Implement multilayered authorization and access controls. • Encrypt the data backup containing sensitive information. • Implement firewall and antivirus technologies.
Procurement	• Evaluate the DLP solution to check compatibility with the organization's data formats. • Choose a product that provides real-time reports regarding DLP policy violations.

5.5.5 DLP Content Analysis Methods

A DLP solution works by performing content analysis of the data loss. The methods operate by triggering policy violations. Some of the major content analysis methods, among a host of other methods available, are:

- **Regular expression matching**—Using this method, DLP solutions match specific set data conditions, such as detecting 16-digit credit card numbers in an email and determining whether the communication channel contains sensitive data. This method serves well as the first filter for sensitive data. The major disadvantage is that without checksum validation the method is prone to high false-positive levels.
- **Structured fingerprinting**—Fingerprinting is performed by algorithms that map data to shorter text strings known as fingerprints, which are unique identifiers for their corresponding data and files. Fingerprinting is used for structured data such as databases and directory services. When applied to forms, DLP solutions can detect sensitive data such as social security numbers and credit card numbers, thus enabling DLP solutions to secure those documents during transmission. Database fingerprinting is also known as exact data matching (EDM).
- **Exact file matching (EFM)**—The IS auditor should be aware that file contents are not analyzed but file hashes are matched against the exact fingerprints. The objective is to determine if file content has changed. The advantage of this method is that it has low false positives. The challenge is that the approach is not effective for files with different versions.
- **Indexed document matching (IDM)**—IDM applies fingerprinting methods to detect sensitive information stored in unstructured data. Unstructured data includes Microsoft Office documents, PDFs, binary files such as JPEGs, and multimedia files. IDM is also capable of detecting "derived" content, such as text that has been copied from the source document to another file.
- **Lexicon matching**—This method is also known as conceptual analysis. It analyzes unstructured data using dictionary terms and other rule-based matches to detect sensitive information. Lexicon matching provides alerts if it detects unstructured ideas that defy the categorization in place. However, this method requires customization to the type of DLP solution in place.
- **Statistical analysis**—This method uses ML and other advanced methods, such as Bayesian analysis, to detect more obscure sensitive information that cannot otherwise be detected. Statistical analysis works by triggering policy violations in secure data and typically requires huge volumes of data for effective analysis. The downside of statistical analysis is that it can yield both false positives and negatives.
- **Categorization**—By categorizing data, the DLP solution can determine if data is highly sensitive and violates compliance regulations. The categorization method involves setting prebuilt categories with rules for highly sensitive data, such as credit card information.

5.5.6 DLP Deployment Best Practices

DLP deployments need the right strategy to avoid costly mistakes and downtime arising out of improper deployment methods. By assessing the organization's

 ©ISACA. All Rights Reserved.

DLP practices against best practices, IS auditors can provide assurance and advise on the organization's DLP deployment. Some of the best practices in DLP deployment include:

- **DLP policy creation**—The organization should develop a DLP policy that addresses the prevention of data loss and dictates the actions taken by the various DLP components. DLP solutions with preconfigured policies that map to common regulations should be customized to meet the organization's requirements.
- **Definition of business and security requirements**—Before deploying a DLP solution, an organization should define the business and security requirements behind the deployment strategy. Compliance and other cybersecurity standards should influence the way the DLP solutions are deployed.
- **Employee involvement**—Every employee is responsible for upholding data security standards. Of course, the IT department does most of the everyday work securing systems and processes but a stakeholder approach across the organization will simplify any security policy implementation. Every IS staff member should be involved in DLP deployments in order to understand the changes and be able to answer customer queries and remediate errors.
- **Senior management support**—The implementation of the DLP solution should have senior leadership support with departmental leaders from all departments involved in the process. This ensures that they will supervise their subordinates in the application of DLP best practices.
- **Deployment mode**—A DLP should be deployed in the appropriate mode. There are two modes of deployment: passive mode and active mode. In passive mode, also called monitoring mode, the potential data leak is not blocked and the DLP monitors and analyzes traffic. In active mode, the DLP blocks any data leakage traffic and informs the DLP administrator of the leakage.
- **Incorporation of encryption technologies**—Strong encryption, which is a critical component of security, should be incorporated into DLP solutions.
- **Insider threats**—The IS auditor should be aware that most threats to an organization's security posture are launched internally.
- **Data classification**—Not all data is equally critical, and each organization has its own definition of critical data. The DLP solution should start with the most valuable or sensitive data that is likely to be targeted by attackers and cascade to less sensitive data.
- **Risk assessment**—Different risk is associated with data distributed to user devices or shared with third parties. Data is often at highest risk at the moment it is in use on endpoints; therefore, a robust DLP program must account for the mobility of data.
- **Control documentation**—At the initial stages of DLP implementation, data use controls are typically simple. As the DLP program matures, organizations can develop more complex controls. It is important to document changes to the environment and any procedures to be followed to avoid mistakes by employees who may not be aware of how the DLP solution works to monitor data.
- **Training and development**—User training can reduce the risk of accidental data loss due to insiders. Training and development enable employees to fully implement DLP best practices.
- **Workflow management**—Most full DLP solutions provide the capacity to configure incident handling, allowing the central management system to route specific incidents to the appropriate parties for resolution. Integration with directory services allows the DLP console to map a network address while backup and restore features allow for the preservation of DLP policies and other configuration settings. A reporting function may be implemented to leverage external reporting tools.
- **Audit infrastructure**—The whole DPL solution and its associated infrastructure should be subject to regular audits. Audits are critical in establishing whether the operations of a DLP are efficient and effective.

5.5.7 DLP Risk, Limitations and Considerations

DLP risk factors and limitations the IS auditor should consider in an audit include:

- **Improperly tuned network DLP modules**—Proper tuning and testing of the DLP system should occur before enabling content blocking. Enabling the system in monitor-only mode allows for tuning and provides the opportunity to alert users to out-of-compliance processes and activities so they may adjust accordingly. Involving the appropriate business and IT stakeholders in the planning and monitoring stages helps to ensure that disruptions to processes will be anticipated and mitigated. Finally, it is important to establish some means of accessibility in the event there is critical content being blocked during off-hours when the team managing the DLP solution is not available.
- **Excessive reporting and false positives**—Similar to an improperly configured IDS, a DLP solution may register significant amounts of false positives,

©ISACA. All Rights Reserved.

which can overwhelm staff and obscure valid hits. Avoid excessive use of template patterns or black box solutions that allow for little customization. The greatest feature of a DLP solution is the ability to customize rules or templates to specific organizational data patterns. It is important that the system be rolled out in phases, focusing on the highest risk areas first. Trying to monitor too many data patterns or enabling too many detection points too soon can quickly overwhelm resources.

- **Encryption**—See section 5.6 Data Encryption for more information.
- **Graphics**—DLP solutions cannot intelligently interpret graphics files. Unless all such information is blocked or manually inspected, a significant gap will exist in an enterprise's control of its information. Sensitive information scanned into a graphics file or intellectual property that exists in a graphics format, such as design documents, fall into this category. Enterprises that have significant intellectual property in a graphics format should develop strong policies that govern the use and dissemination of this information. Although DLP solutions cannot intelligently read the contents of a graphics file, they can identify specific file types, their source and destination. This capability, combined with well-defined traffic analysis, can flag uncharacteristic movement of this type of information and provide some level of control.

5.6 Data Encryption

Encryption is the process of converting a plaintext message into a secure-coded form of text, called ciphertext, which cannot be understood without converting it back via decryption (the reverse process) to plaintext. Encryption is done via a mathematical function and use of a special encryption/decryption password called the key.

Encryption generally is used to:

- Protect data in transit over networks from unauthorized interception and manipulation
- Protect information stored on computers from unauthorized viewing and manipulation
- Deter and detect accidental or intentional alterations of data
- Verify authenticity of a transaction or document

In many countries, encryption is subject to laws and governmental regulations.

Encryption is limited in that it cannot prevent the loss or modification of data. The protection of the keys is of paramount concern when using encryption systems. Therefore, even if encryption is regarded as an essential form of access control that should be incorporated into an organization's overall security landscape, it requires a thorough understanding of how schemes work. Misuse or misconfiguration may significantly undermine the protection an organization believes is in place.

5.6.1 Elements of Encryption Systems

Key elements of encryption systems include:

- **Encryption algorithm**—A mathematically based function that encrypts/decrypts data
- **Encryption key**—A piece of information that is used by the encryption algorithm to make the encryption or decryption process unique. Like a password, a user needs to provide the correct key to access or decrypt a message. The wrong key will decipher the message into an unreadable form.
- **Key length**—A predetermined length for the key. The longer the key, the more difficult it is to compromise in a brute force attack.

Encryption schemes are susceptible to brute force attacks in which an attacker repeatedly tries to decrypt a piece of ciphertext using numerous possible encryption keys until the correct one is found (i.e., brute forcing stops when the ciphertext does not decrypt to a non-sense message). Because the amount of time required to search for the correct key depends exponentially on its length, the key should be chosen adequately to ensure the overall security of the encryption scheme.

Attacks can be mounted against the robustness of the underlying mathematical algorithms to speed up the brute forcing process. Cryptanalysis is the science of finding such weaknesses. For example, an algorithm prone to a known plaintext attack allows an attacker to discard a large portion of the possible decryption keys if samples of ciphertexts and corresponding plaintexts are available. In a variation of this attack, the attacker guesses parts of the plaintext by leveraging statistical properties of the encrypted data (e.g., spotting vowels or finding the word "the" in an English text).

The randomness of key generation is a significant factor in the ability to compromise an encryption scheme. Common words or phrases significantly lessen the key space combinations required to search for the key, diminishing the strength of the encryption algorithm. Therefore, the capabilities of a 128-bit encryption algorithm are diminished when encrypting keys are based on passwords that lack randomness. It is important that

effective password syntax rules are applied and that easily guessed passwords are prohibited.

There are two types of encryption schemes: symmetric and asymmetric. Symmetric key systems use a unique key (usually referred to as a secret key) for both encryption and decryption. The key is known as bidirectional because it encrypts and decrypts and it must be shared out of band (i.e., via a secure, alternative method to the encrypted message).

In asymmetric key systems the decryption key is different from the one used for encryption. The keys are unidirectional—they encrypt or decrypt—but are complementary. The two parties (the sender and the recipient) are not expected to trust each other to keep the secret key. The encryption key is publicly disclosed while the decryption key is kept private (asymmetric systems are also known as public-key schemes).

Hash functions are another important component of cryptographic protection schemes. These functions transform a text of arbitrary length into one of fixed width called the digest or the hash. A hash function must be one-way (i.e., making it hard to find a piece of text that generates a given hash). Such functions can augment encryption schemes with integrity and authenticity properties. Hashing algorithms are an accurate integrity check tool. The hash detects changes of even a single bit in a message. A hash algorithm will calculate a hash value from the entire input message. The output digest itself is a fixed length, so even though the input message can be of variable length, the output is always the same length. The length depends on the hash algorithm used. For example, MD5 generates a digest length of 128 bits; SHA-1, a digest of 160 bits; and SHA-512, a digest of 512 bits.

Until recently, the most common message digest algorithms were MD5 and SHA-1. Due to security considerations, the industry is transitioning to SHA-2. SHA-2 has six hash functions available with varying message digest lengths. SHA-3 has also been announced by the National Institute for Standards and Technology (NIST) in the event a successful attack is developed against SHA-2.

A comparison of encryption and hashing is shown in **figure 5.28**.

Figure 5.28—Comparison of Encryption and Hashing

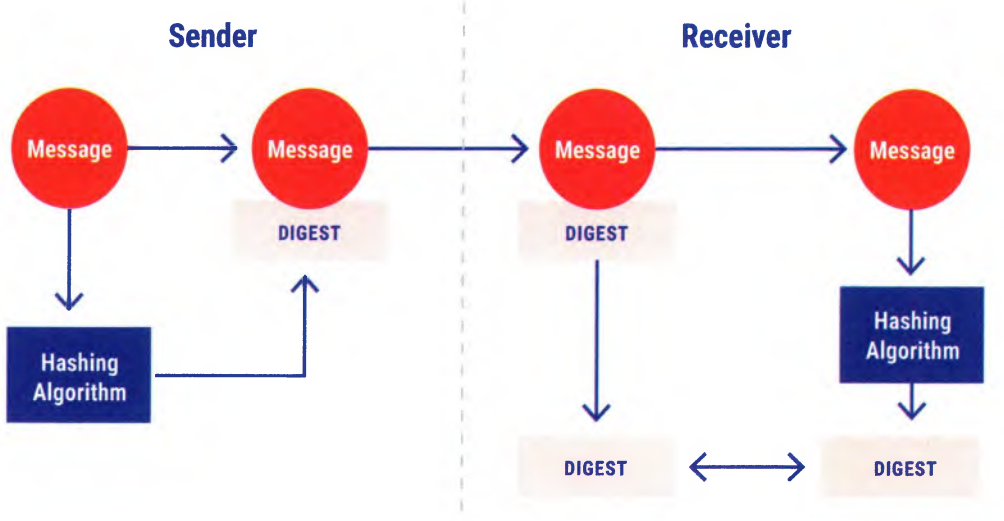
Category	Encryption	Hashing
Characteristics	Two-way function in which information is scrambled in such a way that it can be unscrambled later	One-way function that maps data to a fixed-length value to produce a message digest
Objective	Data security during transmission and at rest	Data verification and authentication
Reversibility	Reversible	Irreversible
Length variability	Variable	Fixed
Key use	Uses asymmetric and symmetric keys	No keys used; a salt can be added[41]
Data transformation	Data are transformed into new data called ciphertext	No data transformation; data remains intact
Common algorithms	Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4), Data Encryption Standard (DES), Rivest–Shamir–Adleman (RSA)	Secure Hash Algorithm 1 (SHA-1), Secure Hash Algorithm 2 (SHA-2), message-digest algorithm (MD5)

When senders want to send a message and ensure that it has not been altered, they can compute the digest of the message and send it along with the message to the receiver. After receiving the message and its digest, the receiver independently computes the digest of the received message and ensures that the digest computed is the same as the digest sent with the message (**figure 5.29**).

[41] A salt is an additional input to a hash function that is attached at the end of the password. The purpose of salting is to defend against dictionary attacks and password attacks using a rainbow table.

©ISACA. All Rights Reserved.

Figure 5.29—Verifying Message Integrity Using a Hash Function



Source: ISACA, *CRISC Review Manual 7th Editon Revised*, USA, 2023

Note

The IS auditor should be familiar with how a digital signature functions to protect data. The specific types of message digest algorithms are not tested on the CISA exam.

5.6.2 Link Encryption and End-to-End Encryption

Link encryption and end-to-end encryption (E2EE) are the main mechanisms for encrypting data:

- **Link encryption**—Link encryption, also known as online encryption, encrypts and decrypts all traffic along a specific communication channel. This includes encrypting user information as well as headers, trailers, addresses and routing data. Only the data link control messaging information, which includes instructions and parameters used for synchronization purposes, is not encrypted. It protects against packet sniffing and eavesdropping. Packets are decrypted at each hop, so the router or other intermediate device is aware of the destination of the packet. After decryption, the router reads the routing and address information within the header, re-encrypts it and forwards it to the next hop. Link encryption works at the data link and physical layers. The main advantage of link encryption is that it is simple, as users have no role in its initiation. The major disadvantage of link encryption is the complexity of key distribution, as each hop has to receive a key. Therefore, as the keys change, each hop device must be updated. Also, because packets are decrypted at each hop, many vulnerabilities are created.
- **E2EE**—E2EE is a form of encryption in which the message stays encrypted from its origin to its destination. It ensures that only the two communicating parties can read the messages at both ends. In E2EE, an intermediary cannot decrypt the messages. This is viewed as more secure than link encryption. Unlike link encryption, E2EE does not require constant encryption and decryption processes at each hop, as the headers and trailers are not encrypted. Communicating devices simply read the necessary routing information and forward the packets. E2EE provides more flexibility for the user to decide on the types of messages to encrypt. The major disadvantage is that headers, addresses and routing information are not encrypted, leaving them vulnerable to attacks. An example of the application of E2EE is WhatsApp messaging.

 ©ISACA. All Rights Reserved.

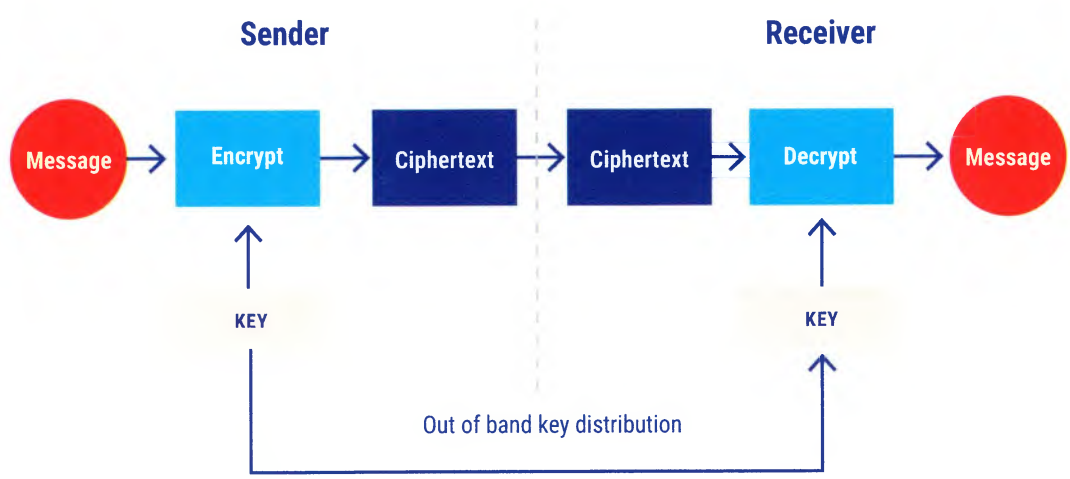
5.6.3 Symmetric Key Cryptographic Systems

Symmetric key cryptographic systems (**figure 5.30**) are based on a symmetric encryption algorithm, which uses a secret key to encrypt the plaintext to the ciphertext and the same key to decrypt the ciphertext to the corresponding plaintext. In this case, the key is said to be symmetric because the encryption key is the same as the decryption key.

Many common symmetric key cryptographic systems are based on the Data Encryption Standard (DES), which has been withdrawn. Extensions of DES (Triple DES or 3DES) were proposed to extend the DES standard while retaining backward compatibility. In 2001, DES was replaced with the Advanced Encryption Standard (AES), a public algorithm that supports keys from 128 bits to 256 bits in size. Another commonly used symmetric key algorithm is Rivest Cipher 4 (RC4), a stream-cipher often used in SSL/TLS protocol sessions.

There are two main advantages symmetric key systems have over asymmetric ones. The first is that keys are much shorter and can be easily remembered. The second is that symmetric key cryptosystems are generally less complicated and use less processing power than asymmetric schemes. This makes symmetric key cryptosystems ideally suited for bulk data encryption. The major disadvantage of this approach is key distribution, particularly in e-commerce environments where customers are unknown, untrusted entities. Also, a symmetric key cannot be used to sign electronic documents or messages due to the fact that the mechanism is based on a shared secret by at least two parties.

Figure 5.30—Symmetric Cryptography



Source: ISACA, *CRISC Review Manual 7th Editon Revised*, USA, 2023

5.6.4 Public (Asymmetric) Key Cryptographic Systems

In public key cryptography (**figure 5.31**), two keys work together as a pair; they are inversely related to each other, based on mathematical integer factorization. One of the keys is kept private while the other one is publicly disclosed. Encryption works by feeding the public key to the underlying algorithm while the resulting ciphertext can be decoded using the private key. This scheme avoids the requirement of the owner of the key pair to share a secret piece of information (the private key) with the other party of the communication. It is important to note that one key pair can be used in one direction only (from the sender to the receiver). To implement bidirectional communication between two parties, two key pairs are required (one for each direction).

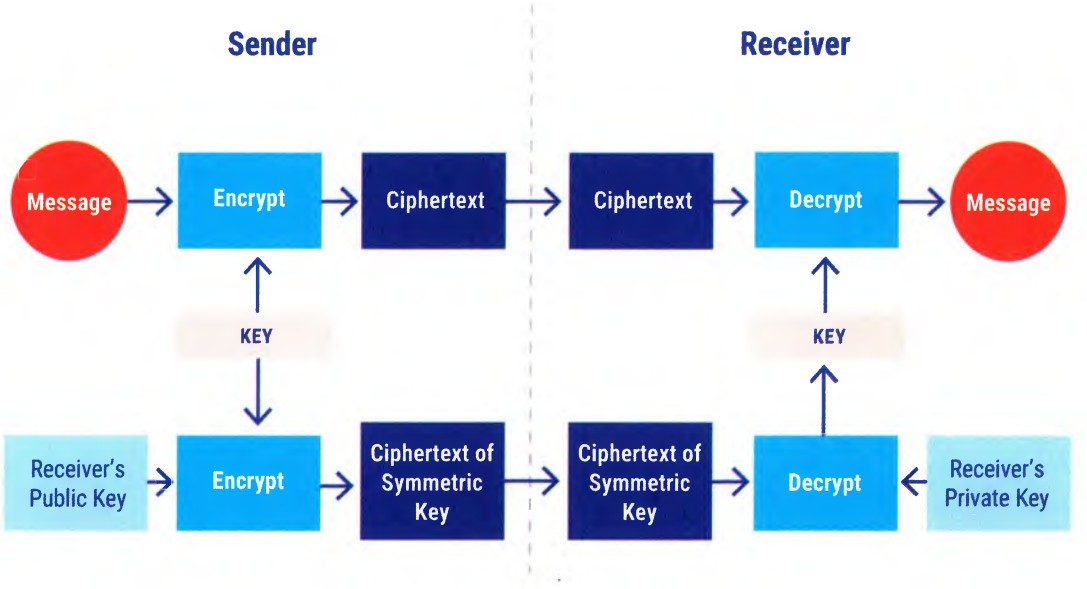
Public key systems were developed primarily to solve the problem of key distribution. Only 2*N key-pairs are employed in a scenario in which communication happens between N parties. In the same scenario, a symmetric scheme would require roughly N^2 keys to be

©ISACA. All Rights Reserved.

transmitted: one key for each pair of the involved parties. In addition, the exchanged keys are public; thus, there is no confidentiality requirement to be fulfilled by the key distribution protocol.

The first practical implementation of a public key system was developed by Ron Rivest, Adi Shamir and Leonard Adleman (the RSA algorithm), which is a widespread asymmetric encryption scheme. The main drawback of this algorithm lies in the length of the keys (varying between 1024 and 4096 bits) and the complexity of the calculations involved for encoding and decoding. To address these issues, other encryption algorithms were developed.

Figure 5.31—Using Asymmetric Algorithms to Support Symmetric Cryptography



Source: ISACA, *CRISC Review Manual 7th Editon Revised*, USA, 2023

5.6.5 Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is a public-key cryptosystem based on the algebraic architecture of the elliptic curves over finite fields. It implements all major capabilities of the asymmetric cryptosystems such as encryption, signatures and key exchange. It is generally considered a natural modern successor of the RSA cryptosystem, because it uses smaller keys and signatures than RSA for the same level of security and provides very fast key generation, fast key agreement and fast signatures. However, while RSA's security is dependent on huge prime numbers, ECC leverages the mathematical theory of elliptic curves to achieve the same level of security with considerably smaller keys. Figure **5.32** provides a comparison of ECC and RSA.

Figure 5.32—Comparison of Elliptic Curve Cryptography (ECC) and RSA

Parameters	ECC	RSA
Working algorithm	Works on a mathematical model of elliptic curves	Based on the prime factorization approach
Bandwidth savings	More bandwidth savings	Less bandwidth savings
Encryption process	Shorter	Longer
Decryption process	Slower	Faster

 ©ISACA. All Rights Reserved.

Figure 5.32—Comparison of Elliptic Curve Cryptography (ECC) and RSA (cont.)

Parameters	ECC	RSA
Security	Considered safer as it continues to adapt	Reaching its maximum lifespan

5.6.6 Quantum Cryptography

Quantum cryptography refers to a cryptographical method that relies on quantum mechanics to secure data. It uses individual light particles known as photons to transmit data over fiber optic cables with the photons representing the binary bit in the implementation of cryptography. Quantum cryptography relies on quantum secure properties, which include the inability to copy whole particle, particles existing in more than one place or state, and the inability to observe a quantum particle without changing it. This means that when data is in a quantum state, it becomes impossible for malicious attackers to tamper with it without being detected by the communicating parties. Quantum key distribution (QKD) schemes allow the secure distribution of a shared encryption key between two parties. The two parties can detect eavesdropping that may happen across the channel. Benefits of quantum cryptography include:

- **Provides secure communication**—Quantum cryptography relies on the laws of physics, making it more secure than other forms of cryptography. When a threat actor attempts to read data encrypted with quantum cryptography, the quantum state immediately changes leading to detection.
- **Protects against eavesdropping**—Quantum cryptography bases security on the quantum state changes that happen when unauthorized users attempt to access information. Such attempts lead to changes in the communication result expected by the end user, leading to their detection.
- **Provides a variety of security methods**—Quantum cryptography provides several protocols that further enhance security. Such protocols can be combined with the usual encryption technologies to increase overall organizational security.
- **Simplicity**—While quantum cryptography may involve huge outlays of funds during initial implementation, the technology is generally simple to operate with less resources required for its ongoing maintenance.

Some of the limitations of quantum cryptography are:

- **Polarization changes**—Quantum cryptography relies on photon dynamics. Polarization may cause the photons to change while in transit, causing errors in the communication channel.
- **Limited range**—Quantum cryptography operates within a limited range, with the maximum range generally being around 500 km through guided communication media. This technology cannot be used for long distance secure communications because of this limitation. However, the Terra Quantum can exceed the 500 km range.
- **Implementation costs**—Quantum cryptography is costly to implement. For example, it often requires its own separate technological infrastructure such as repeaters and fiber optic cables, which are generally expensive.
- **Limited destination range**—Quantum cryptography requires a dedicated channel, and it is impossible to send keys to more than one destination in a single quantum channel. The organization needs to create several quantum channels in some cases, making the process inefficient. Another important point is that multiplexing cannot be implemented in quantum cryptography as it goes against quantum principles.

5.6.7 Homomorphic Encryption

Homomorphic encryption is a form of encryption designed to allow mathematical operations to be performed on encrypted data. It creates an encryption algorithm that allows an infinite number of additions or multiplications of encrypted data. The ultimate result is strong encryption. Homomorphic encryption allows for the outsourcing of data processing activities without requiring third parties to secure the data because without the proper decryption key, it is impossible to access the original data. Benefits of this encryption include:

- **Supply chain security**—Third parties typically require access to an organization's sensitive and proprietary data to perform their jobs. Homomorphic encryption protects a company against supply chain risk as a breach of that data poses minimal risk to the company.
- **Cloud data security**—Organizations can use homomorphic encryption to secure data in the cloud while being able to calculate and search ciphered information that will later be decrypted without compromising data integrity.

©ISACA. All Rights Reserved.

- **Data security**—Homomorphic encryption allows users to add up various values in an unbiased way while keeping their values private, protecting data from manipulation and making it available for independent verification by authorized third parties. This is useful in activities such as general democratic elections.
- **Regulatory compliance**—Regulations such as the General Data Protection Regulation (GDPR) have provided data subjects with extensive rights and placed additional responsibilities and restrictions on businesses. With homomorphic encryption, an organization can store and process data on systems outside the EU and then decrypt it only on servers in locations that comply with GDPR requirements.
- **Data analytics**—Businesses often collect information about their users, process it and sell it to third parties for targeted advertising. However, this practice of monetizing personal data is controversial. With homomorphic encryption, an organization could perform data analytics without the ability to view or access the original data.
- **Privacy**—Homomorphic encryption enables organizations to share private data, especially with customers, without affecting privacy. It provides organizations with the ability to guarantee privacy by performing mathematical operations on encrypted data without exposing the data itself.

Types of Homomorphic Encryption

Homomorphic encryption types are:

- **Partially homomorphic encryption**—Partially homomorphic encryption algorithms allow an infinite amount of operations to be performed. For instance, a particular algorithm may be additively homomorphic (i.e., adding two ciphertexts together produces the same result as encrypting the sum of the two plaintexts). These algorithms are relatively easy to design and deploy. The IS auditor should note that some common encryption algorithms, such as RSA, are partially homomorphic.
- **Somewhat homomorphic encryption**—A somewhat homomorphic encryption algorithm allows a finite number of any operation rather than an infinite number of a particular operation. For instance, the algorithm can support any combination of up to six additions or multiplications; however, a seventh operation of either type would give an invalid result.
- **Fully homomorphic encryption**—A fully homomorphic encryption algorithm allows an infinite number of additions or multiplications of ciphertexts while still producing a valid result. This should be the desired end goal of homomorphic encryption.

Challenges With Homomorphic Encryption

Challenges related to homomorphic encryption include:

- **Inefficiency**—The major challenge with fully homomorphic encryption is inefficiency. Meeting the requirements of full homomorphism results in algorithms that are slow, as the requirements are quite extensive.
- **High storage requirements**—Homomorphic encryption can have very high storage requirements due to the huge processing workloads involved with its implementation.
- **Reduced performance**—The new and improved version is still much slower than plaintext operations, on average.
- **Inability to scale**—Homomorphic encryption may not fully protect personal data from providers if there are too many users. The solution to this would be for the provider to have a separate database for every user, encrypted under that user's public key. However, that is usually infeasible for a large number of users.
- **Large and complex algorithms**—Homomorphic encryption solutions typically have a large overhead ratio of computation time in the encrypted version versus computation time in the clear. Such an overhead is typically a large polynomial, which increases runtimes substantially and makes homomorphic computation of complex functions impractical.

5.6.8 Digital Signatures

An important property of public key systems is that the underlying algorithm works even if the private key is used for encryption and the public key for decryption. This may seem counterintuitive, but a public key system enables a digital signature scheme that can authenticate the origin of an encoded message. Because the private key is known only by the owner of the key-pair, it is certain that if a ciphertext is correctly decrypted using a public key, the owner of the public key cannot deny having performed the encryption process. This is called nonrepudiation.

In most practical implementations of digital signature schemes (**figure 5.33**), the public key algorithm is not applied to the whole document as it would take a lot of processing power to calculate the signed data. Instead, a digest (or "pre-hash") is first derived from the document to be signed; then the public key algorithm is applied

 ©ISACA. All Rights Reserved.

to the digest to produce an encoded piece of data (the signature) that is sent along with the document.

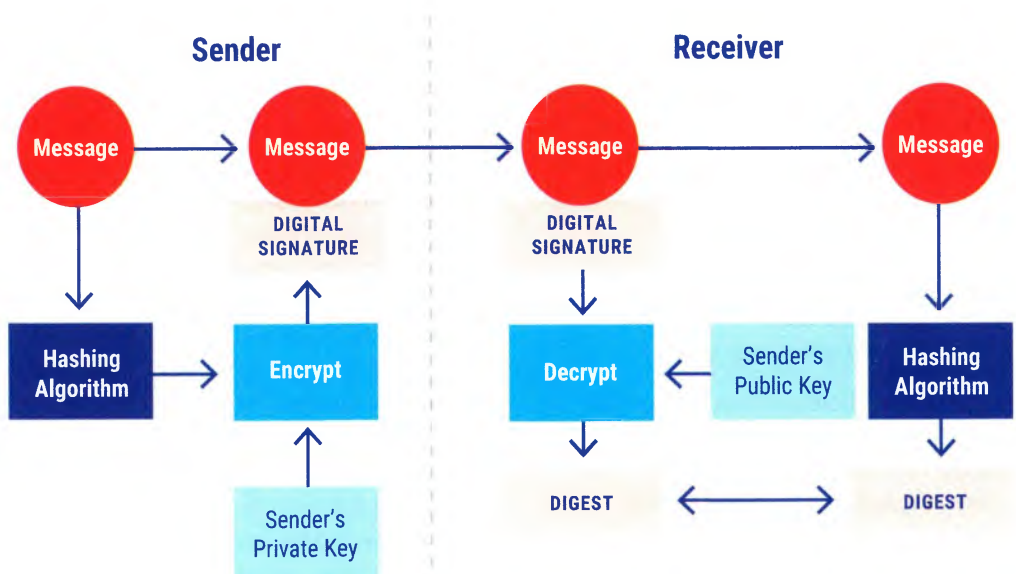
To authenticate the sender as the originator of the document, the recipient applies the same hashing function upon receiving the document and the resulting digest (or post-hash) is compared with the decrypted pre-hash. In case of a match, the receiver can conclude that the document was actually signed by the owner of the public key.

Therefore, digital signature schemes ensure:

- **Data integrity**—Any change to the plaintext message would result in the recipient failing to compute the same document hash.
- **Authentication**—The recipient can ensure that the document has been sent by the claimed sender because only the claimed sender has the private key.
- **Nonrepudiation**—The claimed sender cannot later deny generating the document.

Notice that there is no guarantee that the owner of the public key actually sent the document. A malicious attacker could intercept the signed document and resend it to the recipient. To prevent this kind of attack (known as replay attack), a signed timestamping or a counter may be attached to the document.

Figure 5.33—Verifying Message Integrity and Proof of Origin Using Digital Signatures



Source: ISACA, *CRISC Review Manual 7th Editon Revised*, USA, 2023

5.6.9 Digital Envelope

Similar to a digital signature, a digital envelope is an electronic "container" that can be used to protect data or a message through the use of encryption and data authentication. The message is first encoded using symmetric encryption. Then the code to decrypt the message is secured using public key encryption. This provides a more convenient option for encryption. A digital envelope can also be decrypted by using a receiver's private key to decrypt a secret key, or by using a secret key to decrypt encrypted data. Pretty Good Privacy (PGP), a popular data cryptography software that provides cryptographic privacy and data communication authentication, is a typical example of a digital envelope.

5.6.10 Applications of Cryptographic Systems

Asymmetric and symmetric systems can be combined to leverage each system's peculiarities. A common scheme is to encrypt data using a symmetric algorithm with a secret key that is randomly generated. The secret key is then encrypted using an asymmetric encryption algorithm to allow secure distribution among the parties who need access to the encrypted data. Secure communications

©ISACA. All Rights Reserved.

can thus be sent with both the speed of symmetric systems and the ease of key-distribution of asymmetric systems. In addition, because creating the secret key is an effortless operation, it can be employed just for a limited amount of data, after which a new secret key can be chosen. This limits the possibilities of malicious third parties decrypting the whole set of data because they would be required to attack multiple secret keys. This combined scheme is used in protocols to protect web traffic, such as SSL/TLS, and to encrypt email, such as S/MIME. In the latter case, the resulting document—the combination of the encrypted message and the encrypted secret key—is called a digital envelope.

Transport Layer Security

TLS is a cryptographic protocol that provides secure communications on the Internet. TLS is a session- or connection-layered protocol widely used for communication between browsers and web servers. Besides communication privacy, it also provides endpoint authentication. The protocols allow client-server applications to communicate in a way designed to prevent eavesdropping, tampering and message forgery.

TLS involves a few basic phases:

- Peer negotiation for algorithm support
- Public-key, encryption-based key exchange and certificate-based authentication
- Symmetric cipher-based traffic encryption

During the first phase, the client and server negotiate the cryptographic algorithms that will be used. Choices supported by current implementations are:

- **For public-key cryptography**—RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) or Fortezza
- **For symmetric ciphers**—RC4, International Data Encryption Algorithm (IDEA), Triple DES or AES
- **For one-way hash functions**—SHA-1 or SHA-2 (SHA-256)

TLS runs on layers above the TCP transport protocol and provides security to application protocols, even if it is most used with HTTP to form HTTPS. HTTPS serves to secure World Wide Web (WWW) pages for applications. In e-commerce, authentication may be used in business-to-business (B2B) activities, in which the client and the server are authenticated, and business-to-consumer (B2C) interaction, in which only the server is authenticated. TLS consists of two protocols:

1. **Handshake Protocol**—The TLS Handshake Protocol negotiates and establishes the TLS connection between the two parties. It provides a secure communication channel for data transmission. The whole process is completed before data is transmitted.
2. **TLS Record Protocol**—The TLS Record Protocol is the actual secure communications

method for transmitting data. It supports the encryption and authentication of packets throughout their transmission between the parties. It also performs some compression of the packets and relies entirely upon the handshake protocol for its operation.

TLS replaced a similar protocol, SSL, for which a significant vulnerability was found in 2014. Although TLS and SSL are distinct protocols and are not compatible, references to SSL are common when the intent is to refer to TLS. IS auditors evaluating TLS implementations should take care to determine whether a reference to SSL is legitimate (suggesting a security vulnerability) or might instead refer to TLS in practice.

IP Security

IPSec is used for securing the communications at IP-level among two or more hosts, two or more subnets, or hosts and subnets. This IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods. For the transport method, the data portion of each packet—referred to as the encapsulation security payload (ESP)—is encrypted, achieving confidentiality over the process. In the tunnel mode, the ESP payload and its header are encrypted. To achieve nonrepudiation, an additional authentication header (AH) is applied. In establishing IPSec sessions in either mode, security associations (SAs) are established. SAs define the security parameters that should be applied between the communicating parties as encryption algorithms, keys, initialization vectors, life spans of keys, etc. Within either the ESP or AH header, respectively, an SA is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is a unique identifier that enables the sending host to reference the security parameters to apply, as specified, on the receiving host. The steps for computers to exchange data with the IPSec protocol are:

- The sender system determines whether data transmission requires IPSec by confirming with its security policy. If it does, it initiates a secure IPSec transmission with the recipient system.
- Both systems negotiate the requirements to establish a secure connection, including mutually agreeing on the encryption, authentication and SA parameters.
- The system sends and receives encrypted data, validates that it came from a trusted source and ensures the content is reliable.

- Once the transmission is complete or the session has timed out, the system ends the IPSec connection.

Security Association

An IPsec SA is a simple (one-way) connection used to negotiate ESP or AH parameters. The entire SA process is managed by the Internet Security Association and Key Management Protocol (ISAKM), which is a framework for the negotiation and communication of SAs. Information an SA contains includes:

- Material for encryption and authentication keys
- The algorithms that can be used
- The identities of the endpoints
- Other parameters that are used by the system

SAs require keying material for authentication and encryption. The managing of keying material that SAs require is called key management. The IKE protocol handles key management automatically using asymmetric cryptography. SAs on Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) packets can use automatic key management.

5.6.11 Kerberos

Kerberos is a ticket authentication mechanism that employs a third-party entity to prove identification and provide authentication in a Distributed Computing Environment (DCE). It offers an SSO solution for users and provides protection for logon credentials while allowing principals to positively identify themselves and participate in a DCE. The current version of Kerberos, Kerberos 5, uses the AES symmetric encryption protocol. The major advantage of Kerberos is that it provides confidentiality and integrity for authentication traffic using end-to-end security. This protects the organization against eavesdropping and replay attacks. Kerberos also uses several different elements, as shown in **figure 5.34**.

Figure 5.34—Components of Kerberos

Component	Description
Key Distribution Center (KDC)	The KDC is the trusted third party that provides authentication services to clients. It supports symmetric encryption and maintains secret keys for all members. Both clients and servers should be registered with the KDC.
Ticket-Granting Server (TGS)	A TGS is a logical KDC component used as a trusted third party. It validates the use of a ticket for a specified purpose, such as database access.
Authentication Server (AS)	The purpose of the AS is to host the TGS for ticket distribution. It also verifies or rejects the authenticity and timeliness of tickets.
Ticket-Granting Ticket (TGT)	TGT is a user authentication token issued by the KDC for requesting access tokens from the TGS. It proves that a subject has successfully authenticated through a KDC and is therefore authorized to request tickets to access other objects. Subjects present the encrypted TGT when requesting tickets to access objects.
Service Ticket (ST)	ST is the encrypted proof that a subject is authorized to access an object. Subjects request tickets to access objects with specific usage parameters and lifespans. If a subject is successfully authenticated and therefore authorized to access an object, the Kerberos system issues a ticket.

Kerberos maintains a directory service for the storage of all the data pertaining to its operations. In brief, the steps in the Kerberos logon process are:

- First, the user logs on with a username and password.
- The client encrypts the username with a symmetric encryption algorithm (e.g., AES) for transmission to the Key Distribution Center (KDC).
- The KDC verifies the username credentials stored in its directory service.
- Upon successful verification, the KDC generates a symmetric key for client use and for the Kerberos server.
- The KDC encrypts the symmetric key using the hash of the user's password. It also simultaneously generates an encrypted Ticket-Granting Ticket (TGT).
- The KDC transmits the encrypted symmetric key and TGT to the client.
- The client installs the TGT and decrypts the symmetric key using a hash of the user's password.
- The client then requests a service ticket by sending the TGT to the Ticket-Granting Server (TGS). Once the service ticket is provided, the authentication process is deemed successful and secure communication begins.

©ISACA. All Rights Reserved.

The IS auditor should note that the client's password is never transmitted over the network but only verified. However, Kerberos presents a major risk to the organization because it presents a single point of failure in the form of the KDC. If the KDC gets compromised, the secret key for every system on the network also gets compromised. Also, if a KDC is offline, no subject authentication takes place. Kerberos has strict time requirements. If a system is not correctly synchronized or if the time changes, the TGT becomes invalid and the system cannot receive any new tickets. In short, the client is denied access to system resources.

5.6.12 Secure Shell

SSH is a client-server program that provides a secure, encrypted command-line shell session from the Internet for the purpose of remote logon. It is similar to a VPN and uses strong cryptography to protect data, including passwords and administrative commands transmitted between systems on a network. SSH has largely supplanted Telnet as the foremost remote login protocol. It is typically implemented between two parties by validating each other's credentials through the use of digital certificates. The implementation of SSH was critical in replacing Telnet, which transmitted passwords in the clear, making them available to unauthorized parties. SSH is implemented at the application layer, as opposed to being implemented at the network layer, just like the IPSec implementation. The SSH protocol uses encryption to secure the connection between a client and a server; all user authentication, commands, output and file transfers are encrypted to protect against attacks in transit through the network. SSH is designed to provide strong, encrypted verification and communication between the user and a remote computer. SSH technology is based on the client-server model and provides an ideal way to access remote devices over unsecured networks, like the Internet. The technology is typically used by administrators for several functions including:

- Logging into remote systems for support and maintenance
- Transferring files from one computer to another
- Remote execution of command
- Offering support and updates

SSH Key Security Best Practices

There are several best practices for securing SSH keys, including:

- **Centralizing SSH key management**—Identify and inventory all SSH keys and manage them centrally to eliminate key sprawl. Key sprawl occurs when an organization stores keys in many various places, which increases the chances for key breaches due to the increased attack surface.
- **Changing the default SSH port**—Changing the default SSH port is a simple best practice associated with the defense-in-depth principle. It eliminates a huge amount of basic attack vectors that rely on default ports to gain entry. Default ports are generally well-known to attackers.
- **Disabling the SSH root login**—Root login provides access to the core components of SSH. The organization should ensure that the SSH root login is disabled. Eliminating the SSH root account, especially from remote access, significantly reduces the organization's attack surface.
- **Implementing key attribution**—Key attribution involves tying the SSH keys back to an individual, not a shared, account. When implemented effectively, the key provides an effective SSH audit trail and more direct oversight over SSH keys.
- **Implementing key rotation**—Key rotation is an important component of the SSH key security best practices. The organization should ensure that users are forced to generate SSH keys on a regular basis. The repeated use of the same passwords and passphrases across multiple accounts or iterations should be disallowed. This protects the SSH technology infrastructure from password re-use attacks.
- **Performing continuous audits**—To keep up to date with the operations of SSH technologies, an organization should perform continuous audits. The focus of the audits should include recording and verifying all privileged sessions started through SSH key authentication. Continuous audits also assist the organization in meeting legal and compliance requirements.
- **Implementing firewall technology**—An organization can implement firewall technology for securing SSH. It should define rules that accept incoming SSH traffic emanating only from allowlisted sources by IP address, port or protocol. The firewall can be configured to block IP addresses based on the rate they connect to the SSH. Port knocking can also be implemented to make it harder for threat actors to detect open SSH ports.

 ©ISACA. All Rights Reserved.

5.6.13 Domain Name System Security Extensions

Domain name system security extensions (DNSSEC) is a cryptographic technology developed to resolve DNS security issues as DNS is inherently insecure and does not consist of any security measures. It provides DNS clients (also known as resolvers) with DNS data origin authentication, authenticated denial of existence and data integrity services. It adds digital signatures to a DNS to determine the authenticity of the source domain name. It also uses a chain to verify that the source domain name matches the DNS record stored at the authoritative DNS. If it fails to find the source, it discards the response. This ensures that the user always connects to the actual address for a domain name.

DNSSEC is composed of two stages: signing and validation during the signing process. DNSSEC signs all the data sent on DNS records to enable verification of its authenticity. DNS records are signed with the private key and the signatures are stored in DNS name servers. Security validation is carried out through PKI authentication using two cryptographic keys: one public and one private. By checking the signature that corresponds to a requested DNS record, a user can verify that the record originates directly from its authoritative name server.

DNSSEC prevents third parties from forging records and guarantees a domain's identity by preventing DNS cache poisoning and DNS false zones:

- **DNS cache poisoning**—DNS cache poisoning is a man-in-the-middle attack in which attackers flood a DNS resolver with false DNS information and insert false results into the cache of the DNS resolver. The DNS resolver provides the erroneous or malicious web address to those seeking to access the legitimate website.
- **DNS False zones**—DNSSEC can protect against malicious DNS attacks that provide phony results for zones that are not in existence by exploiting gaps between zones. With DNSSEC, the entire zone is secured with added mechanisms to prevent gap exploitation in unsigned zones. This is commonly referred to as authenticated denial of existence.

DNSSEC can unintentionally introduce critical vulnerabilities. The IS auditor should be aware of security vulnerabilities arising out of the implementation of DNSSEC, including:

- **DoS risk**—DNSSEC can increase the risk and amplify the effects of distributed denial of service (DDoS) attacks where a system is disrupted by traffic from multiple devices at once.
- **Increase in query responses**—DNSSEC increases the number of DNS query responses, as the technology needs additional fields and cryptographic information to properly verify records. High-volume responses afford malicious actors greater attack volume than they would have if DNSSEC were not implemented.
- **Slow performance**—Since TCP is a slow connection-oriented protocol, DNSSEC relies on UDP, a faster yet riskier protocol. UDP has no specific security requirements for opening, maintaining or terminating connections. It also does not guarantee delivery of data to its destination and provides a basic functionality for checking errors using checksum. As it requires no handshake, data transmitted using UDP can be easily intercepted by malicious attackers.

5.6.14 Email Security

Email security is the security practice of ensuring email CIA. It helps protect an organization's email attack surfaces from unauthorized access, compromise and/or loss. Email security is critical because emails, especially enterprise emails, contain sensitive information that can be tampered with by threat actors.

Common Email Attacks and Techniques

Email attacks often cause serious damage to the organization's sensitive data and in some cases to its reputation. There are many tactics that threat actors use to attack emails. Some of the most common email attacks and techniques are:

- **Bombing**—Characterized by abusers repeatedly sending an identical email message to a particular address
- **Spamming**—Spamming refers to sending emails, often unsolicited commercial email or junk email, to hundreds or thousands of users (or to lists that expand to many users). It may also be carried out by sending a message to a mailing list or using an automated response, such as a vacation alert, that is not set up correctly.
  - Spam is considered a business risk because it causes inconvenience and has severe impacts on productivity.
  - Responding to spam validates the email address of the recipient and gives away information.
  - Spam may be combined with email spoofing, making it more difficult to determine the sender.

©ISACA. All Rights Reserved.

  - Spam is managed using the Sender Permitted Framework (SPF) protocol and with the help of tools such as Bayesian filtering and grey listing.
- **Spoofing**—Spoofing may take different forms, but all have a similar result: A user receives an email message that appears to have originated from one source but actually came from a different source. Email spoofing is often an attempt to trick a user into making a damaging statement or releasing sensitive information, such as passwords or account information. Examples of spoofed email that could affect the security of a site include:
  - Email claiming to be from a system administrator and requesting users change their passwords to a specified string and threatening to suspend their account if they do not make the change
  - Email claiming to be from a person in authority and requesting users send a copy of a password file or other sensitive information
- **Business email compromise (BEC)**—A BEC attack targets specific employees, typically those who authorize financial transactions, to trick them into transferring money into an account controlled by the attacker. BEC attacks involve a lot of planning and research in order to be effective. For example, the attacker has to amass large quantities of information relating to the target organization's executives, employees, customers, business partners and potential business partners, and statutory bodies. This information is critical in tricking victims and convincing them to pay funds. To address BEC, employees must be trained to be alert to emails with a fake domain or emails that impersonate a vendor. They also need to show a strong sense of urgency if they encounter anything that looks suspicious.

Implementing security on email is possible, but the efforts should be in tune with the value and confidentiality of the messages being exchanged. An organization can use several protocols, services, and solutions to add security to emails without requiring a complete overhaul of the entire Internet-based Simple Mail Transfer Protocol (SMTP) infrastructure. **Figure 5.35** explains some of the most common email security solutions.

Figure 5.35—Email Security Technologies

Email Security Solution	Description
Secure Multipurpose Internet Mail Extensions (S/MIME)	S/MIME is an email security standard that offers authentication and confidentiality for email through the application of public key encryption and digital signatures. It authenticates both the identity of the sender and receiver through X.509 digital certificates, verifies message integrity, and ensures the privacy of a message and its contents. S/MIME provides secure signed messages and envelopes to ensure integrity, sender authentication, confidentiality and nonrepudiation.
MIME Object Security Services (MOSS)	MOSS is a protocol that uses encrypted frameworks signed by multiple parties. It applies digital signatures to MIME objects and can provide authentication, confidentiality, integrity and nonrepudiation for email messages. However, MOSS has never been widely used.
Privacy Enhanced Mail (PEM)	PEM is a set of email protocols and mechanisms that provide authentication, integrity, confidentiality and nonrepudiation. It uses Rivest-Shamir-Adleman (RSA) and Data Encryption Standard (DES) encryption and is based on the X.509 standard. It enables secure and safe email communication over the Internet.
Domain Keys Identified Mail (DKIM)	DKIM is an email authentication method that uses a digital signature to inform the receiver that the message was sent and authorized by the domain owner. It is used to ensure that valid emails are sent by an organization through verification of domain name identity. Its primary purpose is to detect forged sender addresses. Forging addresses is one of the most common techniques used in email phishing and spam attacks.

 ©ISACA. All Rights Reserved.

Figure 5.35—Email Security Technologies (cont.)

Email Security Solution	Description
Pretty Good Privacy (PGP)	PGP is a public-private key system that uses a variety of encryption algorithms to encrypt files and email messages. It has gained wide popularity, as it provides key aspects of security—namely authentication, integrity, privacy and nonrepudiation—in email communications. The major advantage of PGP is that it is an open-source software package freely available to everyone.

Email Security Controls

Email security should be part of the overall security framework in an organization because email use is widespread and often involves communication of sensitive data. The IS auditor should give adequate attention to email security, as email is often the primary attack vector used by threat actors to launch other sophisticated attacks, such as social engineering attacks and installation of malware. Some of the controls that can be implemented to enhance email security are:

- **Spam filters**—Spam filters detect spam and prevent it from landing in victims' inboxes, directing it instead to a spam or junk mail folder. Spam filters identify and block unwanted emails by examining email contents and searching for certain patterns that constitute abnormal email traffic.
- **Email encryption**—Email can be encrypted in transit so that even when attackers manage to intercept an email, they cannot understand it without the decryption key. This reduces the risk of data leakages and regulatory and policy violations while enhancing email communication security.
- **Antivirus protection**—An antivirus tool screens emails and their associated attachments for viruses and warns users when something suspicious is detected. Viruses are a major security risk, as they can infect an entire email network as well as email servers and applications.
- **Secure email gateway (SEG)**—An SEG filters out potentially unwanted emails in line with the settings as configured by the IS security administrator. The main advantage is that it can be deployed either on-premises or in the cloud, which offers ease of use. An SEG increases security by contributing to the effectiveness of the multilayered security protection architecture.
- **Email attachment control (EAC)**—Most email attacks and attacks that use email as an attack vector rely on tricking users into exposing sensitive information through clicking on links or attachments in an email that contains malicious software. An EAC system allows users to see the type of files sent before opening them. This helps users to verify email before opening it.

5.6.15 Encryption Audit Procedures

When carrying out an encryption audit in an organization, the primary objective of an IS auditor is to ensure that the organization has controls in place to manage the overall data encryption processes. **Figure 5.36** outlines some of the encryption audit procedures that can be followed in an audit of data encryption.

Figure 5.36—Encryption Audit Procedures

Encryption governance	• Verify that written encryption policies and procedures are in place. • Ascertain the presence of a data classification system. • Determine if encryption risk assessments are regularly carried out. • Verify that there is no duplication of encryption. • Verify that management has instituted controls to support encryption, such as dual control and separation of duties. • Verify that the organization complies with all data protection rules and regulations. • Verify the existence of an audit system associated with encryption.

©ISACA. All Rights Reserved.

Figure 5.36—Encryption Audit Procedures (cont.)

Encryption design	• Verify that the process and the selection of an encryption algorithm are effective and efficient. • Review documentation from management attesting that the chosen algorithm ensures adequate protection. • Verify that management has implemented processes to ensure minimal effect on interfacing and other systems. • Determine if management has applied respected standards such Transport Layer Security (TLS) as part of its cryptographic system. • Check whether the cryptographic system in place is compatible with the applications. • Verify that the keys contain all the required properties, including the length, composition and management of the key according to policy. • Ascertain the difficulty of key generation and modification.
Key management	• Verify whether changes to the cryptographic system are adequately controlled. • Determine whether changes or updates to the cryptographic system are performed only by authorized individuals. • Verify that the key transmission is controlled according to a specific written procedure. • Determine if the creation, rotation and destruction of keys based on time is in accordance with policy or best industry standards. • Verify that users and operators do not handle keys.
Digital signatures	• Verify that private keys are never backed up, as backing up private keys increases exposure. • Determine whether the organization uses different key pairs for encryption and digital certificates.
Encryption algorithms	• Ascertain if management has considered the need for the complex mathematical equations. • Verify that the cost of deciphering does not exceed the value of the information the encryption system is supposed to protect.

5.7 Public Key Infrastructure

Public key infrastructure (PKI) is a system for distributing public keys through digital certificates. A PKI is made up of policies, procedures, hardware, software and personnel required to create, manage, store, distribute and revoke public key certificates.

5.7.1 Digital Certificates

A PKI system validates that the public key distributed through the certificate belongs to the individual or organization. Essentially, an individual obtains a digital certificate through a certificate authority (CA), such as Verisign or Thawte, containing one's public key. The CA digitally signs the certificate, validating it, and thus the public key belongs to the alleged owner. CAs also sell digital certificates for varying prices, depending on the type of certificate. An individual or organization may have to present a form of authentication (such as an address or credit report), depending on the type of certificate.

A certificate policy (CP) is a document that identifies the various actors in PKI as well as their roles, duties and responsibilities. It specifies practices such as how certificates should be used, how keys should be generated and how certificate names should be selected.

As well as issuing certificates, a CA maintains a list of compromised certificates (i.e., those whose private key has been leaked or lost) called the certificate revocation list (CRL). In some cases, certificates may be marked as revoked in the CRL when the owner of the certificate voluntarily declares not to use the corresponding key pair any longer. This allows a party to reject a signed document when a signature is generated after the private key has been compromised or revoked.

Certificates usually contain a certificate practice statement (CPS), which is a statement about the way a CA issues certificates. It may contain:

- The type of certificates issued
- Policies, procedures and processes for issuing, renewing and recovering certificates
- Cryptographic algorithms used
- The key length used for the certificate
- The lifetime of the certificate issued by the CA
- Policies for revoking certificates
- Policies for CRLs
- Policies for renewing certificates

 ©ISACA. All Rights Reserved.

Registration authorities (RAs) are delegated some administrative functions for a specific community by the CA. For example, an international corporation may have a PKI setting if national branches act as RAs for the employees in that nation. The administrative functions that a particular RA implements will vary based on the needs of the CA but must support the principle of establishing or verifying the identity of the subscriber. These functions may include:

- Verify information supplied by the subject (personal authentication functions).
- Verify the right of the subject to requested certificate attributes.
- Verify that the subject actually possesses the private key being registered and that it matches the public key requested for a certificate (generally referred to as proof of possession).
- Report key compromise or termination cases where revocation is required.
- Assign names for identification purposes.
- Generate shared secrets for use during the initialization and certificate pick-up phases of registration.
- Initiate the registration process with the CA on behalf of the subject entity.
- Initiate the key recovery process.
- Distribute the physical tokens (such as smart cards) containing the private keys.

5.7.2 Key Management

The IS auditor should be cognizant of the various activities involved in key management. The auditor should also remember that key management is typically difficult with symmetric encryption but is much simpler with asymmetric encryption. Several tasks related to key management are detailed in **figure 5.37**.

Figure 5.37—Key Management Practices

Area	Description
Key creation	Also known as key generation, creation is the process of generating keys for use in cryptographic processes through a device or program known as the key generator.
Key distribution	Key distribution is the process of transferring a key to a user or system. This process must be secure, and secure encryption technologies are often used for the purpose.
Key storage and custody	Keys must be stored securely on the computing device. Often, they are stored in a protected storage facility such as the Windows certificate store. Methods such as dual custody, split knowledge and custody generally require two or more people to share access to a key. It is crucial for the IS auditor to be aware that some keys may be placed under key escrow.
Key rotation	Keys are typically not meant to be used forever, as this increases the risk of them getting stolen or lost, or malfunctioning. To mitigate this risk, it is advisable that organizations retire old keys and implement new ones.
Key recovery and backup	Key recovery is a critical element in key management. Losing a private key often leads to losing data if the key is not placed in escrow. Key escrow enables the organization to safely store keys for later recovery. There is also a need to have a backup method in case the key malfunctions. PKIs typically offer inbuilt backup and recovery facilities.
Key destruction	A key can be suspended (placed on temporary hold), revoked (no reinstatement is possible), expired (inactive until renewed) or destroyed. Key destruction often happens at the end of the key lifecycle or after a compromise is detected on the key. The IS auditor should monitor the key destruction process to ensure that it is appropriate and secure.

5.7.3 Certificate Revocation

Certificate revocation is the process through which the use of a certificate is terminated prior to the expiration of its validity period. The decision to revoke a certificate involves determining the reasons for the revocation, mapping the revocation reasons to the organization's revocation policy, and then performing the revocation.

IS auditors should advise management on the risk involved in the continual use of certificates that would have been revoked. Once certificates are revoked, they become invalid, and transacting parties will cease to place reliance on them for their security. Various reasons lead to certificate revocation, such as:

- **Changes in affiliation**—This includes circumstances in which an individual is terminated, resigns or dies,

©ISACA. All Rights Reserved.

or the computer account to which the certificate was issued is no longer in use. Affiliation change can also occur when individuals change roles within an organization and no longer require the certificate associated with their previous roles.

- **Compromise of the private key**—If the private key is suspected to have been compromised and/or is in the hands of an unauthorized individual, a certificate can be revoked. Typical examples include stolen laptops and tablets causing all private keys stored on the devices to be compromised. The IS auditor should be aware that once a CA's private key is revoked, the CA hierarchy considers all certificates below that CA revoked as well.
- **Cessation of operation**—Cessation of operation includes such events in an organization as a server or workstation getting decommissioned. This renders all the certificates issued to the server revoked as the certificates are no longer required. In other words, the CA is also decommissioned.
- **Superseded**—In PKI, best practice dictates that a new certificate must be issued if an issued certificate is replaced for any reason. For example, if a certificate template is updated or the CA issues the certificate in error and certificates are reissued, the previous certificate can be revoked.
- **Unspecified**—An organization can simply revoke a certificate without providing a specific revocation reason. However, this is not recommended, as it provides an audit trail pinpointing the reasons the certificate was revoked.
- **CA compromise**—A certificate may be revoked due to compromise of the CA itself. For example, the details listed in the certificate may have been tampered with and the CA needs to reissue the certificate. A certificate may also be illegitimate, such as when the certificate was fraudulently signed with a stolen key.

5.7.4 Certificate Revocation List

A CRL is a list of digital certificates that have been revoked by the issuing CA before their scheduled expiration date.[42] These should no longer be trusted. CRLs are a type of blacklist used by browsers to verify the validity and trustworthiness of a certificate. Depending on a CA's operating policies and procedures, CRLs are typically published on a regular periodic basis. When checking for the revocation status of a certificate, an application or browser retrieves the current CRL from a specified CRL distribution point (CDP). The CDP is the location on an LDAP directory server or web server where the CA publishes its CRLs.

There are two different states of revocation—revoked and hold. A certificate is irreversibly revoked if it was improperly made by the CA, the private key was compromised and/or there was nonadherence to specific policy requirements. The hold state of a certificate is reversible and is used to note the temporary invalidity of the certificate—for example, if a user is unsure whether the private key has been lost or stolen. If the private key is found and nobody accessed it, the certificate status could be reinstated and become valid again.

While CRLs may vary, they should include:

- CRL issuer name/common name (CN)
- Revocation date and time
- Reasons for the revocation
- Specific revocation time period
- Certificate's extensions
- Signature algorithm of the certificate
- The certificate's serial number
- The date the next CRL will be issued

Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) is a protocol used to request the revocation status of a digital certificate. Instead of downloading multiple CRLs and analyzing them annually, a client can query the CA's server and instantly know whether a certificate is valid, revoked or unknown. The other advantage is that OCSP provides more updated information about a certificate's revocation status.

An emerging solution is to use OCSP stapling, which is an enhancement of OCSP protocol. Where OCSP stapling is enabled, it becomes unnecessary for a browser or application to send OCSP requests directly to the CA. Instead, the web server caches the OSCP response from the CA and then "staples" the OSCP response to the certificate it sends to the browser. OCSP improves performance by eliminating the costs involved in communicating with the issuing CA. There is also increased security due to the reduction in the attack surface. As the CA gets requests for websites and not users, user privacy is also enhanced.

[42] *Op cit* CSRC glossary

 ©ISACA. All Rights Reserved.

5.7.5 PKI Infrastructure Risk

While PKI is very important in an organization, it has its own associated risk, including:

- **Outdated protocols**—Outdated cryptographic protocols are a major risk as they leave the organization prone to security incidents and data breaches.
- **Weak cryptographic keys**—Weak cryptographic key lengths smaller than 2,048 bits are considered vulnerable and insecure. A large number of weak keys cause issues with the privacy and confidentiality of the data, communications and transactions encrypted using the keys.
- **Infrequent key rotation**—Weak key lengths smaller than 2,048 bits are considered vulnerable and insecure. Because keys do not expire, the frequent rotation of keys is not a common security practice, giving room to cybercriminals to manipulate users.
- **Mismanaged certificates**—Failure to properly manage, issue, renew or revoke digital certificates has a huge impact on organizational security. Expired certificates can lead to unexpected outages and can be gateways for bad actors to move laterally within an organizational network, leading to data breaches that impact an enterprise's security and compliance posture.
- **Lack of automation**—Managing large volumes of digital certificates and private keys taxes an organization's time and resources. Manually monitoring the multitude of certificates, their locations, owners and expiry dates creates additional complexities and is prone to errors. Keys can also be lost or stolen.
- **Insufficient skills and resources**—The talent gap and lack of resources are some of the major problems organizations face in PKI. Organizations require highly skilled IS security professionals for effective PKI architecture and maintenance. However, due to the current talent gap, many organizations eventually hire less-skilled professionals.
- **Unclear certificate ownership**—The primary aim of assigning certificate owners and approvers is to manage and organize the certificate life cycle processes and ensure that only authorized security professionals can alter elements of the PKI infrastructure.
- **Lack of policies**—It is crucial for organizations to enforce well-defined rules and certificate policies to minimize the chances of errors and ensure that the policies are adhered to strictly. A lack of enterprise-wide PKI policies and inconsistencies in policy application provide room for noncompliance and risk of fines and penalties.
- **Limited visibility**—Both lack of centralized inventory and visibility into all certificates in use across the organizational environment and lack of a centralized certificate inventory contribute to weakening the overall PKI architecture. Rogue and insecure temporary certificates may exist and operate in stealth mode, practically impossible to detect.
- **Poor private key management**—In PKI, private keys must remain private since they are a gateway to critical information in the organization's entire infrastructure. Improper key management can result in private key compromise in which an attacker manages to obtain the private key and decrypt sensitive information.
- **Compromised root CA**—The root certificate provides the signature that is used to bind the identity to the public key. It lays a foundation of trust in the PKI architecture by indicating whether a certificate is valid or not. If the root CA is untrustworthy, the overall PKI cannot be trusted. It is pivotal to store the root CA offline in a well-protected vault. A compromised root CA can break the entire chain of trust and cripple the overall PKI architecture.
- **Poor patch management**—Knowledge of patch management is critical in PKI. Inefficient patch management often leads to failure by the organization's IS security teams to promptly detect PKI vulnerabilities and reduce response time.

5.7.6 Audit Procedures for PKI

A secure PKI relies on effective audit procedures that can identify risk in PKI and enable IS auditors to provide assurance and advice on the security of PKI in an organization. IS auditors typically apply several procedures in an audit of PKI (**figure 5.38**).

©ISACA. All Rights Reserved.

Figure 5.38—Audit Procedures for Public Key Infrastructure

Audit Category	Audit Procedures
Certificate authority (CA)	• Determine whether the CA has an information security policy in place. • Evaluate the CA's physical controls. • Verify that the CA performs background checks on its personnel. • Determine whether the CA backs up audit logs. • Inspect how the CA performs key management throughout the entire key management life cycle. • Verify whether the CA systems are appropriately isolated.
Registration authority (RA)	• Verify whether enrollment of RAs is as specified in the CPS. • Verify that the role of the RA is restricted to the submission of details to the CA and no other roles are assigned. • Ascertain whether the RA onboarding and termination procedures are defined. • Determine whether communication channels between the CA and the RA are sufficiently secure for the certificates. • Verify that all activities of the RA are logged. • Verify that RA access to CA systems is based on multifactor authentication (MFA). • Inspect the previous audit reports undertaken on the RA operations and identify issues of noncompliance. • Verify the list of RA violations (if any) and corresponding actions taken by the CA.
Certificate	• Verify that the certificate information is published on the CA's website. • Ascertain whether certificate renewal is per the CPS. • Verify whether certificate suspension and revocation is per the CPS. • Ascertain the availability of a secure certificate distribution system.
Key management	• Check the hardware used to generate keys for Federal Information Processing Standards (FIPS) compliance. • Verify that the keys are distributed using secure mechanisms. • Determine the appropriateness of procedures available to address cases of key compromise. • Verify that the storage of the keys is secure and appropriate. • Verify whether the CA maintains key escrow. • Check on the availability and operation of key backup and archiving procedures. • Ascertain whether procedures for key destruction are appropriate and prevent data remaining.
Certificate policy (CP)	• Verify that the organization has an approved CP in place. • Ascertain whether the CP in place is current. • Determine whether the CP is being followed by all PKI parties, and document identified gaps.
Certificate practice statement (CPS)	• Check whether the CPS complies with applicable laws and regulations. • Verify that the CPS is available to relevant parties. • Ascertain whether responsibilities for maintaining the CPS are appropriately assigned. • Verify that the modification of the CPS follows defined processes and procedures. • Ascertain whether the CPS has a valid object identifier.

 ©ISACA. All Rights Reserved.

Figure 5.38—Audit Procedures for Public Key Infrastructure (cont.)

Audit Category	Audit Procedures
Certificate revocation list/ Online Certificate Status Protocol (CRL/OCSP)	• Verify whether the CRL or OCSP is in place. • Determine whether the CRL issued is digitally signed by the CA. • Verify that a secure mechanism for CRL distribution is in place. • Take a sample of CRL entries and verify that the revoked certificate remains on the CRL up to the end of the certificate's validity period. • Determine whether the OCSP response processes and procedures are automated. • Verify that the CRL and OCSP services comply with relevant industry standards and regulations.

5.8 Cloud and Virtualized Environments

Virtualization and cloud-based infrastructure have brought dramatic changes and risk to IS infrastructure. These technologies have significantly altered the management of IS environments. While virtualization and cloud environments have huge similarities, they are not the same. Virtualization is a broad concept and generally refers to the transformation of physical technologies into virtual resources. Cloud, on the other hand, delivers virtualized resources on demand to users over the Internet. It is critical for IS auditors to understand the types of risk such systems face and advise on the implementation of appropriate mitigating measures.

5.8.1 Virtualization

Virtualization provides an enterprise with a significant opportunity to increase efficiency and decrease costs of IT operations. However, virtualization also introduces additional risk. At a high level, virtualization allows multiple OSs (guests) to coexist on the same physical server (host) in isolation from one another. Virtualization creates a layer between the hardware and the guest OSs to manage shared processing and memory resources on the host. Often, a management console provides administrative access to manage the virtualized system.

Data centers and many other organizations use virtualization techniques to create an abstraction of the physical hardware and make large pools of logical resources consisting of CPUs, memory, disks, file storage, applications and networking. This approach enables greater availability of these resources to the user base. The main focus of virtualization is to enable a single physical computing environment to run multiple logical, yet independent, systems at the same time.

The most common use for full virtualization is operational efficiency, which streamlines the use of existing hardware by placing greater loads on each computer. Second, using full virtualization of desktops enables end users to have one computer hosting multiple OSs if needed to support various OS-dependent applications. Furthermore, an IT team can better control deployed OSs to ensure they meet organizational security requirements, that security threat detection and respective control requirements are dynamic, and that the virtual desktop images can be changed to respond to new threats.

Elements of the virtualized computing environment normally include:

- Server or other hardware product
- **Virtualization hypervisor**—A piece of computer software, firmware or hardware that creates and runs virtual machine environment, normally called the "host"
- **Guest machine**—Virtual environment elements (e.g., OS, switches, routers, firewalls, etc.) residing on the computer on which a hypervisor host machine has been installed

A fully virtualized environment can be deployed using:

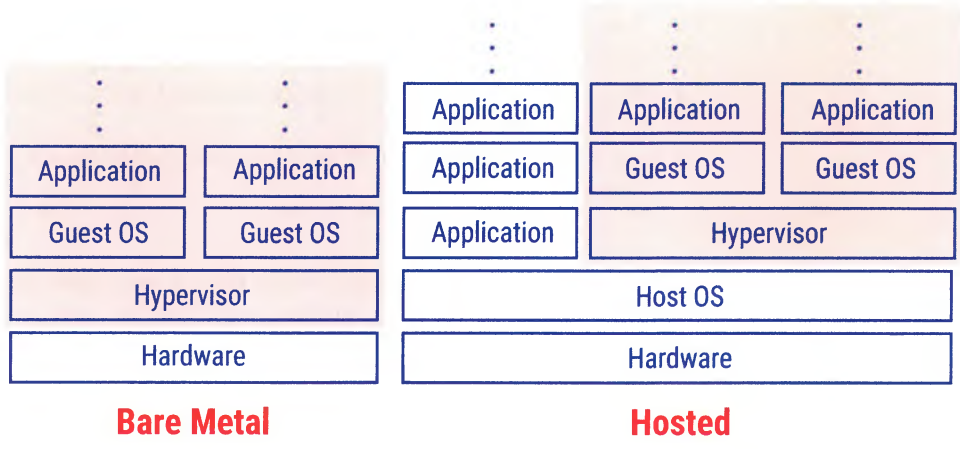
- **Bare metal/native virtualization**—Bare metal virtualization occurs when the hypervisor runs directly on the underlying hardware without a host OS.
- **Hosted virtualization**—Hosted virtualization occurs when the hypervisor runs on top of the host OS (Windows, Linux or MacOS). Architectures usually have an additional layer of software (the virtualization application) running in the guest OS that provides utilities to control the virtualization while in the guest OS, such as the ability to share files with the host OS.
- **Containerization**—Containers include an application and all of its dependencies but share the kernel with

©ISACA. All Rights Reserved.

other containers. A container runs as an isolated process in user space on the host OS.

Figure 5.39 compares two virtualization architectures.

Figure 5.39—Full Virtualization Architectures



Source: Reprinted courtesy of the National Institute of Standards and Technology, US Department of Commerce. Not copyrightable in the United States.

IS auditors need to understand the advantages and disadvantages of virtualization to determine whether the enterprise has considered the applicable risk in its decision to adopt, implement and maintain this technology. **Figure 5.40** summarizes several advantages and disadvantages of virtualization.

Although virtualization offers significant advantages, it brings risk that an enterprise must manage effectively. Because the host in a virtualized environment represents a potential single point of failure within the system, a successful attack on the host could result in a compromise that is larger in both scope and impact.

To address risk, an enterprise can often implement and adapt the same principles and good practices for a virtualized server environment that it would use for a server farm. These include:

- Strong physical and logical access controls, especially over the host and its management console
- Sound configuration management practices and system hardening for the host, including patching, antivirus, limited services, logging, appropriate permissions and other configuration settings
- Appropriate network separation, including the avoidance of virtual machines (VMs) in the DMZ and the placement of management tools on a separate network segment
- Strong change management practices

Figure 5.40—Advantages and Disadvantages of Virtualization

Advantages	Disadvantages
• Server hardware costs may decrease for both server builds and server maintenance. • Multiple operating systems (OSs) can share processing capacity and storage space that often goes to waste in traditional servers, thereby reducing operating costs. • The physical footprint of servers may decrease in the data center. • A single host can have multiple versions of the same OS, or even different OSs, to facilitate testing of applications for performance differences. • Creation of duplicate copies of guests in alternate locations can support business continuity efforts. • Application support personnel can have multiple versions of the same OS, or even different OSs, on a single host to more easily support users operating in different environments. • A single machine can house a multi-tier network in an educational lab environment without costly reconfigurations of physical equipment. • Smaller organizations that previously performed tests in the production environment may be better able to set up logically separate, cost-effective development and test environments. • If set up correctly, a well-built, single access control on the host can provide tighter control for the host's multiple guests.	• Inadequate configuration of the host can create vulnerabilities that affect not only the host, but also the guests. • Exploits of vulnerabilities within the host's configuration, or a denial-of-service attack against the host, can affect all the host's guests. • A compromise of the management console can grant unapproved administrative access to the host's guests. • Performance issues of the host's own OS can impact each of the host's guests. • Data can leak between guests if memory is not released and allocated by the host in a controlled manner. • Insecure protocols for remote access to the management console and guests can result in exposure of administrative credentials.

Typical Controls

Some concepts IS auditors should understand:

- Hypervisors and guest images (OSs and networks) are securely configured according to industry standards. Hardening should be applied to these virtual components as closely as to a physical server, switch, router, firewall or other computing device.
- Hypervisor management communications should be protected on a dedicated management network. Management communications carried on untrusted networks should be encrypted, and encryption should encapsulate the management traffic.
- The hypervisor should be patched as the vendor releases the fixes.
- The virtualized infrastructure should be synchronized to a trusted authoritative timeserver.
- Unused physical hardware should be disconnected from the host system.
- All hypervisor services, such as clipboard- or file-sharing between the guest OS and the host OS, should be disabled unless needed.
- Host inspection capabilities should be enabled to monitor the security of each guest OS. Hypervisor security services can allow security monitoring even when the guest OS is compromised.
- Host inspection capabilities should be enabled to monitor the security of activity occurring between guest OSs. Of special focus is communications in a nonvirtualized environment carried and monitored over networks by network security controls (such as network firewalls, security appliances and network IDS/IPS sensors).
- File integrity monitoring of the hypervisor should be used to monitor for signs of compromise.

Overall, migrating computing resources to a virtualized environment does not change the threat plane for most of the systems' vulnerabilities and threats. If a service has inherent vulnerabilities on a physical server or network product and it is migrated to a virtualized server, the service remains vulnerable to exploitation. However, the use of virtualization may also provide additional virtual environment attack vectors (e.g., hypervisor misconfiguration or security flaws, memory leakage, etc.), thus increasing the likelihood of successful attacks.

©ISACA. All Rights Reserved.

Types of high-level risk that are representative of the majority of virtualized systems in use are:

- Rootkits on the host installing themselves as a hypervisor below the OS, enabling the interception of any operations of the guest OS (i.e., logging password entry, etc.)—Antivirus software may not detect this, because the malware runs below the entire OS.
- Default and/or improper configuration of the hypervisor partitioning resources (CPU, memory, disk space and storage)—This can lead to unauthorized access to resources, one guest OS injecting malware into another or placing malware code into another guest OS's memory.
- On hosted virtualization, mechanisms called guest tools enable a guest OS to access files, directories, the copy/paste buffer, and other resources on the host OS or another guest OS—This functionality can inadvertently provide an attack vector for malware or allow an attacker to gain access to particular resources.
- Snapshots/images of guests' environments contain sensitive data (e.g., passwords, personal data, etc.) like a physical hard drive—These snapshots pose a greater risk than images because snapshots contain the contents of random-access memory (RAM) at the time they were taken and might include sensitive information that was not stored on the drive itself.
- In contrast to bare metal installations, hosted virtualization products rarely have hypervisor access controls—Therefore, anyone who can launch an application on the host OS can run the hypervisor. The only access control is whether someone can log into the host OS.

The IS auditor should keep in mind that the primary software component in virtualization is a hypervisor, which acts as an additional layer of software on the physical server. The security concern of the hypervisor is that it represents an additional attack surface in that an attacker penetrating the physical host can potentially access all the virtual systems hosted on the physical server. It is critical to ensure that virtual hosts are hardened and that VMs are updated individually, as updating the host system does not automatically update the VMs. Organizations should maintain backups of their virtual assets using built-in tools to create full backups and periodic snapshots.

5.8.2 Virtual Circuits

A virtual circuit, also known as a communication path, is a logical pathway or circuit created over a packet-switched network between two specific network endpoints. There are two types of virtual circuits:

- **Permanent virtual circuits (PVC)**—A PVC functions like a dedicated leased line. It always exists and is available for the user to.send data. The IS auditor should monitor the operations of the PVC to ensure that it is always available, closed down when not in use, and instantly reopened whenever required.
- **Switched virtual circuit (SVC)**—An SVC is created on demand using the best paths available at the time and disassembled after the transmission is complete. An SVC is more secure than the PVC as it reduces the length of the exposure of the circuit. It also requires less monitoring when compared to a PVC.

5.8.3 Virtual Local Area Network

A VLAN is used for hardware-imposed network segmentation that logically segments a network without changing its physical topology. It is created by switches. All ports on a switch are part of VLAN by default, which makes it possible to group various ports into distinct segments on the same physical network. There are two types of VLANs:

- **Static VLAN**—This is sometimes referred to as port-based VLAN. With this type of VLAN, switch ports are assigned to the VLAN in a way that is transparent to the user.
- **Dynamic VLAN**—In a dynamic VLAN, a user negotiates VLAN characteristics with the switch. The IP or hardware address can also be used to determine the VLAN.

VLAN characteristics that are of security interest to the IS auditor include:

- Communication between ports within the same VLAN occurs without hindrance.
- Communication between VLANs can be denied or enabled using a routing function.
- Routing can be provided by an external router or by the internal software of the switch.
- VLANs can be used to:
  - Control traffic for security or performance reasons:
  - Control and restrict broadcast traffic
  - Block broadcasts between subnets and VLANs
  - Isolate traffic between network segments
  - Reduce a network's vulnerability to sniffers
  - Protect against broadcast storms (floods of unwanted broadcast network traffic)

While VLANs work in similar fashion as subnets, the IS auditor should remember that they are not subnets.

 ©ISACA. All Rights Reserved.

VLAN are created by switches while subnets are created by IP address and subnet mask assignments.

5.8.4 Virtual Storage Area Networks

A virtual storage area network (VSAN) is a logical partition used to create and manage storage for VMs. It is intended for use in scenarios that leverage virtualized infrastructure and cloud computing and enables isolation of network traffic within certain portions of a SAN. This means that when a problem occurs in one logical partition, it can be addressed with minimum disruption of the entire network. Isolated VSANs also simplify the configuration and scaling out of the physical storage system. A VSAN provides greater visibility by combining several physical servers into a single shared storage medium. A VSAN dynamically allocates available storage for a VM as per requirements using a distributed architecture model. A VSAN is suited for cloud computing environments, virtual desktop infrastructure (VDI) environments, backup and archiving, and data center/disaster recovery processes.

Benefits of VSAN

Benefits organizations can get from implementing VSAN technology include:

- **Cost-effectiveness**—The implementation of a VSAN does not require any physical storage arrays, leading to a significant reduction in costs.
- **Scalability**—A VSAN can be scaled to meet the growing storage requirements of the organization. This is the major reason it is a preferred solution for cloud and virtualized systems that demand rapid and efficient scalability.
- **Performance**—A VSAN improves performance by making use of high-speed network interconnections that are found in virtualized environments. It can deliver fast and dependable storage performance and enable an organization to migrate on-premises data to cloud and virtualized environments without incurring significant downtime.
- **Flexibility**—A VSAN supports both block and file storage allowing organizations to choose the options best suited to their requirements. It is also easier to relocate data that is frequently accessed to high performance data storage systems while moving rarely used data to low-performance storage.
- **Security**—A VSAN is a highly secure solution that incorporates technologies such as data replication and snapshots to prevent data leakage while guaranteeing availability of information. Availability is one of the core components of the CIA triad. A VSAN allows an organization to concentrate on the remaining two components of security: confidentiality and integrity.
- **Simplicity**—One of the major advantages of a VSAN is that it is simple to provision as it is directly embedded within the hypervisor. Its installation and configuration can be carried out rapidly and efficiently. It is also easy to manage, as it can be integrated with other virtualized technologies on a single management plane.

SAN and VSAN Compared

The IS auditor should be able to distinguish between SAN and VSAN technologies and be in a position to advise on the appropriate implementation for the organization. **Figure 5.41** shows the differences between these two technologies.

Figure 5.41—Differences Between SAN and VSAN

Parameter	Storage Area Network (SAN)	Virtual Storage Area Network (VSAN)
Purpose	Provides dedicated block-level access to storage devices	Aggregates physical storage resources of hosts in a cluster and offers a single, shared data storage facility
Infrastructure	Requires dedicated physical storage hardware like disk arrays and switches for implementation	Leverages the host's physical resources
Scalability	Difficult to achieve and often requires additional physical resources	Dynamically allocates more storage resources when needed
Cost	Can be costly; requires specialized and dedicated hardware and a separate network	Less costly; uses existing infrastructure so no specialized hardware is required and does not require a separate storage network

©ISACA. All Rights Reserved.

Figure 5.41—Differences Between SAN and VSAN (cont.)

Parameter	Storage Area Network (SAN)	Virtual Storage Area Network (VSAN)
Performance	Requires specialized hardware such as high-speed switches to optimize performance	Uses caching, data mirroring and data distribution to optimize performance and no specialized hardware is required

5.8.5 Software-Defined Networking

SDN is a network virtualization approach based on the reasoning that traditional networks with on-device configuration are often subject to vendor lock-in, which limits network flexibility. Traditional networks rely on physical infrastructure such as switches and routers to make connections and run properly, while SDNs allow the user to control the allocation of resources at a virtual network level through the control plane. The user interacts with the software to provision new devices. An SDN also has more ability than a traditional switch to communicate with hardware devices throughout the network.

A software-defined wide area network (SD-WAN) is a solution that allows organizations to link numerous distributed locations using broadband and multiprotocol label switching. The main difference between SDNs and SD-WANs is that SDNs are designed to operate on LANs whereas SD-WANs are designed to sustain WANs over a large geographical area. The advantage of SD-WANs is that they eliminate the need to maintain lots of network hardware. Another particularly important distinction between the two is that SDNs are configured entirely by the user or administrator. SD-WAN services are managed by vendors, making deployment simpler. SDN networking protocols can be divided into three planes of functionality:

- **Data plane**—The data plane consists of the forwarding of actual user data through applications like TCP/IP to their final destinations.
- **Control plane**—The network control plane dictates which path flows apply before they reach the data plane. This is done using a flow protocol. This segment is where an administrator interacts with an SDN and manages the network. It consists of routing protocols that find the path to send data.
- **Management plane**—This plane is generally to provide performance and fault management as well as manage configuration of devices remotely connected to an SDN. Protocols such as SNMP help in configuration and monitoring of network elements.

The Advantages of SDN

The overall advantage of an SDN is that it can control the network reconfiguration of an organization by simplifying network management processes. Additional benefits include:

- **Provides centralized control**—An SDN virtualizes both the data and network control planes allowing the user to provision physical and virtual elements from a single location. It eliminates the challenge of monitoring distributed systems that are associated with traditional infrastructure. Through an SDN centralized control architecture an organization has a holistic view of its systems.
- **Abstracts the network**—Services and applications running on SDN technology abstract the underlying technologies and hardware that provide physical connectivity from those providing network control. The separation of the infrastructure layer from the control layer eliminates traditional networking concepts like IP addressing, subnets and routing, thereby simplifying network management.
- **Facilitates scalability**—The benefit of centralized provisioning is that an SDN provides more scalability. An SDN allows an organization to provision resources as changes occur in the network infrastructure. The positive effect of scalability in an SDN is noticeable when compared with traditional network setups in which resources are configured manually.
- **Enhances security**—An SDN controller provides a centralized location for the administrator to control the security of the entire network. While this comes at the cost of making the SDN controller a target, it provides users with a clear perspective of the infrastructure for effective security management of the entire network.
- **Lower operating costs**—An SDN helps an organization reduce its operating costs. With an SDN regular network administration-related tasks and issues can be automated, and older hardware can be optimized and repurposed. Resources are easily shared, unlike in a traditional network where hardware is confined to a single purpose.

 ©ISACA. All Rights Reserved.

- **Promotes network programmability**—An SDN enables network behavior to be controlled by software that resides away from the networking devices that provide physical connectivity. De-coupling the hardware from the software enhances innovative development activities by moving them away from the restrictions of closed platforms.
- **Enhances openness**—An SDN provides open architectures that enable multi-vendor interoperability and foster a vendor-neutral ecosystem. The open APIs support a wide range of applications while intelligent software can control hardware from multiple vendors with open programmatic interfaces like OpenFlow. Intelligent network services and applications can also run within a common software environment.
- **Supports API security**—SDN technology can provide network operators with API platforms to write programs. Applications interact with the network through APIs, instead of via management interfaces that are tightly coupled to the hardware. This enables the development of secure applications.

The Disadvantages of SDN

Organizations should be aware of some potential disadvantages with an SDN, including:

- **Latency**—A major problem that arises from virtualizing infrastructure is latency. The speed of the interaction with an appliance is dependent on the number of virtualized resources available, while service depends on how the hypervisor divides up the usage available. Each active device on a network takes its toll on network availability.
- **Limited management**—In virtualization environments an organization can manage the services of devices throughout the network, but it is impossible to manage the devices themselves. This affects the upscaling of the network, as all the devices need to be monitored, patched and upgraded regularly, leaving maintenance requirements unaddressed.
- **Network management complexity**—While traditional networks have limitations, there are standards for responding to security threats and developing procedures. An SDN has neither standards nor consensus, with numerous SDN solution providers operating independently. This results in complexities and creates challenges in terms of network management necessitating the hiring of skilled network personnel.
- **Dependency on the controller**—The centralized controller is one of the critical components of an SDN. If the controller fails, the entire network can go down, which affects the security aspect of availability. The organization should therefore ensure that the controller is always up and running and that a robust backup and disaster recovery plan is in place.

SDN Attacks and Vulnerabilities

It is critical for an IS auditor to be able to provide assurance on the detection and mitigatory controls in place to address attacks and vulnerabilities. Some of the attacks and vulnerability prevalent in SDN environments are shown in **figure 5.42**.

Figure 5.42—SDN Attacks and Vulnerabilities

Type of Attack/ Vulnerability	Description
Unauthorized access	A compromised controller/application can gain access to network elements and manipulate actions.
Data loss	Credentials can be stolen using compromised switches. This typically happens when switches are instantiated as part of a virtualization thrust in an organization.
Data modification	Man-in-the-middle attacks between the controller and data plane are possible in a software-defined network (SDN) if Transport Layer Security (TLS) is not mandatory. This provides room for the modification of data.
Denial of service (DoS)	This typically targets the SDN controller. It involves attackers sending bogus calls to the controller switch, which results in a packet flood, thereby denying legitimate service.
Malicious/compromised applications	The integration of third-party applications with the controller may lead to malicious/ compromised applications capable of taking control of the network.

©ISACA. All Rights Reserved.

Figure 5.42—SDN Attacks and Vulnerabilities (cont.)

Type of Attack/ Vulnerability	Description
Misconfiguration	SDN allows the installation of third-party applications on various network elements, often leading to inconsistencies and creating vulnerabilities.

SDN Deployment Best Practices

While SDN provides several advantages, its deployment is generally complex. Best practices for SDN include:

- **Perform careful deprovisioning processes**—One of the most significant benefits provided by an SDN solution is the ability to deploy new resources quickly. However, this capability needs to be closely managed to maintain performance by regularly de-provisioning resources when they are not in use or needed. Leaving resources active when not required consumes valuable virtual network resources that would be better used elsewhere in the organizational network.
- **Regularly perform network monitoring**—The SDN requires regular network monitoring to pinpoint any security loopholes affecting the mitigatory controls in the network and devices. To effectively monitor an SDN, the organization requires APIs for integration with the SDN, and this process is usually complex to undertake.
- **Consider onboarding security risk**—When onboarding an SDN, the organization needs to consider new security risk as new vulnerabilities that can be targeted by malicious actors. The organization should always be ahead in terms of current security threats and how to address them. The IS auditor should understand that an SDN is a form of virtualization and not a security solution itself.
- **Combine an SDN with other security technologies**—One benefit of an SDN is that it can be combined with other security technologies, such as a VPN, to simplify a large and complex network and make it easier for IS security professionals to visualize and manage. The result is a layered defense architecture with various security layers residing on the same underlying network.
- **Maintain quality of service (QoS)**—The SDN network and associated infrastructure should be monitored regularly to ensure that the QoS is always maintained. IS security professionals and IS auditors should ensure that the default settings on the SDN network are removed to enhance security and quality of network performance.

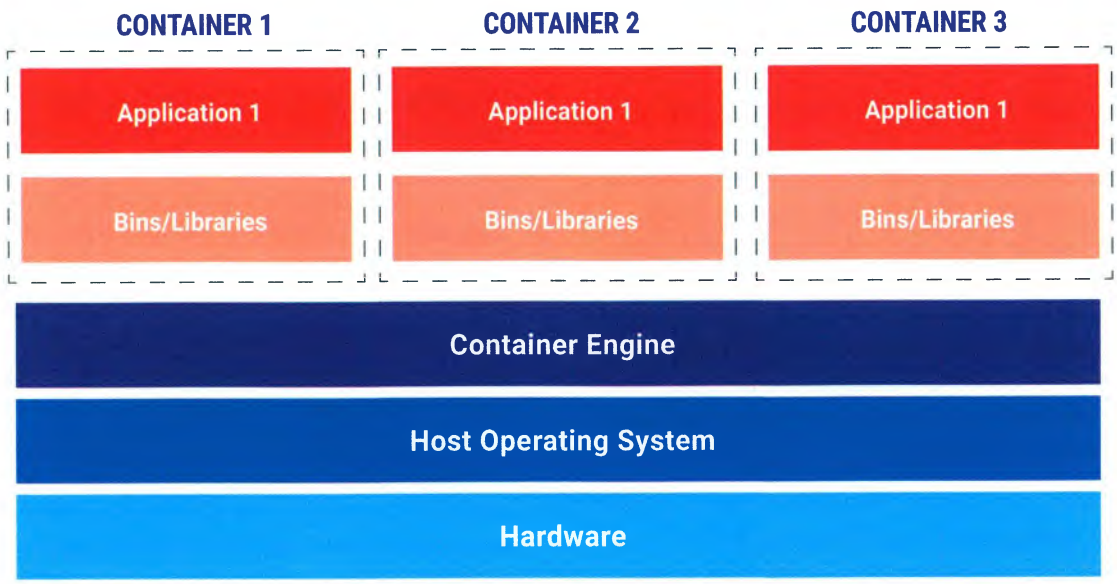
5.8.6 Containerization

Containerization is a form of virtualization that runs a single OS instance with multiple user spaces to isolate processes from each other. It involves packaging of an application with the configuration files, libraries and dependencies required across different computing environments. The technology is generally considered a lightweight alternative to full virtualization and involves encapsulating an application in a container within its own operating environment. Instead of installing an OS for each VM, containers employ the host OS. Each container is treated as an executable package of software that runs on top of a host OS with each host able to support many containers concurrently (**figure 5.43**).

The most common tools used in containerization are Docker and Kubernetes. Docker is basically a suite of software development tools for building, sharing, running and orchestrating individual containers, while Kubernetes is a platform for running and managing containerized applications at scale. These tools operate in a complementary manner in the entire containerization process.

 ©ISACA. All Rights Reserved.

Figure 5.43—Diagram of Containerization



Some of the benefits of containers are:

- **Faster deployment**—Containers are lightweight and faster to deploy. In the traditional systems environment, the larger an application, the longer the deployment period. Containerization solves this challenge by dividing and compartmentalizing applications into smaller parts.
- **Platform-agnostic**—Containers are platform-agnostic and can be deployed and/or redeployed in any platform or environment. This means that containerization can be implemented in any IS ecosystem.
- **Improved security**—The isolation aspects that are introduced by containerization provide an additional layer of security. If one container is compromised, other containers residing on the same host will remain secure.
- **Promotes flexibility**—Containerization provides the developers with the flexibility to operate in both virtualized and non-virtualized environments. This is critical in an organization when resources unexpectedly change without any prior indications.
- **Enhance operational efficiency**—Containerization can improve efficiency by using all the available resources and minimizing associated overheads. Isolated containers can perform their own operations without interfering with other containers. This configuration allows a single host to perform a variety of functions.
- **Cost reductions**—The lightweight nature of containers results in significant cost reductions for the organization. Containerization reduces the number of physical machines required and the skills needed to operate the technology.
- **Provides scalability**—Containerization provides high scalability and can handle increasing workloads by reconfiguring existing architectures. More containers can be added with ease within a defined cluster. In addition, new functions, updates and features can be added without interfering with the original application.
- **Enhances portability**—Containerization creates executable software packages that are abstracted from the host OS. No container is tied to the host OS; thus, it can be run consistently and uniformly across any platform or in the cloud. This enhances application portability.

The limitations of containerization include the following:

- Containerization is well-supported on Linux-based systems but not on Windows.
- If vulnerabilities are present in the container kernel, it makes all containers vulnerable to attacks.
- Networking is difficult with each container running on a single server. The container architecture requires a network bridge for mapping container network interfaces to host interfaces.
- Monitoring can sometimes be challenging. In fact, monitoring several containers containing individual processes can prove more difficult than monitoring multiple processes on a single VM instance.
- Containerization requires effective management by employees who have the required expertise. If

©ISACA. All Rights Reserved.

containerization is not properly monitored and managed, it can result in lower performance overall.

Best Practices for Container Security

The process of securing containers is continuous. It should be integrated into the development process and ideally automated. Container security involves the implementation and maintenance of security controls that protect containers and underlying infrastructures. Integrating security into the development pipeline can help ensure that all components are secured, starting with the initial development phase and continuing through the end of their life cycle. When securing containers, the main concerns include security of the host, network traffic and applications within the container as well as the container management stack.

Some of the best practices for container security include:

- **Systems hardening**—A good starting point to determine security controls and guidance is to use the vendor-provided security benchmark or hardening guidelines.
- **Monitoring**—Monitoring containers is difficult and specific tools to support the detection of malicious activity within the container (like host-based firewalls, antimalware, antivirus, etc.) are not readily available. Having knowledge of what each container includes, down to the libraries, is key in understanding what the threats and vulnerabilities are.
- **Continuous auditing**—Continuous auditing is always recommended, and logs are key to determining gaps in security, especially when an organization is rebuilding instances repeatedly and may not notice an issue until after an instance is rebuilt.
- **Vulnerability assessments**—Vulnerability scanners offer some container security scanning to help identify known vulnerabilities and configuration issues.
- **Patching**—Patching is different in a containerized environment. With containers, there are two components: the base and the application image. It is critical to update the base image and then rebuild the application image, thereby enforcing a more complex patching process and more interaction between infrastructure support and development.
- **Isolation**—Migrating to containers lessens the isolation that was once available with VM and/or bare metal systems since containers share the same kernel. One approach some organizations are using is to run containers from an operating system on a VM.
- **Incident response**—Migrating to containers greatly limits an organization's ability to perform forensics since the instance or host could have been replaced already. Reviewing all incident management and response processes specifically for containers is required.
- **Securing the container management stack**—It is advisable to implement a strong access control strategy throughout the pipeline, starting with code repositories and branching strategy and extending to the container repository. POLP should also be implemented and access rights audited regularly.
- **Securing images**—Container images are used to create containers. A misconfiguration or malicious activity in container images can introduce vulnerabilities into containers deployed in production. A container image holds a subset of the OS along with the application designed to run in the container.

Figure 5.44 compares virtualization and containerization.

Figure 5.44—Comparison of Virtualization and Containerization

	Virtualization	Containerization
Isolation	Enables full isolation from the host operating system and other virtual machine (VM) instances	Enables lightweight isolation from the host and other containers. This means that all containers will be at risk if an attacker compromises the host.
Operating system	Runs more than one complete operating system	Runs all containers through the user mode of the operating system
Guest support	Runs a wide range of operating systems (OSs) inside the VM	Runs on the same operating system as the host. For example, Linux containers cannot be run on Windows.

 ©ISACA. All Rights Reserved.

Figure 5.44—Comparison of Virtualization and Containerization (cont.)

	Virtualization	Containerization
Deployment	Deploys VMs individually using the hypervisor software; each VM has its own hypervisor.	Deploys individual and multiple containers
Storage	Uses virtual hard disk (VHD) for each VM and server message block (SMB) for multiple servers	Uses local disks for local storage per node and SMB for multiple nodes
Load balancing	Runs VMs in other clusters in failover cluster	Is managed automatically by the orchestrator, such as Kubernetes
Networking	Uses virtual network adapters for networking	Uses multiple isolated views of virtual network adapters

5.8.7 Secure Cloud Migration

Cloud adoption continues to increase as cloud technology transforms the conduct of business in the current digital world. While there are many considerations with the adoption of cloud technologies, the IS auditor should be most concerned about the security implications. Cloud migration refers to the process of transferring an organization's data and applications from its on-premises servers to a cloud infrastructure. It typically takes three major forms:

1. On-premises to the cloud
2. Cloud-to-cloud migration
3. Reverse cloud migration

Cloud Migration Security Risk

The process of cloud migration leaves data vulnerable to attacks and requires careful planning by management. Risk factors associated with cloud migration include:

- **Multi-tenancy**—Multi-tenancy is a situation in which cloud users share cloud resources with other users through common software virtualization layers. The challenge of multi-tenancy is that tenants are usually unaware of other tenants' identities. The migration by one tenant may bring inconsistencies and challenges in terms of resource provision to the other tenants.
- **API vulnerabilities**—APIs act as communication channels between environments. APIs must be secured at all stages of the cloud migration process. Clients of CSPs often employ APIs to set up software-server interactions, but they might not be reliable enough and could significantly boost the risk of unauthorized network penetration and in-house data theft.
- **Compliance risk**—Compliance requirements, such as data protection and privacy regulations, are a major risk in cloud migration. Regulations typically require that data governance frameworks address data ownership, responses to breaches, and coordination activities required to meet regulatory requirements. Moving to the cloud may increase an organization's compliance risk. It is critical to ensure that the target cloud environment supports the organization in meeting compliance requirements.
- **Uncontrolled growth**—Cloud migration is not a one-time process. After migrating applications to the cloud, the organization typically adds more resources, consumes new cloud services and adds more applications. It is very common to start using additional SaaS applications once they are running in the cloud. These new services and applications must be properly secured, creating a major operational challenge.
- **Data loss**—During the migration process there is a possibility of data being lost, incomplete or corrupt due to various factors that include technical issues, power outages and human error. To address this risk, the organization should back up data on a disk and ensure that the CSP has data backup, restoration and failover facilities. It is also a good idea to have backup with more than one cloud.
- **Data security**—Data security is a major risk during the migration process. Migrating to the cloud involves security risk such as insecure APIs, accidental errors, malware and external attacks while the data is in transit. Encryption for data at rest, in process and in transit is essential to reduce security risk during the data migration process. Configuration of firewalls and the isolation of individual workloads can also be implemented to minimize security risk.
- **Incompatibility of existing architecture**—Cloud migration is risky for organizations that depend on legacy infrastructure. Legacy infrastructure often relies on programming languages, execution environments and system libraries that may not be readily supported in the cloud. Because of this, a migration may fail, forcing an organization to

©ISACA. All Rights Reserved.

purchase new compatible infrastructure to reduce the risk.

- **Reduced visibility—Reduced** visibility is a major risk of cloud migration that can affect security. When the organization migrates to external cloud services, responsibilities automatically transfer to the CSP leading to reduced visibility for the organization. Continuous monitoring during the migration process greatly helps in mitigating this risk.
- **Data remanence**—It may be necessary for an organization to migrate valuable data to the cloud and destroy useless data during the migration process. Sometimes the data removal tools used by the organization may not permanently remove data, leading to data remanence. A typical example is deletion, which just changes pointers on storage media but does not permanently remove data. Organizations should invest in effective data removal technologies to reduce this risk.
- **Talent gap**—This often arises both at the CSP and the organization. Both may lack skilled cloud security personnel to support the migration process, or the skills may only be resident on either side. This may lead to errors in handling the migration process. It is therefore critical for an organization to develop its own personnel in cloud security and choose a CSP with strong skills to mitigate the risk.

Some of the steps an organization can take to ensure that a cloud migration process is secure are:

- **Develop a plan for secure migration**—A proper plan helps an organization to determine the applications and data to be migrated, the migration strategy, personnel involved in the migration and how to reduce migration risk. From this plan, an organization can derive its cloud migration strategy for implementation.
- **Assess current security measures on on-site premises**—This assessment will help an organization avoid or reduce data leakage during the migration process.
- **Establish security standards and map the security requirements**—The security risk in the cloud are more pervasive than in traditional on-premises sites. If an attack occurs in the cloud the security holes may remain open. Organizations should establish security standards and map out security requirements. Monitoring should be undertaken to assess compliance with standards for each application in the migration process.
- **Train employees on cloud security**—Training should be prioritized when introducing a new technology, such as the cloud, so that employees are well prepared for the disruptions involved. All employees who are targeted to use cloud services should be aware of the security risk involved in the migration process.
- **Secure the DevSecOps pipeline code**—Attackers typically attempt to exploit vulnerabilities in cloud applications throughout the development and distribution pipeline as developers often maintain security identifiers as source code stored on shared storage or public repositories. Organizations should secure source code by removing secrets and automatically monitor and control access to source code.
- **Evaluate regulatory requirements**—When migrating to the cloud it is critical to meet regulatory requirements. Organizations should identify the regulations to be met and devise a plan for complying with them to avoid costly penalties associated with noncompliance.
- **Assess infrastructure**—This assessment will reveal whether the infrastructure an organization migrates to meets information security standards. It also determines whether the data centers are secure. Checking on the certification of the data centers against international standards is also key in making the migration process secure.
- **Encrypt data with secure protocols**—It is very important to ensure that all organizational data subject to transfer to the cloud is encrypted with secure protocols such as HTTPS and TLS. Encryption should be in place for both data at rest and in transit for maximum security.
- **Ensure clear, efficient and effective communication**—Communication plays a critical role in the migration process. All parties involved in the migration process should receive adequate and clear communication, especially pertaining to what is expected of them.
- **Enable strict access control**—Cloud migration security should include strict access control features so that the connectivity between on-premises systems and the cloud is secure. Also, access to data prior, during and after migration should be tightly controlled to reduce risk from malicious attackers. Security administrators should have visibility of all data as it travels from on-premises systems to the cloud.
- **Automate the migration process**—The migration process should be automated to avoid misconfigurations so that the cloud migration strategy is viable. AI and ML capabilities can be incorporated in the migration process to enable continuous and

dynamic analysis of activities for the purpose of identifying malicious behavior during the migration process.

- **Data backup**—It is a best practice in cloud migration for organizations to create file backups. This means that in the event of data loss, the data can be easily restored. An organization can even have backups stored with multiple cloud providers to spread the risk.
- **Implement a cloud security posture management (CSPM) solution**—CSPM performs monitoring activities for cloud misconfigurations during various stages of the migration process. The advantage of CSPM solutions is that they can immediately remediate the identified misconfiguration issues.

5.8.8 The Shared Responsibility Model

The shared responsibility model (SRM) is a security and compliance framework that outlines the responsibilities of CSPs in cloud security. Practically, the respective responsibilities meet somewhere in the middle with each party expected to adopt certain security controls depending on the type of cloud service provisioned. The cloud SP ordinarily manages, operates and controls infrastructure operations, from the virtualization layer to hardware device security, including storage and computing systems, networking systems, databases and physical data centers. The cloud customer, on the other hand, is typically responsible for managing the security of data and the guest operating system, including IAM controls, OS configuration, encryption of data, security policies and firewalls. Some security functions may be shared, including security training and awareness, patch management and configuration management. These security responsibilities vary among cloud service types.

The IS auditor should be aware that the customer, which is the organization, cannot transfer the risk of data security and security governance, risk and compliance (GRC) in the cloud. The CSP always assumes responsibility for the physical security of the cloud. The shared responsibilities vary across the cloud types. While the SRM is complex and requires careful consideration and coordination between the CSP and customer, the approach offers several important benefits to users. These include:

- **Efficiency**—Though the customer bears significant levels of responsibility under the SRM, major aspects of security—such as security of hardware, infrastructure and the virtualization layer—are almost always managed by the CSP. In a traditional on-premises model, these aspects are managed by the customer, who bears all the risk.
- **Reduces IT staff costs**—The shift to the cloud and the adoption of the SRM frees IT to concentrate on other tasks. It also reduces the staff complement and allows the organization to reduce the labor budget and dedicate available resources and investments to other areas of business.
- **Enhanced protection**—Many CSPs give high priority to the security of their cloud environment because that is their business. They do not hesitate to dedicate significant resources to ensure their customers are fully protected. As part of the service agreement, CSPs also conduct regular monitoring, patching and testing, which the organization may not be able to perform.
- **Expertise**—CSPs often have a higher level of knowledge and expertise than the organization when it comes to the emerging field of cloud security. The organization can benefit from this expertise by adopting the SRM.

Cloud Deployment Models

There are many things to take into consideration when selecting a cloud deployment model that is right for the organization, and IS auditors need to properly advise management in that regard. **Figure 5.45** provides brief explanations on the security aspects of the major cloud deployment models.

©ISACA. All Rights Reserved.

Figure 5.45—Comparison of Cloud Deployment Models

Cloud Deployment	Security Dimensions
Public cloud	The cloud service provider (CSP) owns and operates data centers and is responsible for the security of the cloud, while the customer is responsible for security in the cloud (i.e., the applications they deploy and configuration of services they leverage). Customers are not adequately protected from information security attacks as the cloud is accessible to everyone.
Private cloud	The CSP has a lesser role regarding security in the private cloud. Private clouds consist of dedicated infrastructure, so customer organizations have more visibility and control over physical security and data storage. Resources can be segmented in a private cloud, an approach that leads to increased security and improved access. The private cloud deployment model is suitable for organizations that deal with highly private data, such as healthcare and finance.
Hybrid cloud	In a hybrid deployment model, the CSP has a lesser role in cloud security. Customers have increased control over their data, which allows them to choose different security environments for each use case. Customer data is typically segmented to lessen the chances of attack; hence, the hybrid model is generally considered secure.
Community cloud	A community cloud is managed and controlled by member organizations. The CSP has less visibility and control over security in a community cloud. Community members are generally responsible for the security of their applications as a collective. Data security is high, as the model is more like a private cloud.
Multi-cloud	The multi-cloud deployment model is similar to the hybrid model. However, while a hybrid approach combines both private and private clouds, a multi-cloud model combines public clouds. Due to its complexity, the multi-cloud approach may have loopholes that can be targets for attackers. The attack surface is also increased, thus raising the risk exposure. This makes the model insecure from the customer's perspective.

Cloud Service Models

There are three basic cloud delivery models (**figure 5.46**), each offering a distinct computing service to the enterprise that uses it:

1. **Software as a service (SaaS)**—Provides a business application that is used by many individuals or enterprises concurrently
2. **Platform as a service (PaaS)**—Provides an application development sandbox in the cloud
3. **Infrastructure as a service (IaaS)**—Provides online processing or data storage capacity

Figure 5.46—Cloud Delivery Models

Service Model	Description	Considerations
IaaS	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include OSs and applications. IaaS puts these IT operations into the hands of a third party.	IaaS can provide infrastructure services such as servers, disk space, network devices and memory and is designed for users wanting complete freedom with regard to the OS and applications they use.

 ©ISACA. All Rights Reserved.

Figure 5.46—Cloud Delivery Models (cont.)

Service Model	Description	Considerations
PaaS	Capability to deploy onto the cloud infrastructure customer-created or customer-acquired applications developed using programming languages and tools supported by the provider.	PaaS provides an application development sandbox and is specifically designed for developers.
SaaS	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).	SaaS provides applications that are complete and available on demand to the end customer. Traditional licensing and asset management are changed.

Source: ISACA, *Controls and Assurance in the Cloud: Using Cobit 5*, USA, 2014

SRM Best Practices

It is best to follow standard practices when it comes to cloud security responsibility. As organizations shift to the cloud, many are defining their relationships with CSPs for the first time. When navigating this complex territory, it is advisable for companies to adopt these best practices:

- **Carefully review the SLA**—Security responsibilities will differ depending on the cloud model, cloud provider and other variables. It is critical for organizations to carefully review their SLAs with their cloud vendors to ensure they are fully aware of their security responsibilities and to identify any potential gray areas that need further clarification.
- **Prioritize data security**—Cloud customers are always fully responsible for any data stored in the cloud or produced by applications in the cloud. Organizations must develop a robust data security strategy specifically designed to protect cloud-based data, whether it is in use, at rest or in motion.
- **Ensure robust IAM**—The cloud customer is completely responsible for defining access rights to cloud-based resources and granting access to authorized users. These efforts should be incorporated into the organization's broader IAM policy and solution set.
- **Identify a trusted cybersecurity partner**—Updating and adapting a cybersecurity strategy and toolset to address new cloud-based risk can be both overwhelming and complicated. A cybersecurity partner can assist an organization's internal security team in managing all aspects of cloud security, from selecting a CSP, to understanding their specific security responsibilities, to deploying and integrating the tools and solutions that will protect the business.
- **Embrace DevSecOps**—DevSecOps is the practice of integrating security continuously throughout the software and/or application development life cycle in order to minimize vulnerabilities and improve compliance without impacting speed of release cycles. It is useful for any IT organization that is leveraging containers or the cloud, both of which require new security guidelines, policies, practices and tools.

5.8.9 Key Risk in Cloud Environments

According to the Cloud Security Alliance (CSA),[43] the most common cloud security threats are:

- **Insufficient identity, credentials, access and key management**—Identity management is mostly targeted in cloud environments because identity is the main method of accessing cloud resources. Insufficient credentials are therefore a serious threat to cloud computing.
- **Insecure interfaces and APIs**—Everything in the cloud is virtual, and each application has to communicate with other applications to function. This is typically enabled through APIs and other interfaces. The risk is that these interfaces and APIs may not be secure.
- **Misconfiguration and inadequate change control**—CSPs typically provision resources in the cloud in a matter of minutes. Any misconfiguration errors are generally pervasive in the operating environment.
- **Lack of cloud security architecture and strategy**—Organizations often lack clear strategies for

[43] Cloud Security Alliance, *Top Threats to Cloud Computing: Pandemic Eleven*, 6 June 2022, *https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/*

©ISACA. All Rights Reserved.

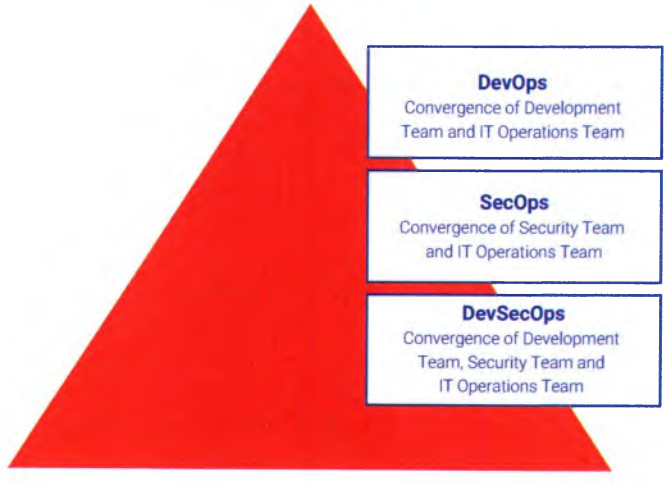
the deployment of cloud infrastructure. Key areas of concern include the SRM, POLP and the establishment of isolation zones.

- **Insecure software development**—Critical endpoints like laptops and tablets developers use for their work should be properly protected. This limits points of entry for viruses and similar attacks, as the developers typically download code from repositories such as GitHub.
- **Unsecured third-party resources**—Virtually all cloud products contain elements of third parties. Supply chain vulnerabilities are therefore a major challenge, as attackers exploit weaknesses in the supply chain.
- **System vulnerabilities**—System vulnerabilities are constantly evolving, so continuous vulnerability scanning is essential. Organizations should know the topical vulnerabilities at any given time and undertake periodic security audits.
- **Accidental cloud data disclosure**—Data disclosure often results from employees sharing hyperlinks on emails that can then be shared with recipients outside the organization. This is a major risk but can be mitigated through DLP solutions.
- **Misconfiguration and exploitation of serverless and container workloads**—Containers form part of cloud-native devices with no OSs. They run on top of server hardware just like VMs. These are often misconfigured, leading to security holes that can be exploited by attackers.
- **Organized crime, hackers and APTs**—While organizations have no control over hackers, cybercriminals and APTs, they can limit damage by hardening their cloud configurations and monitoring their security postures.
- **Cloud storage data exfiltration**—Data exfiltration presents huge challenges to data owners and information security professionals. Organizations should proactively ensure that cloud data is secure. Any attacks to cloud data centers should be detected and/or prevented promptly and in real time.

5.8.10 DevSecOps

DevSecOps is basically the convergence of development, security and operations. It is an organizational discipline and arrangement that aims to integrate security from the beginning of the software development life cycle (SDLC) to the end. Previously, security was added to applications later in the life cycle, after development was complete. Agile development practices and advances in cloud platforms, microservices and containers make that impractical, because security cannot keep up with rapid releases. DevSecOps solves this problem by integrating security with DevOps. Security becomes an integral, automated part of continuous integration (CI) and continuous delivery (CD) pipelines, and it is viewed as a responsibility shared by all teams. Developers become aware of security practices and implement them from the onset of a development project. **Figure 5.47** shows the placement of DevSecOps in an organization.

Figure 5.47—DevSecOps Architecture



 ©ISACA. All Rights Reserved.

DevSecOps Benefits

Benefits associated with DevSecOps:

- **Enhances fast, cost-effective and secure software delivery**—DevSecOps enables fast, secure software delivery by eliminating repeated processes at the end of the delivery cycle. It lowers the chances of information security issues due to continuous monitoring and testing of processes. Less staff are required, leading to an overall reduction in employment costs.
- **Addresses security issues proactively**—DevSecOps introduces security processes early in the SDLC and ensures that code passes continued reviews, audits, tests and scans throughout the development pipeline. Development teams can address security issues immediately when discovered, remediating problems before they spread. This approach makes security more effective and less expensive.
- **Encourages fast vulnerability remediation**—DevSecOps helps teams identify security vulnerabilities quickly and apply patches early in the development cycle, thereby reducing opportunities for attackers to exploit the vulnerabilities. It also integrates vulnerability detection and patching into the development cycle to prevent the release of vulnerable software.
- **Enhances automation-driven development**—DevSecOps teams can integrate security testing into automated test suites, enabling streamlined operations. Organizations can leverage CI/CD pipelines to automate development and security processes.
- **Simplifies compliance reporting**—Employing DevSecOps tools can simplify compliance auditing and reporting. The automation of data collection activities makes the compliance process easier and quicker. Automated intelligent scans are scheduled for applications to discover areas of noncompliance in an easy and reliable way.
- **Standardizes information security efforts**—In DevSecOps, security is integrated into every step of the application development process. This leads to uniform security across all stages of development of a software application, ensuring that all security vulnerabilities are addressed.

DevSecOps Best Practices

Best practices for effective DevSecOps implementation include:

- **Practice shifting security left**—Shifting left involves moving security from the end of the delivery process to the beginning. DevSecOps places security at the beginning (left) of the development life cycle, making the DevSecOps team responsible for ensuring security throughout the process.
- **Incorporate compliance security processes**—Information security requires knowledge of compliance, so every member of the team should work closely with the compliance function. This collaboration ensures that everyone in the organization understands its security policies and the security environment in which it operates. All employees should undergo periodic training to ensure they understand their responsibilities.
- **Invest in information security training**—All members of the organization involved in the software delivery process should be trained to understand basic application security principles, security testing processes and other best practices. It is important that they know how to identify security threats and be able to apply appropriate security controls.
- **Improve the workplace culture**—DevSecOps thrives in an environment that embraces change and values information security. Leadership should encourage collaborative attitudes toward good security practices and promote communication to support security efforts. This creates a workplace culture supportive of security initiatives.
- **Enhance observability and monitoring processes**—Effective maintenance of security is supported by continuous monitoring and observability solutions. Such solutions provide security insights and assist in monitoring risk in the development environment. The observability and monitoring processes in place should support visibility to ensure accountability. They should also support traceability, which is necessary to enforce controls, and auditability to enable compliance with requirements.

5.9 Mobile, Wireless and Internet of Things Devices

Portable and wireless devices present a ubiquitous threat to an enterprise's information assets and must be properly controlled. Policies and procedures and additional protection mechanisms must be put into place to ensure that data is protected to a greater extent on portable devices, because such devices will most likely operate in environments where physical controls are lacking or nonexistent. Mobile devices are easily lost or stolen and require the use of encryption technologies and strong authentication. It also may be necessary to classify some data as inappropriate for storage on a

©ISACA. All Rights Reserved.

mobile device. The IS auditor should understand that all such media and devices can also be used by an individual to steal data and programs for personal use or gain.

5.9.1 Mobile Computing

Mobile computing refers to devices that are transported or moved during normal use. Common mobile devices include tablets, smartphones, laptops, USB storage devices, digital cameras and similar technologies. Their mobility makes it more difficult to implement logical and physical access controls.

Figure 5.48 describes known vulnerabilities and associated threats related to mobile devices.

Figure 5.48—Mobile Device Vulnerabilities, Threats and Risk

Vulnerability	Threat	Risk
Information travels across wireless networks that are often less secure than wired networks.	Malicious outsiders can do harm to the enterprise.	Information interception resulting in a breach of sensitive data, enterprise reputation, adherence to regulation or legal action
Mobility provides users with the opportunity to leave enterprise boundaries and thereby eliminates many security controls.	Mobile devices cross boundaries and network perimeters, carrying malware that it can bring into the enterprise network.	Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data
Bluetooth technology is very convenient for many users to have hands-free conversations, but it is often left on and then is discoverable.	Hackers can discover the device and launch an attack.	Device corruption, lost data, call interception, possible exposure of sensitive information
Unencrypted information is stored on the device.	In the event that a malicious outsider intercepts data in transit or steals a device or if an employee loses the device, the data is readable and usable.	Exposure of sensitive data, resulting in damage to the enterprise, customers or employees
Lost data may affect employee productivity.	Mobile devices may be lost or stolen due to their portability. Data on mobile devices is not always backed up.	Workers dependent on mobile devices being unable to work due to broken, lost or stolen devices and data not backed up
The device has no authentication requirements applied.	In the event that the device is lost or stolen, outsiders can access the device and all of its data.	Data exposure, resulting in damage to the enterprise and liability and regulation issues
The enterprise is not managing the device.	If no mobile device strategy exists, employees may choose to bring in their own unsecured devices.	Data leakage, malware propagation or unknown data loss in the case of device loss or theft
The device allows for installation of unsigned third-party applications.	Applications may carry malware that propagates Trojans or viruses; the applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network.	Malware propagation, data leakage or intrusion on the enterprise network

Source: ISACA, *Securing Mobile Devices*, USA, 2012

5.9.2 Mobile Device Threats

Mobile devices are often preferred in organizations, as they increase mobility and allow for remote work along with increases in efficiency and productivity. However, these benefits are often accompanied by many security threats. The IS auditor should assess the threat landscape and be in a position to advise IT management

 ©ISACA. All Rights Reserved.

accordingly. The most common threats to mobile devices are:

- **Information interception**—Attackers can intercept information on mobile devices leading to unauthorized access to sensitive data. This can also lead to reputational damage as well as regulatory and compliance risk.
- **Malware propagation**—If mobile devices are not well-secured, they can allow malware to infect organizational systems and propagate along the organization's internal networks.
- **Lost business**—Employees who rely on mobile devices for business may be unable to work if their devices malfunction or are lost or stolen.
- **Data leakage**—When a mobile device is lost or stolen, any data not backed up is lost. To mitigate the risk of data leakage, the organization should ensure that data on mobile devices is backed up.
- **Open public Wi-Fi**—Open Wi-Fi technologies are usually less secure than closed networks. They typically do not require passwords or use encryption technologies. Hence, it is easier to spy on a device's online activities.
- **Outdated devices**—Mobile devices that are outdated may not receive security updates from device manufacturers. To mitigate this risk, all outdated mobile devices should be replaced.
- **Identity theft**—Attackers steal device user credentials and use them to open new phone accounts or add phone lines, among other criminal activities. This is done without the victims' knowledge and can lead to huge losses, as criminals may incur huge bills on their behalf.
- **Drive-by downloads**—Malware can be installed on mobile devices without users' knowledge or consent as a result of visiting suspicious websites or opening malicious email links. Some downloaded files may contain bots that perform malicious tasks on victims' mobile devices.

5.9.3 Mobile Device Controls

Controls are available to reduce the risk of disclosure of sensitive data stored on mobile devices. Many of these controls can be enforced by mobile device management (MDM) systems and/or secure containers:[44]

- **Device registration**—All mobile devices authorized for business use should be registered in a database. Devices that are personally owned should be flagged. Organizations can push updates or manage authorized devices and exclude personally owned mobile devices.
- **Physical security**—If a device is stationary and permits its use, a cable locking system or a locking system with a motion detector can sound an audible alarm. The organization should maintain physical control of mobile devices equipped with these controls and avoid connecting to unknown devices and removable media. Protected cases to cover these devices should be considered, and cameras should be covered when not in use.
- **Bluetooth**—It is advisable to disable Bluetooth functionality when it is not in use. (Note that airplane mode does not always disable Bluetooth.)
- **Wi-Fi**—Mobile device owners should not connect to public Wi-Fi networks, and Wi-Fi should be disconnected when not needed. All unused Wi-Fi networks should be deleted.
- **Software updates**—Device and software applications should be updated as soon as the updates become available.
- **Location**—Location services should be disabled when not needed. Organizations should restrict users from bringing mobile devices to sensitive locations.
- **Passwords**—Strong lock screen passwords should be used. Devices should be set to lock automatically after short, specified time intervals (e.g., after three minutes).
- **Applications**—Only a minimal number of applications should be installed on mobile devices and only from official application stores. Applications not in use should be closed.
- **Data storage**—Only content that is absolutely needed should be stored on the device. If data is not stored locally, then a lost or stolen device will not be an issue. The data that is stored should be backed up on a regular basis, preferably to shared folders on the enterprise's file server.
- **Virus detection and control**—The threat associated with viruses applies to all mobile devices. The enterprise should update the mobile device antivirus software to prevent perpetuation of malware.
- **Compliance**—Mobile devices should comply with the security requirements defined in enterprise standards. All mobile devices should require a password. MFA can be used to further enhance security.
- **Approval**—Mobile device use should be appropriately authorized and approved in accordance with organizational policies and procedures.

[44] National Security Agency, "Mobile Device Best Practices," *https://media.defense.gov/2021/Sep/16/2002855921/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF*

©ISACA. All Rights Reserved.

- **Acceptable use policy**—A security policy should exist for mobile devices. The enterprise should have a policy that addresses mobile device use and specifies the type of information and kind of devices and information services that may be accessible through the devices.
- **Due care**—Employees should exercise due care within office environments and especially during travel. Any loss or theft of a mobile device must be treated as a security breach and reported immediately in accordance with security management policies and procedures.
- **Awareness training**—Employee orientation and security awareness training should include coverage of mobile device policies and guidelines. The training will allow propagation of awareness that mobile devices are important business tools when used properly and have risk associated with them if not managed accordingly. Users should be educated not to communicate sensitive information on mobile devices, to avoid opening email attachments and links, and to use trusted accessories, among other awareness training topics.
- **Network authentication, authorization and accounting**—IT organizations should adopt a solution that allows them to tie devices connecting to the network with each user's identity and role, and then apply role-based policies to grant proper access privileges. This enables IT to differentiate access for different levels of employees, guests or device types. It also lets IT take a proactive stance on tracking and monitoring how mobile devices are used within the network.
- **Secure transmission**—Mobile devices should connect to the enterprise network via a secure connection, such as over a VPN.

5.9.4 Mobile Device Management

MDM is a collective suite of tools and technologies used to secure and manage mobile devices, applications, data and access. It solves the challenging task of managing the myriad mobile devices that employees use to access company resources. The objectives of MDM are to improve security, provide monitoring, enable remote management and support troubleshooting of mobile devices. MDM should be able to remove undesirable applications, manage data and enforce configuration settings across a carrier network and Wi-Fi connections. The basic features of MDM include:

- **Encryption**—See section 5.6 Data Encryption for more information.
- **Remote wiping**—A remote wipe feature of MDM deletes all data from the mobile device and can be carried out over the mobile phone service or the Internet. However, for the IS auditor it should be emphasized that a remote wipe does not guarantee data security by itself as it does not permanently remove data. Data may still be present, and attackers can use data recovery utilities to recover data on a wiped device.
- **Device lockout**—Lockout disables a device if a user fails to provide credentials after repeated attempts. An administrator needs to clear the lockout flag to allow use of the device again. More sophisticated lockout features of MDM cause a persistent lockout that requires the user to sign in with a different account or master password/code to regain access to the device.
- **Assets management**—Many mobile devices include a GPS chip to support navigation, which allows the organization to track its devices and personnel movements such as deliveries and geotagging. However, for GPS tracking to work, the mobile device must have Internet or wireless phone service to communicate its location information.
- **Application control**—Application control is an MDM solution that controls the installation of applications onto a device. It can also be used to enforce the settings of certain applications in order to support a security baseline or maintain other forms of compliance. Organizations can reduce exposure to malicious applications by limiting users' ability to install applications that originate from unknown sources or are not work-related.
- **Device troubleshooting**—An MDM solution can allow remote troubleshooting from the management console. Using this feature, an organization is able to discover mobile device problems and fix them remotely without any need to have the device hands-on.
- **Credential management**—Credential management is basically centralized storage of credentials. MDM solutions can be a means to securely store a wide range of credential sets. These typically employ a master credential set, preferably MFA, to unlock the dataset. Some MDM credential management options also provide auto-login options for apps and websites.
- **Secure remote**—Employees relying on personal devices to conduct work are often out of the office. Having a secure way to support and fix devices from a remote location is imperative to maintain employee satisfaction. Depending on device type, remote support solutions allow help desks to configure devices, chat, transfer files and remotely

 ©ISACA. All Rights Reserved.

see and control the device. It is important to select a solution that supports a wide variety of devices and keeps all access and activity logs behind the enterprise firewall to ensure security.
- **Standard mobile device applications**—Configuration and use of mobile devices should be baselined and controlled. Only applications that either meet with the enterprise security architecture or are delivered as standard on mobile devices should be authorized for use, and all software applications must be appropriately licensed and installed by the organization's IS support team. MDM solutions support this.

Best Practices for MDM

The best practices for MDM include:
- **Craft an implementation policy**—The organization should craft the MDM policy prior to the deployment of the MDM solution. The policy should address the unique technical and business needs of the organization. The major objectives of the MDM policy are to provide direction and to ensure the orderly, standardized deployment, operation and maintenance of MDM solutions in the organization.
- **Simplify device enrollment**—The enrollment of mobile devices to the MDM solution should not be so complicated that it discourages users or causes them to lose interest in enrolling their devices. The organization should ensure that the enrollment process is simple and that all devices are enrolled.
- **Establish self-service**—End-user self service capabilities are critical in encouraging users to maintain compliance with MDM solutions. Self-service capabilities include remote data wipe-out, password reset and lost device tracking.
- **Enforces updated MDM versions**—It is crucial to ensure that MDM features—such as push configuration changes, patches and software—are updated and available to users.
- **Protect end-user privacy**—User privacy is key in MDM implementation and encourages a culture of compliance. Organizations should respect and protect employee privacy by restricting data collection to a bare minimum and only for business purposes while putting in place procedures for eliminating the misuse of personal employee information.
- **Deploy containers**—Containers are important in mobile device security as they can separate organizational applications, data and MDM controls from the personal use of the mobile devices. When such containment is enabled, the MDM rules and features can be deployed in such a way that they only apply when a mobile device is used for organizational work.
- **Perform data backup**—Data backup should be carried out before the deployment of an MDM solution and throughout its use. This makes it easier for the organization to restore and access essential data in case of complications in the deployment process. The organization can also invest in cloud-based MDM solutions for critical organizational data and files.
- **Train employees**—Organizations should provide regular security training for employees on the reasons for and operation of MDM solutions. Employees should be periodically reminded about the MDM policy, associated risk and best practices. New employees should receive MDM policies and general information security training as part of their onboarding process. Retraining should be undertaken whenever the organization updates an existing MDM or acquires a new one.

5.9.5 Bring Your Own Device

BYOD is a policy that allows employees to bring their own personal mobile devices to work and use them to connect to the organization's network, to business resources and/or the Internet. BYOD offers many benefits to organizations that choose to adopt the practice, including:
- Increased productivity and innovation
- Improved employee morale
- Cost savings due to reduction of investment to procure and maintain end-user hardware and software licenses

Security and control issues related to BYOD include:
- Protection of sensitive data and intellectual property
- Protection of networks to which BYOD devices connect
- Responsibility and accountability for the device and information stored on it
- Removal of the organization's data from employee-owned devices on termination of employment or loss of the device
- Malware protection

Risk related to BYOD is similar to mobile computing risk. Some specific BYOD-related risk is:
- Access controls and controls over device security
- Ability to eliminate sensitive enterprise data on termination of employment or loss of the device
- Management issues related to supporting many different types of devices, OSs and applications

©ISACA. All Rights Reserved.

- Ensuring that employee-owned BYOD devices are properly backed up at all times

An employee BYOD agreement or acceptable use agreement (AUA) should be required before use of a is permitted for business purposes. The agreement may state that devices can be seized, if necessary, for legal matters. An AUA ensures that maintaining security when using personal devices is a responsibility shared between the user and the IT department. In addition, BYOD should be approved by executive management and be subject to oversight and monitoring.

Some of the best security practices for BYOD include:

- **Establish data ownership**—When a personal device is used for business tasks, there is commingling of personal data. Business data and establishing data ownership can be complicated. For example, if a device is lost or stolen, the company may wish to trigger a remote wipe, clearing the device of all valuable information, including personal information.
- **Obtain user acceptance**—BYOD needs to be clear and specific regarding all requirements for using a personal device at work. Organizations use awareness training programs to fully explain the details of a BYOD policy prior to allowing a personal device into the production environment. Only after a user has expressed consent and acceptance should the user's device be onboarded. It is critical to outline the consequences of failure to adhere to policy.
- **Enforce adherence to organizational security policies**—A BYOD agreement should clearly indicate that using a personal mobile device for business activities does not exclude an employee from adhering to the organization's security policies. Each employee should treat BYOD equipment as organizational property and stay in compliance with all restrictions, on and off premises and during and after hours.
- **Support device ownership**—When an employee's mobile device experiences a failure, fault or damage, the BYOD policy should define the kind of support provided by the organization and what support is left to the individual and, if relevant, the individual's SP.
- **Define processes for patch management**—It is critical for an organization to define the means and mechanisms of patch management for a personally owned mobile device and specify who should install updates. The need for the organization to test updates prior to installation on devices and the update level desired should be established.
- **Implement effective antivirus management**—The BYOD policy should dictate whether antivirus, antimalware and antispyware scanners are to be installed on mobile devices. There should be clarity as to which products/apps are recommended for use and which settings should be applied to those solutions.
- **Consider infrastructure requirements**—When implementing BYOD, organizations should evaluate their network and security design, architecture and infrastructure alongside the costs involved. BYOD typically increases the number of devices on the network, requiring proper infrastructure planning. Also, most mobile devices are wireless-enabled and require a robust wireless network to better deal with congestion.
- **Have an exit BYOD strategy**—There should be an exit strategy in place for BYOD, specifying the procedures to be followed when employees who uses their own devices leave the organization. Failure to enforce this may lead to backdoor attacks from disgruntled employees.

5.9.6 Internet Access on Mobile Devices

Smartphones and other mobile devices access the Internet by connecting to WLANs. These devices can also connect to the Internet over mobile networks.

Most mobile devices use fourth generation (4G) networks to connect to the Internet with the use of 5G increasing. 4G is an IP packet-switched network that offers increased speed and other capabilities, such as video conferencing, high definition (HD) streaming, VoIP and mobile TV. 5G is the latest generation of wireless communication technology that provides enhanced coverage, low latency and ultra-high speed data rates. These advances have also led to changes in the way Internet content is accessed, with applications that are supported and accessed through an Internet browser.

General issues and exposures that are related to wireless and/or mobile access include:

- **The interception of sensitive information**—Information is transmitted through the air, which increases the potential for unprotected information to be intercepted by unauthorized individuals.
- **The loss or theft of devices**—Devices tend to be relatively small, making them much easier to steal or lose.
- **The loss of data contained in the devices**—Theft or loss can result in the loss of data that has been stored on the device. This could be several gigabytes, depending on the capacity of the device. If encryption is weak or not applied, an attacker may access the information because it may only be protected by a password or personal identification number.

 ©ISACA. All Rights Reserved.

- **The misuse of devices**—Devices can be used to gather information or intercept information that is being passed over wireless networks for financial or personal benefit.
- **Distractions caused by the devices**—The use of the devices may distract users. If devices are being used in situations that require full attention (e.g., driving a car), the result could be an increased number of accidents.
- **OS vulnerabilities**—The OS may contain vulnerabilities that allow access to the device. Vulnerabilities allow devices to be jail broken, which means that restrictions are intentionally removed from a device, allowing some enhancements but potentially making it more vulnerable.
- **Applications**—Applications may contain vulnerabilities or malicious code that can allow access to data and the device itself. Jailbroken devices may be more susceptible because the apps may not come from secure sources.
- **Wireless user authentication**—There is a need for stronger user authentication and authorization tools at the device level. The current technology is just emerging.
- **File security**—Wireless phones and tablets do not use the type of file access security that other computer platforms provide.

5.9.7 Audit Procedures for Mobile Devices

Mobile devices should be subject to regular audits to ensure that any vulnerabilities and threats are addressed before they propagate to other systems in an organization. They constitute endpoints; therefore, audit procedures for mobiles devices are similar to audit procedures for endpoints. Audit procedures for mobile devices are the same procedures the IS auditor would undertake in a BYOD audit. **Figure 5.49** lists typical audit procedures for mobile devices.

Figure 5.49—Mobile Device Audit Procedures

Audit Area	Audit Procedures
Governance	• Verify that a security policy exists for mobile devices. • Verify that mobile devices have protective features enabled. • Verify that the policy prohibits users to carry mobile devices to sensitive areas. • Ascertain whether mobile devices have been subjected to risk assessments and periodic audits.
Patch management	• Ascertain whether device software is up to date. • Verify whether mobile antivirus software is up to date. • Verify that all mobile applications are up to date. • Verify procedures for testing and approving patches and determine whether they are secure.
Configuration and change management	• Determine whether mobile device gateways are running the latest approved software. • Verify that Bluetooth functionality is disabled when not in use. • Determine whether mobile operating systems (OSs) are appropriately patched. • Evaluate whether effective change management processes exist for mobile devices.
Device management	• Verify that the mobile device is not connected to unknown removal media. • Determine the effectiveness of device security controls around data protection. • Verify that there are no unmanaged devices on the network. • Verify whether remote wiping/locking on mobile devices is enabled. • Evaluate controls in place for life cycle device management for both organization-owned mobile devices and BYOD. • Verify that cameras are always covered when not in use. • Verify that location services are disabled when not required.
Bring Your Own Device (BYOD)	• Verify whether a BYOD policy is in place. • Evaluate controls in place to manage personally owned mobile devices. • Verify that BYOD procedures are in place for installing applications.

©ISACA. All Rights Reserved.

Figure 5.49—Mobile Device Audit Procedures (cont.)

Audit Area	Audit Procedures
Security monitoring	• Determine whether an asset management process is in place for monitoring and tracking of mobile devices. • Evaluate whether security monitoring systems, including log reviews, are in place. • Verify whether there are rules for downloading software onto mobile devices. • Determine whether mobile devices are subject to a centralized mobile device management (MDM) system.
Disaster recovery/ business continuity (DR/BC)	• Evaluate DR/BC processes to restore mobile devices and continue operations in case of disaster. • Verify that the DR/BC plan for mobile devices is tested regularly.
Awareness training	• Determine whether an awareness program on securing mobile devices is in place. • Verify that the training programs on mobile device security are in place. • Specify the types of information that can be stored on mobile devices. • Evaluate whether the training educates users not to open unknown links and attachments.
Encryption	• Verify whether sensitive data is properly secured while at rest and in transit. • Verify that mobile device users connect to the organization using secure channels such as Transport Layer Security (TLS), virtual private network (VPN), etc.

5.9.8 Mobile Payment Systems

A mobile payment system refers to a form of payment carried out through a mobile device.[45] Mobile payment systems can be linked to other payment infrastructure, such as credit cards and bank accounts. Mobile payment systems/applications are vulnerable to various types of threats and their security features often need to be enhanced on a continual basis. **Figure 5.50** lists mobile payment systems typically found in corporate organizations.

Figure 5.50—Types of Mobile Payment Systems

Payment System	Description
Digital wallets	Digital wallets, also known as e-wallets, are financial applications that can store value in digital form and allow users to perform transactions online, such as making purchases or transferring funds. Information that is stored in digital wallets include debit, credit and personally identifiable information.
Mobile wallets	Mobile wallets are digital payment systems that carry cash in a digital format. A mobile wallet is often regarded as a replacement for traditional credit and debit cards. Examples include Apple Pay and Samsung Pay. Mobile wallets are generally specific to the combination of software and hardware on certain devices. For example, Apple Pay only works with Apple products.
Digital currency wallets	Digital currency wallets are also known as cryptowallets. They typically store private keys representing ownership of a digital currency keeping them safe and accessible. A private key is used to sign over ownership of the digital currency when transferring value. They allow individuals to perform transactions digitally, such as sending, receiving and spending cryptocurrencies.

[45] European Union Agency for Cybersecurity, "Security of Mobile Payments and Digital Wallets," 19 December 2016, *https://www.enisa.europa.eu/publications/mobile-payments-security*

Figure 5.50—Types of Mobile Payment Systems (cont.)

Payment System	Description
Contactless payment communication technologies	This is a form of digital payment system that allows device-based mobile wallets to use communications technologies to transmit payment data from the mobile payment device to the merchant point of sale. These technologies allow individuals to conduct payment transactions through contactless chips embedded in devices such as payment cards, tags and mobile phones. The embedded chip communicates with the reader device through radio frequency or near field communication standards.

Mobile Payment Threats

IS auditors should be able to identify information security threats that use mobile payments as the attack vector. These threats manifest through the mobile phones themselves and mobile applications that users download to perform transactions. Threats directed against the users of mobile payment systems include:

- **Phishing**—Mobile phones generally mix business and social media, collecting customer data, some of it personally identifiable information. This often leads to sophisticated social engineering attacks, such as phishing attacks. These are typically easy to carry out as data about users is available in the public domain in places like social media sites. In phishing attacks, threat actors count on victims to click on insecure links, open emails containing security threats, and/or download malware.
- **Mobile malware**—Threat actors may install malware, including rootkits, on a mobile device through social engineering techniques. Another attack vector for malware infection is insecure Wi-Fi hotspots that allow an attacker to target a mobile device using man-in-the-middle techniques. The installation of malware can be facilitated by download attacks. Attackers can also upload malware to merchant point-of-sale (POS) servers and contactless terminals to remotely steal victim payment data that passes through the card readers.
- **Spoofing**—A malicious attacker sets up a fake AP with a network name similar to an existing one, such as a popular café name. It is possible for attackers to create a fake website for the purpose of collecting customer data, which is then used to carry out further attacks.
- **Unauthorized access**—An attacker may possess a device that has been lost or stolen. Once in possession of the device, the attacker might bypass user personal identification numbers (PINs) or fingerprint locks and connect to a public Wi-Fi. The attacker might proceed to intercept data in transit, such as a bank transfer or online payment.
- **Tampering**—When tampering with a mobile application, an attacker may create a backdoor in a mobile payment application for the purpose of capturing login details, which are sent to a server controlled by the attacker. The attacker can download an authorized application, tamper with it and upload it back to the store.
- **Application vulnerabilities**—Many mobile applications have vulnerabilities that can be exploited by attackers to gain unauthorized access and steal sensitive data stored by the application. This is prevalent where the applications have weak authentication systems.
- **Payment fraud**—Malicious actors can perpetrate fraud with stolen bank and credit card accounts linked to mobile payment application systems. For instance, a threat actor may exploit weaknesses in the registration process. This allows the attacker to add another mobile device to the user profile for the purpose of conducting fraudulent payments.
- **Token data compromise**—Another threat to mobile payment systems is token data compromise. This is more prevalent where issuers seek to leverage the tokenization service from the payment networks. They may also implement their own token service leading to an increased risk of threats against token data if the data is compromised.
- **Identity theft**—Attackers can steal identity information from users and use the information to open new accounts or perform other transactions in the victim's name. Users should protect their identities during the transaction process and minimize the amount of information they share on public platforms.
- **Cloned applications**—Mobile payment system threats may come from cloned applications. This is a major challenge, as users generally are not aware that they are using cloned applications, which perform the same as original applications. If users are duped into using cloned applications, it is easier for attackers to commit fraud, as clones have poor security features.

©ISACA. All Rights Reserved.

Mobile Payment Systems Security Best Practices

Some of the best practices focus on enhancing the security of mobile payment systems include:

- **Employ tokenization**—Tokenization refers to the process of scrambling information into a string of randomly generated data so that it is unusable to threat actors. The scrambled data is known as a token and is used as a replacement for the original data—it cannot be unscrambled and returned to its original state. The token is typically sent through the Internet or payment networks to complete the payment. If the token is not exposed, the data will be useless to an attacker if intercepted. Tokenization thus promotes mobile payments while protecting sensitive customer data against threat actors.
- **Implement device-specific cryptograms**—The implementation of cryptograms on specific devices ensures that a payment originates from the cardholder's mobile device and is genuine. If an attacker intercepts data during a mobile payment transaction, the cryptogram sent with the token to a POS terminal cannot be used on another mobile device. This is because the token is unique to the original device.
- **Implement 3D Secure**—3D Secure is an authentication method designed to prevent the unauthorized use of cards and mobile phones. It seeks to protect online businesses from chargebacks in the event of a successful fraudulent transaction. Using 3D Secure requires merchants, card networks and financial institutions to share information required for transaction authentication.
- **Implement strong customer authentication (SCA)**—SCA is a type of authentication designed to reduce fraud and increase online payments security. It requires two or more factors for customer authentication purposes. This is very effective in mitigating identity theft and automated or bot attacks.
- **Continuously monitor fraud**—Mobile payment systems typically require a payment gateway for the detection and management of fraud. The IS auditor may also advise the organization to invest in built-in fraud monitoring systems to identify areas posing real risk of fraudulent transactions. The organization can set rules, based on its risk tolerance, and accept or reject transactions posing high risk.
- **Conduct regular audits**—Regular audits for mobile payment systems are crucial as they assist the organization in the identification of vulnerabilities and potential threats in mobile payment platforms. Audits also prod management with recommendations that can be used in the implementation of mobile payment systems controls.
- **User awareness training**—User awareness training defends against social engineering attacks by making users aware, encouraging them to stay alert to indicators of social engineering attacks and instructing them in how to properly respond to such attacks.

5.9.9 Wireless Networks

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections (i.e., without requiring a network or peripheral cabling). Wireless is a technology that enables organizations to adopt e-business solutions with tremendous growth potential. Wireless technologies use radio frequency transmissions/electromagnetic signals through free space as the means for transmitting data, whereas wired technologies use electrical signals through cables. Wireless technologies range from complex systems (e.g., wireless wide area networks [WWANs], WLANs and cellphones) to simple devices (e.g., wireless headphones, microphones and other devices that do not process or store information). Wireless technologies include Bluetooth devices, which are equipped with mini radio frequency transceivers; and infrared devices such as remote controls, cordless computer keyboards and mice, and wireless headsets—all of which require a direct line of sight between the transmitter and the receiver to close the link.

Wireless introduces new elements that must be addressed. For example, existing applications may need to be retrofitted to make use of wireless interfaces. Also, decisions need to be made regarding general connectivity to facilitate the development of completely wireless mobile applications or other applications that rely on synchronization of data transfer between mobile computing systems and enterprise infrastructure. Other issues include narrow bandwidth, the lack of a mature standard, and unresolved security and privacy issues.

Wireless networks serve as the transport mechanism between devices, and among devices and traditional wired networks. Wireless networks are many and diverse but are frequently categorized into four groups based on their coverage range:

- WWANs
- WLANs
- Wireless personal area networks (WPANs)
- Wireless ad hoc networks

 ©ISACA. All Rights Reserved.

Wireless Wide Area Networks

Wireless wide area networking is the process of linking different networks over a large geographical area to allow wider IT resource sharing and connectivity. While computers are often connected to traditional WANs using cable networking solutions (such as telephone systems), WWANs are connected via radio, satellite and mobile phone technologies.

WWANs can complement and compete with more traditional systems of cable-based networking. The most common WWAN technology in use today is advertised as fourth-generation Long Term Evolution (4G LTE), with fifth-generation (5G) capabilities rapidly gaining acceptance. The Global System for Mobile Communications (GSM) third-generation standard is still commonly available.

For some organizations, such as those in rural areas where laying cable is too expensive, wireless technology offers the only networking solution. For others, WWAN provides greater system flexibility and the opportunity to control costs where the equipment is owned. Implementing a WWAN requires careful attention to the planning and surveying of the network. The total cost of ownership involved in switching to this rapidly evolving system of networking should also be considered.

Wireless Local Area Networks

WLANs allow greater flexibility and portability than traditional wired LANs. Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN uses an AP device to connect computers, tablets, smartphones and other components to the network. An AP, or wireless networking hub, communicates with devices equipped with wireless network adaptors within a specific range of the AP; it connects to a wired Ethernet LAN via an RJ-45 port. AP devices typically have coverage areas of up to 300 feet (approximately 100 meters). A coverage area is called a cell or range. Users move freely within a cell with their laptops or other network devices. AP cells can be linked to allow users to roam within a building or between buildings.

WEP and Wi-Fi Protected Access

Symmetric private keys periodically cause difficulties when new keys are distributed to network interface cards (NICs). As a result, keys remain unchanged on networks for extended times. With static keys, several hacking tools can easily break through the relatively weak Wired Equivalent Privacy (WEP) encryption mechanisms. Because of the key-reuse problem and other flaws, the current standardized version of WEP does not offer strong enough security for most enterprise applications. Newer security protocols use public key cryptography techniques to provide effective authentication and encryption between users and APs.

Common WEP technologies include:

- **Wireless Protected Access (WPA)**—WPA was adopted by the Wi-Fi Alliance as a temporary enhancement and alternative for WEP. The WPA standard consists of two modes that use distinct encryption methods: WPA-Enterprise and WPA-Personal. WPA-Personal is a common method to secure wireless networks, and it is suitable for most home networks. WPA-Enterprise provides security for wireless networks in business environments where a RADIUS server is deployed.
- **Wireless Protected Access 2 (WPA2)**—WPA2 was ratified in 2004 as the new Wi-Fi security standard improving over WPA. The most significant improvement in the WPA2 security standard is the implementation of AES, which provides higher security and performance. However, a vulnerability exists that allows an attacker to get access to a secured WPA2 network and obtain certain keys to attack other devices on the same network. This attack is more pronounced in enterprise networks than home networks.
- **Wireless Protected Access 3 (WPA3)**—This is the newest generation of Wi-Fi security with the aim of simplifying Wi-Fi security. It delivers more robust authentication and increases cryptographic strength, making it suitable for highly sensitive communication environments. WPA3 was proposed by the Wi-Fi Alliance to remedy the flaws prevalent in WPA2, such as dictionary attacks. For public networks WPA3 enhances security by automatically encrypting connections without the need for credentials.

Figure 5.51 compares wireless security solutions.

©ISACA. All Rights Reserved.

Figure 5.51—Comparison of Wireless Security Solutions

	Wired Equivalent Privacy (WEP)	Wireless Protected Access (WPA)	Wireless Protected Access 2 (WPA2)	Wireless Protected Access 3 (WPA3)
Encryption method	Rivest Cipher 4 (RC4)	Temporary Key Integrity Protocol (TKIP) with RC4	CCMP and Advanced Encryption Standard (AES)	AES
Session key size	40-bit	128-bit	128-bit	128-bit (WPA3-Personal) 198-bit (WPA-Enterprise)
Cipher type	Stream	Stream	Block	Block
Data integrity	CRC-32	Message Integrity Code (MIC)	Cipher Block Chaining Message Authentication Code (CBC-MAC)	Secure Hash Algorithm (SHA)
Vulnerabilities	Fragmentation Denial of service (DoS) attacks	Pre-Shared Keys (PSK) attacks DoS attacks	DoS attacks MAC spoofing	Downgrade attacks Side channel attacks
Deployment complexity	Easy to deploy and configure	Relatively easy to deploy and configure	Complicated setup for Enterprise version	Easier to add new devices
Key management	No key management provided	4-way handshaking mechanism	4-way handshaking mechanism	Simultaneous Authentication of Equals (SAE)
Replay attack protection	No replay attack protection in place	Implements sequence counter solution to address replay attacks	Protects against replay attacks using a 48-bit datagram/packet number	Implements mandatory use of protected management frames (PMF) technology to deal with attacks such as replay

Wireless Personal Area Networks

WPANs are short-range wireless networks that connect wireless devices to one another. The most dominant form of WPAN technology is Bluetooth, which links wireless devices at very short distances. The oldest way to connect devices in a WPAN fashion is infrared communications. Bluetooth is an open-source standard that borrows many features from existing wireless standards—such as Institute of Electrical and Electronics Engineers (IEEE) 802.11, IrDA, Digital Enhanced Cordless Telecommunications, Motorola's Piano and TCP/IP—to connect portable devices without wires via short-range radio frequencies.

Bluetooth is a wireless protocol that connects devices within a range of up to 49 feet (15 meters). It has become a feature on many tablets, mobile phones, PC keyboards, mice, printers, etc. It is a system that changes frequencies from moment to moment using a technique called frequency-hopping. Bluetooth is used in computer systems, especially laptops, as a replacement for physical cables and for infrared connections, which are limited to line of sight. Bluetooth devices find one another when they are in range and automatically set up a background connection.

Bluetooth allows for high data speeds (between 1 Mbps and 2 Mbps) but is designed only for peer-to-peer data transfer. An alternative form of WPAN technology, called ZigBee, offers slower data speeds (250 Kbps) than Bluetooth but is cheaper than Bluetooth and requires far less energy to power.

Ad Hoc Networks

Ad hoc networks are designed to dynamically connect remote devices, such as mobile phones, laptops and tablets. These networks are termed ad hoc because of their shifting network topologies. Whereas WLANs

 ©ISACA. All Rights Reserved.

or WPANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a system of mobile routers connected by wireless links to enable devices to communicate. Bluetooth networks can behave as ad hoc networks because mobile routers control these networks' changing topologies.

The routers also control the flow of data between devices that can support direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured to handle the dynamic topology. The routing protocol employed in Bluetooth allows the routers to establish and maintain these shifting networks.

The mobile router is commonly integrated in a handheld device. The mobile router, when configured, ensures that a remote mobile device, such as a mobile phone, stays connected to the network. The router maintains the connection and controls the flow of communication.

Wireless Security Threats and Risk Mitigation

Wireless security threats can be classified as:

- Errors and omissions
- Fraud and theft committed by authorized or unauthorized users of the system
- Employee sabotage
- Loss of physical and infrastructure support
- Malicious hackers
- Industrial espionage
- Malicious code
- Foreign government espionage
- Threats to personal privacy

All of these represent potential threats to wired networks as well. Ensuring CIA is the prime objective in wireless networks.

Security requirements include:

- **Authenticity**—A third party must be able to verify that the content of a message has not been changed in transit.
- **Nonrepudiation**—The origin or the receipt of a specific message must be verifiable by a third party.
- **Accountability**—The actions of an entity must be uniquely traceable to that entity.
- **Network availability**—The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability includes ensuring that resources are used only for intended purposes.

Risk in wireless networks is equal to the sum of the risk of operating a wired network plus the new risk introduced by weaknesses in wireless protocols. To mitigate the risk, an organization must adopt security measures and practices that help bring risk to a manageable level. Some of the more salient threats and vulnerabilities of wireless systems include:

- All of the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Weaknesses in wireless protocols increase the threat of disclosure of sensitive information. Many wireless networks are either not secure or use outdated encryption algorithms.
- Malicious entities may gain unauthorized access to an agency's computer or voice (IP telephony) network through wireless connections, potentially bypassing firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and is transmitted between two wireless devices may be intercepted and disclosed.
- DoS attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identities of legitimate users and masquerade as them on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and track their physical movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and APs) to surreptitiously gain access to sensitive information.
- Mobile devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and be subsequently introduced to a wired network connection.
- Malicious entities may use wireless connections to connect to other agencies for the purposes of launching attacks and concealing their activity.
- Interlopers may be able to gain connectivity to network management controls and thereby disable or disrupt operations.
- Malicious entities may use an untrusted third-party wireless network service to gain access to network resources.

Another problem with WPANs is the uncontrolled propagation of radio waves; for example, the radio traffic on Bluetooth connections can be passively intercepted and recorded using Bluetooth protocol sniffers, such as

©ISACA. All Rights Reserved.

Red Fang, Bluesniff and others. If the device addresses are known, then even if the devices are currently in non-discoverable mode, it is possible to synchronize to the frequency hopping sequence. All the layers of the Bluetooth protocol stack can be examined and analyzed offline. If encryption is not used, then it is possible to extract and monitor the transmitted user data. Use of an antenna with a strong directional characteristic and electronics that are capable of amplifying Bluetooth signals can make passive listening attacks possible from a greater distance than the functional range. Transmitting power control is optional and is not supported by every Bluetooth device.

Wireless Secure Encryption Protocols

Wireless networks are now prevalent in both businesses and home environments. While convenient, they also pose widespread security risk. Most security risk and vulnerabilities are exacerbated by the inadequacies of the wireless security protocols in place. Some protocols are secure while some are insecure, and others are in-between. **Figure 5.52** provides brief descriptions of some of the secure wireless encryption protocols.

Figure 5.52—Secure Wireless Encryption Protocols

Protocol	Description
802.1X/EAP	802.1X/EAP is a standard port-based network access control that ensures clients only communicate after proper authentication has taken place. It supports both Wireless Protected Access (WPA) and Wireless Protected Access (WPA2). Through 802.1X, organizations can integrate techniques and solutions such as Remote Access Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System (TACACS), certificates, smart cards and token devices into wireless networks. This adds the security benefit of mutual and multifactor authentication (MFA).
Extensible Authentication Protocol (EAP)	EAP is an authentication framework that supports compatibility of new authentication technologies with existing wireless or Point-to-Point Protocol (PPP) connection technologies. Several EAP methods of authentication are widely supported, including LEAP, Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS). The information systems (IS) auditor should be alert to the fact that not all EAP methods are secure. For example, Extensible Authentication Protocol-Message Digest Algorithm (EAP-MD5) has been proven breakable.
Protected Extensible Authentication Protocol (PEAP)	PEAP encapsulates EAP methods within a Transport Layer Security (TLS) tunnel, thus providing authentication and, potentially, encryption. PEAP was introduced because EAP is typically not encrypted.
Lightweight Extensible Authentication Protocol (LEAP)	LEAP was implemented mainly to address deficiencies in TKIP prior to the ratification of 802.11i/WPA2. LEAP is insecure and should not be implemented; it has been attacked before. However, where use of LEAP cannot be avoided, IS auditors should recommend the implementation of strong passwords alongside LEAP.
MAC filter	A MAC filter is simply a list of authorized wireless client interface MAC addresses used by a WAP to block access to all non-authorized devices. This is an important technology to implement but has proven to be difficult to manage. It is ideal for static environments. Attackers have been known to discover MAC addresses and spoof them onto their wireless attack client.

 ©ISACA. All Rights Reserved.

Figure 5.52—Secure Wireless Encryption Protocols (cont.)

Protocol	Description
Temporal Key Integrity Protocol (TKIP)	TKIP was designed as the replacement for WEP without requiring replacement of legacy wireless hardware. TKIP was implemented into 802.11 wireless networking under WPA. TKIP improvements include a key-mixing function that combines the initialization vector with the secret root key before using the key with Rivest Cipher 4 (RC4) to perform encryption. A sequence counter is incorporated into the solution to prevent packet replay attacks, and a strong integrity check is applied. KIP and WPA were officially replaced by WPA2. Attacks specific to WPA and TKIP have made WPA's security unreliable.
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)	CCMP was created to replace WEP and TKIP/WPA. CCMP uses Advanced Encryption Standard (AES) with a 128-bit key. CCMP is the preferred standard security protocol of 802.11 wireless networking indicated by 802.11. To date, no information security attacks have yet been successful against the AES/CCMP encryption.

Auditing Procedures for Wireless Networks

A wireless network security audit evaluates all the security aspects of a wireless network. The IS auditor should undertake audit procedures for such an evaluation and be familiar with the tools and technologies typically applied in wireless network security audits. It is critical for the IS auditor to understand that attackers may use the same tools and technologies used by the IS auditor. Attackers may even employ more advanced technologies. Therefore, IS auditors and organizations in general should always strive to have an upper hand over attackers. **Figure 5.53** shows some of the typical audit procedures that can be applied in an audit of wireless networks.

Figure 5.53—Wireless Security Audit Procedures

Audit Component	Audit Procedures
Governance	• Ask management whether there is an approved wireless communications policy in place. If so, inspect whether it is current and is being followed. • Ask whether the organization undertakes regular risk assessments. If so, obtain and review prior risk assessment reports. • Ask whether the access point (AP) configuration is subject to periodic audits to detect unauthorized modifications. If subject to audit, request the prior audit reports and review them.
Wireless architecture	• Verify that a site survey was performed prior to deployment of APs for adequate data rates. • Identify sources of unauthorized wireless installations and advise on their uninstallation. • Verify that APs are running on the latest approved software. • Review the overall architecture for wireless deployment and determine whether it is appropriate. • Determine whether the placement of wireless networks is secure and appropriate to meet the organization's needs. • Examine the physical security of the APs and related infrastructure. • Verify that the wireless network is appropriately segmented from the local area network (LAN). • Verify that rogue APs are not used on the organization's wireless network.

©ISACA. All Rights Reserved.

Figure 5.53—Wireless Security Audit Procedures (cont.)

Audit Component	Audit Procedures
Configuration management	• Verify that a system of configuration management is in place and is used for all changes in the wireless network. • Determine whether wireless intrusion detection system (IDS) sensors are properly placed. • Verify that all default AP configuration settings were changed prior to connecting them to the organization's production network. • Verify that wireless networks are appropriately segmented. • Verify that the wireless network is not connected to public Wi-Fi networks.
Encryption	• Ascertain whether the strongest encryption technologies were implemented. 128 bits is generally considered the minimum acceptable level. • If Wireless Protected Access 2 (WPA2) has been implemented, verify that it uses Advanced Encryption Standard (AES) encryption. • Determine whether authentication is mutual and centralized. • Verify that weak protocols such as Wired Equivalent Privacy (WEP) have not been implemented. WEP is weak and usually a last option.
Credential management	• Verify that all default passwords have been changed. • Verify that all unused management interfaces have been disabled. • Determine whether an out-of-band network or a separate virtual LAN network has been implemented to manage APs. • Examine service set identifier (SSID) construction and ensure that its name does not include the name of the organization, the address, phone number, etc. • Verify that the SSID is not broadcast.
Monitoring	• Verify whether real-time monitoring is implemented. • Examine the placement of the wireless IDS/intrusion prevention system (IPS) solution for appropriateness. • Verify that a session timeout process has been instituted. • Review prior security assessments and verify that the weaknesses identified have been addressed. • Evaluate procedures in place to detect rogue wireless devices, hidden wireless networks and unauthorized devices. • Determine whether the organization keeps abreast of developments in wireless authentication and authorization schemes and replaces schemes that have been broken before.

5.9.10 Internet of Things

IoT refers to a collection of devices that can communicate over the Internet with one another or with a certain control console to affect and monitor the real world. The term is used to describe any physical devices that are mounted with sensors and specific software with the ability to connect, exchange and process data, including home appliances. Many organizations require specific auditing procedures that are tailored to the challenges and risk specific to IoT environments.

Closely associated with IoT are embedded systems. An embedded system is implemented as part of a larger system. It is typically designed around a limited set of specific processing functions in relation to the larger system of which it is a component. It may consist of the same components found in a typical computer system, or it may be a microcontroller (i.e., an integrated chip with on-board memory and peripheral ports). Examples of embedded systems include network-attached printers, smart TVs, heating ventilation and air conditioning controls, smart appliances, smart thermostats and medical devices.

The growing IoT is comprised of physical objects with the capability to communicate in new ways—with each other, with their owners or operators, with manufacturers or with others—to make people's lives easier and enterprises more efficient and competitive.

Business value and organizational competitiveness can be derived as enterprises capitalize on IoT capabilities to gain more and better business value from the devices

 ©ISACA. All Rights Reserved.

they purchase. Additionally, businesses can compete more effectively in the marketplace because they provide these features in products they sell and incorporate them into service offerings they provide.

IoT Risk

With additional value comes additional risk. Although specific risk depends on use, some of IoT risk areas include:

- Business risk (e.g., health and safety, regulatory compliance, user privacy, unexpected costs)
- Operational risk (e.g., inappropriate access to functionality, shadow use, performance)
- Technical risk (e.g., device vulnerabilities, device updates, device management)

Some of the major risk of IoT are:

- **Low software quality**—The quality of software in IoT devices is generally low due to developers and end-users being unaware of potential security issues of embedded devices and their firmware.
- **Lack of encryption**—Most IoT devices do not implement encryption technologies in their security functionalities. As a result, attackers can access important information such as account credentials as they traverse the network to an IoT device.
- **Low processing power**—Firmware is applied in IoT to provide connectivity to the network and certain functionalities. This firmware has to run on hardware such as a system on a chip. This poses challenges due to low-end computational power. This leads to less energy being used and low processing power.
- **Outdated hardware and software components**—The hardware and OSs used in IoT might be outdated and contain security vulnerabilities that can be exploited by attackers. For example, attackers can run an IoT botnet or eavesdrop on IoT traffic.
- **Backdoor accounts**—Some IoT devices and accounts can contain backdoors, which often masquerade as "service" accounts. Attackers can use them to bypass access controls implemented on a device and access organizational resources.
- **Poor device management**—Organizations often lack visibility into all IoT devices that are connected to disparate systems. Most IoT devices connect remotely, which leads to little insight into the IoT security risk in the network environment.
- **Interconnectedness**—IoT devices are typically interconnected, so if one device is compromised it is possible that the attack can spread to other devices or even compromise the entire organizational network.
- **Absence of inbuilt security**—IoT devices often do not possess any inbuilt security features, which makes them a perfect target for attackers. Because of this, it is often recommended to disconnect IoT devices when they are not in use to reduce the attack surface for the overall network.

IoT Security Controls

Security is imperative for IoT technology. For most IoT businesses and vendors, the continued increase in IoT devices brings greater security risk, which should be addressed with strong IoT controls. IoT controls are similar to mobile device controls. The IS auditor reviewing controls in an IoT environment should assess many aspects of the control environment, including:

- **Physical security**—Since IoT applications are remote, physical security is crucial for preventing unauthorized access to the IoT device. The organization should use resilient components and specialized hardware to make corporate data difficult for unauthorized parties to access. For example, in cellular IoT devices, the SIM card stores most of the critical information. An organization can implement an International Mobile Station Equipment Identity (IMEI) lock. The organization can also implement eSIM technology, thus allowing for the activation of mobile data without using the physical SIM card.
- **Remote access security**—An organization should implement robust remote-access security protocols that have certain capabilities. For example, the remote access implemented should be able to lock the SIM functionality to a specific device and to remotely disable connection upon detection of any physical security breaches.
- **Public vs. private networks**—The use of public networks, especially Wi-Fi networks, should be avoided at all costs. Connecting IoT devices and enabling them to communicate using public networks is a serious security risk, as it opens up those messages for interception and other types of attacks. Organizations should prefer to use private networks instead, especially when communicating sensitive information.
- **Encryption**—See section 5.6 Data Encryption for more information.
- **Network isolation**—The IS auditor should understand that IoT applications are typically designed for a specific purpose and for network connectivity. Therefore, the IoT device's network connectivity should be isolated as much as possible from its core functions. This enhances security by reducing the attack surface. Unneeded functions

©ISACA. All Rights Reserved.

should be disabled to further minimize the attack surface.

- **Abnormality prevention and detection**—There should be controls in place so that users are aware the moment any abnormal activity occurs across the organization's systems. Such abnormal activity should be thoroughly analyzed as it may point to attackers attempting to breach an IoT system. Firewalls can be implemented to monitor and block traffic outside the organization's network perimeter.

 ©ISACA. All Rights Reserved.

Part B: Security Event Management

Security event management (SEM) is the process of identifying, collecting, monitoring, responding and reporting security-related events in components of the IS infrastructure and the overall IS environment. SEM solutions enable the recording and evaluation of security events and help IS auditors to analyze information security architecture, policies, procedures and guidelines in place. It is critical for the IS auditor to understand the solutions available across vendors, assess the appropriateness of the solutions and proffer sound advice to management.

5.10 Security Awareness Training and Programs

Effective security in an organization depends on people. This means that the success and effectiveness of any security initiative is largely based on whether the people (in this case employees and partners) understand the operation of the security solution and know what is expected of them. They should at least know why the security controls are in place, how to support the controls and the consequences to the organization and themselves of violating security controls. Because everyone is fallible, people are considered the weakest link in information security; hence the emphasis on security awareness, training and education programs. If the programs are carried out efficiently and effectively, organizations will experience a decline in information security attacks. An IS auditor should be able to differentiate between security awareness, security training and security education and be in a position to provide guidance on their implementation.

5.10.1 The Information Security Learning Continuum

Information security learning starts with security awareness, builds to security training and evolves into security education:

- **Security awareness**—The aim of a security awareness program is to change the behavior of people regarding their daily operations and create a culture of good security practices. In building awareness, learning is often passive. Employee awareness should start at point of hire and continue regularly. Techniques for delivery need to vary to prevent the awareness-building effort from becoming stale or boring to the audience.
- **Security training**—The purpose of security training in an organization is to teach employees relevant skills to perform their jobs in a more secure manner. In a nutshell, training is more formal than awareness and focuses on building knowledge, skills and competencies. It usually targets functional areas of the organization. An example of security training is an IS security course for IS security administrators that covers all the security controls to be implemented in the organization.
- **Security education**—Security education is more intensive than security training and targets security professionals—that is, employees whose jobs require expertise in information security. It is mainly earmarked for those seeking careers in information security and is obtained through colleges, universities and other specialized training programs. Education is obtained through college or graduate classes or through specialized training programs. Security education typically integrates various security skills and competencies to produce a multidisciplinary common body of knowledge on information security.

Management may sometimes request advice from IS auditors regarding the best program to undertake between awareness, training and education given the prevailing circumstances in the organization. Therefore, it is very critical for IS auditors to distinguish between awareness, training and education as regards information security in an organization. **Figure 5.54** summarizes these differences.

©ISACA. All Rights Reserved.

Figure 5.54—Differences Among Awareness, Training and Education

	Awareness	Training	Education
Knowledge level	Delivery of knowledge regarding the characteristics of an information security component; for example, explaining the "what" of an information security policy	Delivery of focused information on the operations of an information security component; in other words, answering the "how" of an information security procedure	Delving into the reasons underlying the use of a particular information security component; answering the "why" of an information security tool
Objective	Knowledge retention, so that the employees may recall concepts	The practical ability to complete an information security task	An understanding of the broader view regarding information security, incorporating critical analysis
Typical training methods	Self-paced e-learning, web-based training, videos	Instructor-led training, demos, laboratory experiments, hands-on activities	Seminars, research, lectures
Time frame	Short term	Intermediate term	Long term
Testing method	Short quizzes, true/false, multiple choice	Application-level problem solving and practical tests	Interpretation of learning, architecture exercises and examinations

5.10.2 Benefits of a Security Awareness, Training and Education Program

Some of the benefits of having an awareness, training and education program in an organization are:

- **Supports individual accountability**—Employees cannot be held accountable for their actions if they are unaware of the security controls in place or how to operate them. Most security threats result from employee negligence or ignorance. When employees are trained and are aware of what is expected of them in terms of information security, it becomes easier for management to enforce accountability.
- **Serves as a preventive control**—As employees become aware of their security roles and responsibilities, they assist in maintaining best security practices in the organization.
- **Serves as a detective control**—Training and education encourages employees to identify and report possible security violations in their daily activities in their respective departments. This enables the organization to quickly address security incidents.
- **Lowers security risk**—It should be clear to the IS auditor that security risk is generally inherent in using various information systems and cannot be addressed solely by implementing technical solutions and technologies. It often requires the support of the people in the organization; in fact, it is people who oversee the operation of technical solutions. A security-trained and security-aware workforce significantly lowers security risk in the organization.
- **Serves as a foundation for other security controls**—In almost any security implementation, the best practice is awareness training, especially before deployment of any security solution. Without training and awareness, it would be difficult to successfully implement and operate security controls. The chief reason is that the operation of security controls requires people. Even when automation is successful, the decisions to deploy solutions and the interpretation of automated reports rests on people.

5.10.3 Approach to Security Awareness, Training and Education

In larger organizations, there may be a large enough population of middle and senior management to warrant special management-level training on information security awareness and operations issues. All employees of an organization and, if relevant, third-party users must receive appropriate training and regular updates on the importance of security policies, standards and procedures in the organization. This includes security requirements, legal responsibilities, business controls and training in the correct use of information processing facilities (e.g., login procedures, use of software packages). For new employees, this training should occur before access to information or services is granted, and it should be included in new employee orientation.

 ©ISACA. All Rights Reserved.

A methodical approach should be taken to developing and implementing the education and awareness program with the following aspects being considered:

- Who is the intended audience (senior management, business managers, IT staff, end users)?
- What is the intended message (policies, procedures, recent events)?
- What is the intended result (improved policy compliance, behavioral change, better practices)?
- What communication method will be used (computer-based training [CBT], all-hands meeting, intranet, newsletters, etc.)?
- What is the organizational structure and culture?

Mechanisms for raising information security awareness include:

- Computer-based security awareness and training programs
- Email reminders and security tips
- Written security policies and procedures (and updates)
- Nondisclosure statements signed by employees
- Use of different media in promulgating security (e.g., company newsletters, web pages, videos, posters, login reminders)
- Visible enforcement of security rules
- Simulated security incidents for improving security
- Rewarding employees who report suspicious events
- Periodic reviews
- Job descriptions
- Performance reviews

There are three major steps in the development of an IT security awareness and training program: 1) designing the program (including the development of the IT security awareness and training program plan), 2) developing the awareness and training material, and 3) implementing the program.

5.10.4 Conditions for a Successful Security Awareness Training and Education Program

An effective IS security awareness, training and education program consists of:

- Developing a security culture that encourages a shared mindset and empowers individuals to be vigilant about cybersecurity, which is critical in shaping a comprehensive strategy for information assets protection
- Developing an IS information security policy that incorporates the elements of security awareness, training and education to provide direction to the organization
- Informing everyone in the organization of their IS security roles and responsibilities and what is expected of them to enhance information security
- Establishing processes and procedures for monitoring and reviewing the program
- Focusing on the entire organization
- Setting the tone at the top for proper IS security behavior in the organization
- Explaining, in simple terms, the proper rules of behavior in the use of information systems
- Establishing the basis for any penalties and other sanctions to be imposed due to noncompliance
- Centering on the organization's IS security policy and issue-specific policies

Developing a rollout plan or strategy for the IS security awareness, training and education program to occur after a needs assessment is carried out

5.10.5 Conducting a Needs Assessment

A needs assessment is a process that determines an organization's awareness and training needs. Its results can provide justification to convince executive management to prioritize the assessed program among other competing needs. If management is convinced, it will allocate adequate resources in terms of time and money to meet the identified awareness and training needs. In conducting a needs assessment, everyone's needs should be considered, and all key personnel should be involved.

Roles that should be considered in the analysis of security training needs include:

- **Executive management**—These are the leaders of the organization, and they need to fully understand information security in general, its importance and the legal frameworks underpinning information. Once an organization's leaders understand the importance of information security, it becomes easier for them to provide direction along with the resources and commitment required.
- **Information security personnel**—Information security personnel in an organization include the security architects, security software engineers, security program managers and security officers. These individuals provide expert advice and implement and operate the security infrastructure in the organization. They should be trained and educated in the technical aspects of information security, the security policy and best practices in information security.
- **System owners**—System owners are generally not expected to be experts in information security as they

©ISACA. All Rights Reserved.

are not directly responsible for information security. However, they should have a general and high-level understanding of the information security policy and the security controls applicable to the systems they own. If they encounter any technical challenges beyond their comprehension, they should forward such challenges to information security personnel for resolution.

- **System administrators and IS support**—This group of personnel is ordinarily entrusted with providing adequate information security support to organizational operations. They often hold a high degree of authority and can make decisions on who should be allowed or denied access, for example. These individuals require a high degree of technical information security knowledge, almost to the same level of information as security personnel. They also need an understanding of the implications of their actions on organizational operations.
- **Operational staff and system users**—These individuals are not technical IS personnel and rarely understand information security. Their major focus is to meet organization goals, such as productivity and profitability, with less-to-no focus on information security. They need to be provided with a high degree of security awareness and training on security controls and the acceptable rules of behavior for systems they use to conduct their roles. From an IS audit perspective, this group is the riskiest when it comes to information security in an organization; therefore, assessing it should be prioritized.

Information Sources for Needs Assessment

Numerous sources of information can be used to determine the IS security awareness, training and education needs of an organization. There are also many ways of collecting that information. The methods for information collection should be as simple as possible as long as they reliably collect the required information. Some of the sources of information are:

- Interviews with all identified key personnel or groups of personnel in the organization
- Organizational security surveys
- Reviews and assessments of available security awareness, training and education resource material
- Analyses of metrics related to awareness, training and education, such as percentage of users trained in social engineering
- Reviews of information security plans to identify the appointed individuals and their respective security roles and responsibilities
- Reviews of system access databases to determine individuals access levels
- Reviews of findings and recommendations from oversight bodies such as internal audit
- Discussions with management and system owners whose business functions rely on IS
- Analyses of security events, incidents and attacks to gain insight on the training needs of specific personnel
- Current trends in the industry provided by academia, government publications and training organizations

5.10.6 Implementing an Awareness and Training Program

After a needs assessment has been conducted, a strategy developed, material developed and resources availed, an IS security awareness, training and education program can be implemented. The program requires proper planning, implementation, maintenance and evaluation as shown in **figure 5.55**.

The implementation can be carried out through a series of steps, which include:

- **Define program scope**—This is the first step in developing an organizational awareness and training program. The scope should include the goals, objectives and strategies of the program rollout and should cover various groups of employees who interact with the organization's information systems. Smaller organizations may have one program to cover the whole organization; large organizations may have one master program and several more specific programs. The overall objective of the program should be to enhance security awareness, training and education initiatives in the organization.
- **Select training staff**—The next stage is to identify staff to facilitate the training process. These trainers can be sourced internally or externally or from a combination of these sources. What is most critical is to ensure that the selected trainers have sufficient knowledge of the content they are supposed to present.
- **Identify target audience**—For any particular topic up for training, the organization should ensure that the appropriate people are targeted. Everyone does not need the same type of training, so this approach helps the organization channel training resources to areas of most need. The needs assessment greatly assists in identifying the target audience for any training program in the organization.
- **Motivate management and trainees**—For successful implementation, a program should gain

the support and commitment of both management and employees. Motivational techniques can be implemented to arouse interest in the program with a presentation of how their participation benefits the organization. Management commitment is critical, as it ensures the adequacy and delivery frequency of resources allocated to the awareness and training program.

- **Administer the program**—The program should be administered in an efficient and effective manner. The program should be given visibility in the organization, training materials should be adequate and timely provided, and the training methods should conform to the material available. In addition, the topics should be relevant, and the presentation clear.
- **Maintain the program**—The field of IS is an ever-evolving field and concepts and practices are always changing. Therefore, a training program that is currently relevant may not be relevant in the future. Hence the organization should ensure that the program is maintained, and efforts are made to keep abreast of changing knowledge requirements.
- **Evaluate the program**—One of the major challenges in the implementation of an awareness and training program is that it is often difficult to measure its effectiveness, and its return on investment (ROI) is often unquantifiable. However, an organization should attempt to evaluate the program using other measurements, such as ascertaining the amount of information retained, the extent of compliance with the information security policy, and the general attitudes and behaviors of people toward information security. The results of the evaluation should be used to solve any problems in the program. Some evaluation methods include:
  - Using student evaluations, mainly in the form of questionnaires
  - Observations of employees following security procedures
  - Testing and examining employees on material covered
  - Monitoring incidents received before and after training
  - Establishing focus groups (i.e., combining trainees into groups to discuss program effectiveness and ways to improve)
  - Carrying out interviews with selected trainees according to specific criteria and areas of feedback

Figure 5.55—Steps in the Implementation of an IS Awareness and Training Program



©ISACA. All Rights Reserved.

5.11 Information System Attack Methods and Techniques

Risk arises from vulnerabilities (whether technical or human) within an environment. Attack techniques exploit those vulnerabilities and may originate either within or outside the enterprise. Computer attacks can result in proprietary or confidential data being stolen or modified, loss of customer confidence and market share, embarrassment to management and legal actions against an enterprise. Understanding the methods, techniques and exploits used to compromise an environment provides the IS auditor with a more complete context for understanding the risk that an enterprise faces.

Taking these techniques into consideration and understanding that they can be launched from any location allows for more thorough evaluations, ultimately providing more secure environments. The IS auditor should understand enough attack types to recognize their business risk and how they should be addressed by appropriate controls.

5.11.1 Fraud Risk Factors

Fraud is the crime of using dishonest methods to take something valuable from a person or organization. There can be many reasons a person commits fraud, but one widely accepted explanatory model is the fraud triangle (**figure 5.56**). Cressey identified three key elements in the fraud triangle:[46]

1. **Motivation**—Refers to a perceived financial (or other) need. The fraudster may be in debt, hold a personal grudge, have a problem with drugs or gambling, or want to enjoy status symbols such as a bigger house or car.
2. **Rationalization**—Refers to the way fraudsters justify crimes to themselves. Rationalizations may include thoughts such as, "I deserved the money," "I was only borrowing the money," "my family needs the money," "my employer has loads of money anyway," or "my employer treats me unfairly."
3. **Opportunity**—Refers to the method by which a crime is to be committed. Opportunity is created by abuse of position and authority, poor internal controls, poor management oversight, etc. Failure to establish procedures to detect fraud increases the likelihood of fraud occurring. Opportunity is the element over which organizations—and, by extension, IS auditors—have the most control. With respect to information assets, the opportunities to commit fraud can be limited by security controls that typically include logical access (including for third parties), SoD, human resources security, etc.

Figure 5.56—The Fraud Triangle



Source: Adapted from Association of Certified Fraud Examiners, "The Fraud Triangle," *https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud*

5.11.2 Computer Crime Issues and Exposures

Computer systems can be used to fraudulently obtain money, goods, software or enterprise information. Crimes can also be committed when a computer application process or data is manipulated to accept false or unauthorized transactions or when equipment is stolen.

Crimes that exploit the computer and the information it contains can be damaging to the reputation, morale and the continued existence of an organization. Loss of customers or market share, embarrassment to management and legal actions against the organization can result. Threats to business include:

- **Financial loss**—These losses can be direct, through loss of electronic funds, or indirect, through the costs of correcting the exposure.
- **Legal repercussions**—There are numerous privacy and human rights laws an organization should consider when developing security policies and procedures. These laws can protect the organization but also can protect the perpetrator from prosecution.

[46] See Association of Certified Fraud Examiners, "Fraud 101: What is Fraud," *https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud*, and "NANO SELF-STUDY: The Fraud Triangle," *https://www.acfe.com/training-events-and-products/all-products/product-detail-page?s=The-Fraud-Triangle*.

 ©ISACA. All Rights Reserved.

In addition, if a significant loss occurs from a security violation, not having proper security measures could expose the organization to lawsuits from investors and insurers. Most companies must comply with industry-specific regulatory agencies' requirements. The IS auditor should obtain legal assistance when reviewing the legal issues associated with computer security.

- **Loss of credibility or competitive edge**—Many organizations, especially service firms such as banks, savings and loans and investment firms, need credibility and public trust to maintain a competitive edge. A security violation can damage their credibility severely, resulting in loss of business and prestige.
- **Blackmail/industrial espionage/organized crime**—After gaining access to confidential information or the means to adversely impact computer operations, a perpetrator can extort payments or services from an organization by threatening to exploit the security breach or publicly disclose the confidential information of the organization. Also, by gaining access, the perpetrator can sometimes obtain proprietary information and sell it to a competitor.
- **Disclosure of confidential, sensitive or embarrassing information**—Disclosure of information not only threatens an organization's credibility and its means of conducting business, but also exposes it to possible legal or regulatory actions.
- **Sabotage**—Some perpetrators are not looking for financial gain. They merely want to cause damage due to a dislike of the organization or for self-gratification. Hacktivism occurs when perpetrators make nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends.

It is important that the IS auditor knows and understands the differences between computer crime and computer abuse to support risk analysis methodologies and related control practices. What constitutes a crime depends on the established law within a jurisdiction. Certain breaches of security may be civil or criminal offenses. This brings into play requirements for what the organization needs to do should a crime be suspected (i.e., protecting evidence, reporting the incident, etc.).

Perpetrators of computer crimes are often the same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex. Possible perpetrators include:

- **Hackers**—Persons with the ability to explore the details of programmable systems and the knowledge to stretch or exploit their capabilities, whether ethically or not. Hackers are typically attempting to test the limits of access restrictions to prove their ability to overcome obstacles. Some do not access a computer with the intent of destruction, although it is often the result. Hacktivists are a category of hackers. Most hackers do not seek to commit crimes through their actions but mainly hack systems to achieve some level of personal satisfaction.
- **Crackers**—Crackers are attackers who break into an organization's systems with malicious intentions, such as stealing or destroying data. They work the same way as hackers, but the major difference is that while the affected organization is mainly interested in the intruding hackers, law enforcement often targets crackers due to the illegality of their actions and the potentially fertile grounds for litigation. Crackers often acquire extensive knowledge of computer systems through learning various IS disciplines, such as programming, to breach organizational systems. The IS auditor should always assess the activities of hackers and crackers in the organization's systems and networks as the terms are mistakenly used interchangeably by many IT professionals and businesspeople.
- **Script kiddies**—Script kiddies refer to individuals who use scripts and programs written by others to perform their intrusions. They are often incapable of writing similar scripts on their own.
- **Employees (authorized or unauthorized)**—Affiliated with the organization and given system access based on job responsibilities, employees can cause significant harm to an organization. Screening prospective employees through appropriate background checks is an important means of preventing computer crimes within an organization.
- **IT personnel**—These individuals have the easiest access to computerized information, as they are its custodians. In addition to logical access controls, good SoD and supervision help in reducing logical access violations by employees.
- **End users**—End users often have broad knowledge of the information within the organization and have easy access to internal resources.
- **Former employees**—Former employees who have left on unfavorable terms may have access to systems if they are not immediately blocked at the time of termination or if the system has back doors.
- **Nations**—As more critical infrastructure is controlled from the Internet (e.g., SCADA systems) and more nation's key organizations and businesses rely on the Internet, it is not uncommon for nations to attack each other.

©ISACA. All Rights Reserved.

- **Interested or educated outsiders**—These may include:
  - Competitors
  - Terrorists
  - Organized criminals
  - Phreakers
- **Part-time and temporary personnel**—Facility contractors, such as office cleaners, often have a great deal of physical access and could perpetrate a computer crime.
- **Third parties**—Vendors, visitors, consultants or other third parties who, through projects, gain access to the organization's resources could perpetrate a crime.
- **Opportunists**—Opportunists take advantage of situations in which information or systems can be easily accessed.
- **Accidental unaware**—Someone who unknowingly perpetrates a violation.

Other examples of criminals include hacktivists, small-time crooks, members of organized crime and state-sponsored criminal groups.

Although collaboration has been improved in solving cybercrimes committed from one country to another, political issues existing between adversaries might hinder an investigation. Therefore, additional preventive measures should be taken to protect IS vulnerable to international attacks.

Figures 5.57 and **5.58** describe common attack methods and techniques for computer crimes. Perpetrators may use one or more methods in tandem to commit a crime.

Figure 5.57—Computer Crimes

Source of the Attack	Target of the Attack	Examples
Computer is the target of the crime. Perpetrator uses another computer to launch an attack.	A specific computer is identified and targeted.	• Denial of service (DoS) • Hacking
Computer is the subject of the crime. Perpetrator uses computer to commit crime and the target is another computer.	The target may or may not be defined. Perpetrator launches the attack with no specific target in mind.	• Distributed DoS • Malware
Computer is the tool of the crime. Perpetrator uses computer to commit crime, but the target is not the computer.	The target is data or information stored on a computer.	• Fraud • Unauthorized access • Phishing • Installing key loggers

Computer symbolizes the crime. Perpetrator lures a computer user to get confidential information.	The target is a computer user.	• Social engineering methods:
		  ▪ Phishing
		  ▪ Fake websites
		  ▪ Scam mail
		  ▪ Spam mail
		  ▪ Fake resumes for employment

Figure 5.58—Common Attack Methods and Techniques

Alteration attack	Occurs when unauthorized modifications affect the integrity of the data or code Examples: Unauthorized alteration of binary code during the software development life cycle (SDLC) or addition of unauthorized libraries during recompilation of existing programs Cryptographic hash is a primary defense against alteration attacks.

 ©ISACA. All Rights Reserved.

Figure 5.58—Common Attack Methods and Techniques (cont.)

Botnets	A collection of compromised computers (called zombie computers) running software, usually installed via worms, Trojan horses or back doors. Examples: DoS attacks, adware, spyware and spam
Denial of service (DoS) attack	Examples: Internet Control Message Protocol (ICMP) flood attack: • **Smurf attack**—Occurs when misconfigured network devices allow packets to be sent to all hosts on a particular network via the broadcast address of the network • **Ping flood**—Occurs when the target system is overwhelmed with ping packets • **SYN flood**—Sends a flood of Transmission Control Protocol (TCP)/SYN packets with a forged sender address, causing half-open connections, and saturates available connection capacity of the target machine • **Teardrop attack**—Involves sending mangled Internet Protocol (IP) fragments with overlapping, oversized payloads to the target machine • **Peer-to-peer attack**—Causes clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead. As a result, several thousand computers may aggressively try to connect to a target website, causing performance degradation. • **Permanent denial of service (PDoS) attack (also known as phlashing)**—Damages system hardware to the extent of requiring replacement Application-level flood attack: • **Buffer overflow**—Consumes available memory or central processing unit (CPU) time • **Brute-force attack**—Floods the target with an overwhelming flux of packets, oversaturating its connection bandwidth or depleting the target's system resources • **Bandwidth-saturating flood attack**—Relies on the attacker having higher bandwidth available than the victim • **Banana attack**—Redirects outgoing messages from the client back onto the client, preventing outside access and flooding the client with the sent packets • **Pulsing zombie**—A DoS attack in which a network is subjected to hostile pinging by different attack computers over an extended time period. This results in a degraded quality of service (QoS) and increased workload for the network's resources. • **Nuke**—A DoS attack against computer networks in which fragmented or invalid ICMP packets are sent to the target Modified ping utility is used to repeatedly send corrupt data, thus slowing the affected computer to a complete stop. • **Distributed denial of service attack (DDoS)**—Occurs when multiple compromised systems flood the bandwidth or resources of the targeted system • **Reflected attack**—Involves sending forged requests to a large number of computers that will reply to the requests. The source IP address is spoofed to that of the targeted victim, causing the replies to flood. • **Unintentional attack**—Website ends up denied, not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity.

©ISACA. All Rights Reserved.

Figure 5.58—Common Attack Methods and Techniques (cont.)

Eavesdropping	An intruder gathers the information flowing through the network with the intent of acquiring and releasing the message contents for either personal analysis or for third parties who might have commissioned such eavesdropping. This is significant when considering that sensitive information traversing a network can be seen in real time by all other machines, including email, passwords and, in some cases, keystrokes. Eavesdropping can enable the intruder to gain unauthorized access, to fraudulently use information such as credit card accounts and to compromise the confidentiality of sensitive information that could jeopardize or harm an individual's or an organization's reputation.
Phishing	This is the criminally fraudulent process of attempting to acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing techniques include social engineering, link manipulation and website forgery. Types of phishing include: • **Spear phishing**—A pinpoint attack against a subset of people (such as users of a website, members of an organization) to undermine that organization • **Whale-phishing**—Whale-phishing, sometimes known as whaling, is aptly named because it targets the leadership of the organization, which is typically members of the C-suite. These individuals possess valuable proprietary business information that is valuable to attackers. The IS auditor should note that if whale-phishing is performed though ransomware, a ransom is likely to be paid to guard against reputation risk. • **Smishing and vishing**—Smishing is a form of phishing that is carried out through text messages and is sometimes known as Short Message Service (SMS) phishing. Voice phishing, also known as vishing, is phishing perpetrated through phone calls. Smishing and vishing usually involve threat actors informing victims about their accounts having been frozen or a fraud detected. Out of panic, the victims usually divulge account information to the attacker. Armed with the information, the attacker is able to further perpetrate criminal activities.
Flooding	A DoS attack that brings down a network or service by flooding it with large amounts of traffic. The host's memory buffer is filled by flooding it with connections that cannot be completed.
Interrupt attack	Occurs when a malicious action is performed by invoking the OS to execute a particular system call Example: A boot sector virus typically issues an interrupt to execute a write to the boot sector.
Juice jacking	Occurs when malware is surreptitiously installed on, or data are copied from, a smartphone, tablet or other device using an often-public universal serial bus (USB) charging port that doubles as a data connection.

Figure 5.58—Common Attack Methods and Techniques (cont.)

Malicious code	• **Trojan horses (often called Trojans)**—Programs that are disguised as useful programs, such as operating system (OS) patches, software packages or games. Once executed, Trojans perform actions that the user did not intend, such as opening certain ports for subsequent access by the intruder. • **Logic bomb**—A program or a section of a program that is triggered when a certain condition, time or event occurs. Logic bombs typically result in sabotage of computer systems and are commonly deployed by disgruntled insiders who have access to programs. For example, when terminated from an organization, a disgruntled software programmer could devise a logic bomb to delete critical files or databases. Logic bombs can also be used against attackers. Administrators sometimes intentionally install pseudo flaws, also called honey tokens, that look vulnerable to attack but really act as alarms or triggers of automatic actions when the intruder attempts to exploit the flaw. • **Trap doors**—Commonly called back doors, trap doors are bits of code embedded in programs by programmers to quickly gain access during the testing or debugging phase. If an unscrupulous programmer purposely leaves in this code (or simply forgets to remove it), a potential security hole is introduced. Hackers often install a back door on previously compromised systems to gain subsequent access. Threat vector analysis (a type of defense-in-depth architecture), separation of duties (SoD) and code audits help to defend against logic bombs and trap/back doors.
Man-in-the-middle attack	Possible scenarios include: • The attacker actively establishes connections with two devices. The attacker connects to both devices and pretends to each of them to be the other device. Should the attacker's device be required to authenticate itself to one of the devices, it passes the authentication request to the other device and then sends the response back to the first device. Having achieved authentication in this way, the attacker can then freely interact with the device. To successfully execute this attack, both devices have to be connectable. • The attacker interferes while the devices are establishing a connection. During this process, the devices have to synchronize the hop sequence that is to be used. The aggressor can prevent this synchronization so that both devices use the same sequence but a different offset within the sequence.
Masquerading	An active attack in which the intruder presents an identity other than the original identity. The purpose is to gain access to sensitive data or computing/network resources to which access is not allowed under the original identity. Masquerading also attacks the authentication attribute by letting a genuine authentication session take place and subsequently entering the information flow, masquerading as one of the authenticated users of the session. Impersonation by both people and machines falls under this category. Masquerading by machines (also known as IP spoofing) occurs when a forged IP address is presented. This form of attack is often used as a means of breaking a firewall.
Message modification	Involves the capturing of a message and making unauthorized changes or deletions (of full streams or parts of the message), changing the sequence or delaying transmission of captured messages. This attack can have disastrous effects if the message is an instruction to a bank to make a payment, for example.

©ISACA. All Rights Reserved.

Figure 5.58—Common Attack Methods and Techniques (cont.)

Network analysis	An intruder applies a systematic and methodical approach known as footprinting to create a complete profile of an organization's network security infrastructure. During this initial reconnaissance phase, the intruder uses a combination of tools and techniques to build a repository of information about a particular company's internal network. This probably would include information about system aliases, functions, internal addresses and potential gateways and firewalls. Next, the intruder focuses on systems within the targeted address space that responded to the network queries. Once a system is targeted, the intruder scans the system's ports to determine what services and OS are running on the targeted system, possibly revealing vulnerabilities that could be exploited.
Packet replay	A combination of passive and active modes of attack. The intruder passively captures a stream of data packets as the stream moves along an unprotected or vulnerable network. These packets are then actively inserted into the network as if the stream were another genuine message stream. This form of attack is effective particularly if the receiving end of the communication channel is automated and will act on receipt and interpretation of information packets without human intervention.
Pharming	An attack that aims to redirect the traffic of a website to a bogus website. Pharming can be conducted either by changing the host's file on a victim's computer or by exploiting a vulnerability in Domain Name System (DNS) server software. DNS servers are computers responsible for resolving Internet names into their real addresses—they are the signposts of the Internet. Compromised DNS servers are sometimes referred to as poisoned. In recent years, both pharming and phishing have been used to steal identity information. Pharming has become a major concern to businesses hosting e-commerce operations and to online banking websites. Sophisticated measures known as ant pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming.
Piggybacking	The act of following an authorized person through a secured door or electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions. Piggybacking is considered a physical access exposure.
Race conditions (time of check [TOC]/time of use [TOU] attacks)	Exploit a small window of time between the time the security control is applied and the time the service is used. The exposure to a race condition increases in proportion to the time difference between TOC and TOU. Interference occurs when a device or system attempts to perform two or more operations at the same time, but the nature of the device or system requires the operations to happen in proper sequence. Race conditions occur due to interferences caused by: • **Sequence or nonatomic**—These conditions are caused by untrusted processes, such as those invoked by an attacker, that may get in between the steps of the secure program. • **Deadlock, livelock or locking failure**—These conditions are caused by trusted processes running the same program. Since these different processes may have the same privileges, they may interfere with each other if not properly controlled. Careful programming and good administration practices help to reduce race conditions.
Remote maintenance tools	If not securely configured and controlled, maintenance tools can be used by malicious hackers to remotely gain elevated access and cause damage to the target system.
Resource enumeration and browsing	An attacker's list of resources (names, directories, privileges, shares, policies) on targeted hosts and networks A browsing attack is a form of resource enumeration attack performed by a manual search, frequently aided with commands and tools available in software, OSs or add-on utilities

 ©ISACA. All Rights Reserved.

Figure 5.58—Common Attack Methods and Techniques (cont.)

Salami	Involves slicing small amounts of money from a computerized transaction or account, similar to the rounding down technique. The difference between the rounding down technique and the salami technique is that in rounding down, the program rounds off by the smallest monetary fraction. For example, in the rounding down technique, a US$1,235,954.39 transaction may be rounded to US$1,235,954.35. On the other hand, the salami technique truncates the last few digits from the transaction amount, so US$1,235,954.39 becomes US$1,235,954.30 or $1,235,954.00, depending on the algorithm/formula built into the program. In fact, other variations of the same technique are applied to rates and percentages.
Social engineering	The human side of breaking into a computer system. Organizations with strong technical security countermeasures (such as authentication processes, firewalls and encryption) may still fail to protect their information systems (IS). This situation may occur if an employee unknowingly gives away confidential information (e.g., passwords and IP addresses) by answering questions over the phone to someone they do not know or by replying to an email message from an unknown person. Some examples of social engineering include impersonation through a telephone call, dumpster diving and shoulder surfing. The best means of defense for social engineering is an ongoing security awareness program that educates all employees and third parties who have access to the organization's facilities about the risk involved in falling prey to social engineering attacks.
Injection attack	An injection attack takes advantage of websites that depend on databases in a client-server architecture. An injection attack typically uses a Structured Query Language (SQL) query from the client to a database that resides on the server. This command is inserted into data in place of a security solution such as a password or login. As the server that holds the database runs the command, the system is penetrated. Injection attacks lead to loss, deletion or modification of sensitive data. The attacker can execute system administrator operations that interfere with the proper functioning of the database.
Zero-day exploit	A zero-day exploit is a type of attack that exploits a previously unknown vulnerability. Attackers typically learn of the existence of a vulnerability in widely used software prior to its fix becoming available and target organizations using that software. This is a major risk because it usually cannot be prevented; in fact, antivirus solutions are not effective against zero-day exploits because they are unknown. Implementing a continuous patch management process, maintaining updated software and sandboxing assist in addressing zero-day exploits, while a regularly updated incident response plan (IRP) assists in quick recovery from zero-day exploits.
Cryptojacking	Cryptojacking is a form of attack in which attackers take control of a user's computer or device for the purpose of mining cryptocurrencies such as Bitcoin. This is a new method of attack that is usually carried out without the victim being aware. In organizations where there is not much visibility into the network, criminals can control the whole network to mine cryptocurrencies. To address this risk, organizations need to regularly monitor the CPU usage of all network devices and train employees to be alert to any performance issues or suspicious emails that may contain cryptojacking malware.
Cross-site scripting (XSS)	XSS is an attack in which scripts are used to infect users who visit a website or to redirect users to a malicious website. It is a complex attack vector that requires a basic understanding of web development concepts and technologies, such as HyperText Markup Language (HTML) and JavaScript. However, and typically important for the IS auditor, the techniques that are used to prevent XSS attacks are the same as those that are used to prevent SQL injection attacks. Most importantly, the organization should ensure input validation and sanitization to ensure that attackers cannot inject malicious scripts into web pages.

©ISACA. All Rights Reserved.

Figure 5.58—Common Attack Methods and Techniques (cont.)

Cross-site request forgery (CSRF)	CSRF is an attack that forces the victim to execute unwanted actions on a web application in which they are currently authenticated. It usually employs a social engineering process, such as sending a link through a chat platform. This allows the attacker to trick the user into executing the attacker's preferred actions. If the victim is a general user, a successful CSRF attack can force users to perform system state changing requests, such as transferring funds or changing their email addresses. If the victim is an administrative account, CSRF can compromise the entire web application and render it unsafe to use.
DNS tunneling	DNS tunneling is a form of attack vector that is designed to provide attackers with persistent access to a given target. It is particularly important to IS auditors because the attack is usually successful—many organizations fail to monitor DNS traffic for malicious activity. This enables attackers to insert or "tunnel" malware into DNS queries. The malware is designed to create a persistent communication channel that most firewalls will fail to detect. To address this type of attack, organizations should ensure that they employ tools that can automatically block the execution of malware contained in malicious DNS queries, denylist all destinations known to be used for data exfiltration and provide real-time analysis of all DNS queries to determine suspicious patterns.
URL poisoning	This type of attack is sometimes known as URL interpretation. With this attack, attackers alter and fabricate certain URL addresses, which they then use to gain access to the target's personal and professional data. This kind of attack is also referred to as URL poisoning. To successfully carry out a URL interpretation attack, an attacker may guess URLs to get administrator privileges to a site or to access the site's back end to get into a user's account. After reaching the required page, the attacker can then manipulate the site itself or gain access to sensitive information about the people who use the site. To address URL interpretation attacks, the IS auditor should advise on the use of secure authentication methods such as MFA for any sensitive areas of the website.
DNS spoofing	With DNS spoofing, an attacker alters DNS records to send traffic to a fake website with the expectation that once on the fraudulent site, the victim may enter sensitive information thinking that the website is legitimate. The fake website is sometimes known as the spoofed website. The sensitive information is then used by the attacker for nefarious purposes, even to commit crimes in the name of the organization. Another method that may be employed by an attacker in DNS spoofing is to construct a poor-quality site, which make the organization look bad. To address DNS spoofing, DNS servers should always be kept up to date, as the most recent software versions often contain fixes that address known vulnerabilities.
Traffic analysis	An inference attack technique that studies the communication patterns between entities in a system and deduces information. This typically is used when messages are encrypted, and eavesdropping would not yield meaningful results. Traffic analysis can be performed in the context of military intelligence or counterintelligence and is a concern in computer security.

Figure 5.58—Common Attack Methods and Techniques (cont.)

Unauthorized access through the Internet or web-based services	Many Internet software packages contain vulnerabilities that render systems subject to attack. Additionally, many systems are large and difficult to configure, resulting in many unauthorized access incidents. Examples include: • Email forgery (Simple Mail Transfer Protocol) • Telnet passwords transmitted in the clear (via path between client and server) • Alteration of the binding between IP addresses and domain names to impersonate any type of server. If the DNS is vulnerable and used to map URLs to sites, there can be no integrity on the Web. • Release of common gateway interface (CGI) scripts as shareware. CGI scripts often run with privileges that give them complete control of a server. • Client-side execution of scripts (via Java in Java applets), which presents the danger of running code from an arbitrary location on a client machine.
Viruses, worms and spyware/ malware	• Viruses involve the insertion of malicious program code into other executable code that can self-replicate and spread from computer to computer, via sharing of removable computer media, USB removable devices, transfer of logic over telecommunication lines or direct link with an infected machine/code. A virus can harmlessly display cute messages on computer terminals, dangerously erase or alter computer files, or simply fill computer memory with junk to a point where the computer can no longer function. An added danger is that a virus may lie dormant for some time until triggered by a certain event or occurrence, such as a date or being copied a prespecified number of times, during which time the virus has silently been spreading. • Worms are destructive programs that may destroy data or use up tremendous computer and communication resources, but worms do not replicate like viruses. Such programs do not change other programs but can run independently and travel from machine to machine across network connections by exploiting vulnerabilities and application/system weaknesses. Worms also may have portions of themselves running on many different machines. • Spyware/malware is similar to viruses. Examples are keystroke loggers and system analyzers that collect potentially sensitive information, such as credit card numbers, bank details, etc., from the host and then transmit the information to the originator when an online connection is detected.

5.11.3 Internet Threats and Security

The Internet poses significant security problems for organizations seeking to protect their information assets. For example, hackers and virus writers try to attack the Internet and computers connected to the Internet. Some want to invade others' privacy and attempt to crack into databases of sensitive information or sniff information as they travel across Internet routes. Consequently, it is important for IS auditors to understand the risk and security factors that are needed to ensure that proper controls are in place when a company connects to the Internet.

The IP is designed solely for the addressing and routing of data packets across a network. It does not guarantee or provide evidence of the delivery of messages; there is no verification of an address; the sender will not know if the message reaches its destination at the time it is required; the receiver does not know if the message came from the address specified as the return address in the packet. Other protocols correct some of these drawbacks.

Network Security Threats

One class of network attacks involves probing network information. These passive attacks can lead to actual active attacks or intrusions/penetrations into an organization's network. By probing for network information, the intruder obtains network information that can be used to target a particular system or set of systems during an actual attack.

Passive Attacks

Examples of passive attacks that gather network information include network analysis, eavesdropping and traffic analysis as explained in **figure 5.58**.

©ISACA. All Rights Reserved.

Active Attacks

Once enough network information has been gathered, the intruder will launch an actual attack against a targeted system to either gain complete control over the system or enough control to cause certain threats to be realized. This may include obtaining unauthorized access to modify data or programs, causing a DoS, escalating privileges, accessing other systems, and obtaining sensitive information for personal gain. These types of penetrations or intrusions are known as active attacks. They affect the integrity, availability and authentication attributes of network security. Common forms of active attacks (explained in **figure 5.58**) may include:

- Brute-force attack
- Masquerading
- Packet replay
- Phishing
- Message modification
- Unauthorized access through the Internet
- DoS
- Remote access penetration attacks
- Email bombing and spamming
- Email spoofing

Causal Factors for Internet Attacks

Generally, Internet attacks of both a passive and active nature occur for a number of reasons, including:

- Availability of tools and techniques on the Internet or as commercially available software that an intruder can download easily. For example, to scan ports, an intruder can easily obtain network scanners such as strobe, netcat, jakal, nmap or Asmodeous (Windows). Additionally, password-cracking programs, such as John the Ripper and L0phtCrack, are available free or at a minimal cost.
- Lack of security awareness and training among an organization's employees
- Exploitation of known security vulnerabilities in network- and host-based systems. Many organizations fail to properly configure their systems and to apply security patches or fixes when vulnerabilities are discovered. Most problems can be reduced significantly by keeping network- and host-based systems properly configured and up to date.
- Inadequate security over firewalls and host-based OSs, allowing intruders to view internal addresses and use network services indiscriminately

With careful consideration when designing and developing network security controls and supporting processes, an organization can effectively prevent and detect most intrusive attacks on its networks. In this situation, it becomes important for IS auditors to understand both the risk and the security factors needed to ensure proper controls are in place when a company connects to the Internet. There are several areas of control risk that must be evaluated by the IS auditor to determine the adequacy of Internet security controls.

Targeted Attacks

In a targeted attack, attackers launch an attack on a specific organization to compromise its security and steal its data. This type of attack consists of multiple-level attacks initiated through malware that was specifically written to get entry into an organization's systems. After the malware is installed, it creates a back door and communicates with the attacker. The attacker tries to conceal evidence of the attack to avoid detection. Using this malware, the attacker then traverses the system to understand its contents and begins to send sensitive data out of the system through a back door that the malware created. This attack continues for a sustained period of time. After enough data is compromised, the breach is exposed.

Organizations must monitor systems continuously to identify indicators of compromise, including outgoing traffic (egress monitoring), dummy user accounts, etc. Preventive controls include baselining, hardening, exception monitoring, endpoint controls, etc.

The OWASP Top 10

The Open Web Application Security Project (OWASP) developed several resources regarding the common vulnerabilities that exist in various systems, including web applications, APIs and mobile devices. The OWASP Top Ten describes the 10 most common and impactful vulnerabilities that appear in production web applications.[47]

5.11.4 Malware

The term malware is generally applied to a variety of malicious computer programs that send out requests to the OS of the host system under attack to append the malware to other programs. In this way, malware is self-propagating to other programs. The malware can be relatively benign (e.g., web application defacement) or malicious (e.g., deleting files, corrupting programs or

[47] OWASP Foundation, "OWASP Top Ten," *https://owasp.org/www-project-top-ten/*

causing a DoS). Generally, malware attacks four parts of the computer:

- Executable program files
- The file-directory system, which tracks the location of all the computer's files
- Boot and system areas, which are needed to start the computer
- Data files

Types of malware include ransomware, worms, viruses, adware, spyware, rootkits, etc. A variant of malware frequently encountered is a worm, which, unlike a virus, does not physically attach itself to another program. To propagate itself to host systems, a worm typically exploits security weaknesses in OS configurations. Worms are particularly severe problems in highly decentralized client-server environments. Currently, viruses or worms are transmitted easily from the Internet by downloading files to computers' web browsers. Malware is also transmitted as attachments to email, so that when an attachment opens, the system becomes infected if it is not using scanning software to review unopened attachments. Other methods of infection occur from files received through online services, social media, LANs and even shrinkwrapped software the user may buy from a retail store.

Virus and Worm Controls

To effectively reduce the risk of computer viruses and worms infiltrating an organization, a comprehensive and dynamic antimalware program needs to be established. There are two major ways to prevent and detect malware that infect computers and network systems. The first is by having sound policies and procedures (preventive controls) and the second is by technical means (detective controls), including antimalware software. Neither is effective without the other.

Management Procedural Controls

Some of the policy and procedural controls that should be in place include:

- Build systems from original clean master copies. Boot only from original media whose write protection has always been in place, if applicable.
- Allow no media (e.g., hard/flash drives) to be used until they have been scanned on a standalone machine that is used for no other purpose and is not connected to the network.
- Update malware software scanning definitions/ signatures frequently.
- Protect removable media against theft and hazards.
- Have vendors run demonstrations on their own machines.
- Enforce a rule of not using shareware without first scanning it thoroughly for malware.
- Scan before any new software is installed because commercial software occasionally includes a Trojan horse (viruses or worms).
- Insist that field technicians scan their disks on a test machine before they use any of their disks on the system.
- Ensure the network administrator uses workstation and server antimalware software.
- Ensure all servers are equipped with an activated current release of the malware-detection software.
- Consider encrypting files and then decrypting them before execution.
- Ensure bridge, router and gateway updates are authentic.
- Because backups are a vital element of an antimalware strategy, ensure a sound and effective backup plan is in place. This plan should account for scanning selected backup files for malware infection once malware has been detected.
- Educate users so they will heed policies and procedures. For example, many types of malware are propagated in the form of an email attachment, such as an executable Visual Basic script, that infects the system once the user opens it. The attacker relies upon social engineering tactics to get users to open such attachments.
- Review antimalware policies and procedures at least once a year.
- Prepare a malware eradication procedure and identify a contact person.
- Develop, rehearse and maintain clear incident management procedures in the event that antimalware software reports an infection.

Technical Controls

Technical methods of preventing malware can be implemented through hardware and software means. Some hardware tactics that can reduce the risk of infection:

- Use boot malware protection (i.e., built-in, firmware-based malware protection).
- Use remote booting (e.g., diskless workstations).
- Use a hardware-based password.
- Protect removable media against theft and hazards.
- Ensure that insecure protocols are blocked by the firewall from external segments and the Internet.

However, antimalware software is, by far, the most common antimalware tool and is considered the

©ISACA. All Rights Reserved.

most effective means of protecting networks and host-based computer systems against malware. Antimalware software is both a preventive and detective control. Unless updated periodically, antimalware software will not be an effective tool against malware.

Antimalware software contains a number of components that address the detection of malware via scanning technologies from different angles. There are different types of antimalware software.

Scanners look for sequences of bits called signatures that are typical of malware programs. The two primary types are:

- **Malware masks or signatures**—Antimalware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signatures are specific code strings that are recognized as belonging to malware. For polymorphic viruses, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.
- **Heuristic scanners**— Heuristic scanners analyze the instructions in the code being scanned and decide on the basis of statistical probability whether malicious code could be present. Heuristic scanning results indicate that malware could be present (i.e., the code is possibly infected). However, heuristic scanners tend to generate a high level of false-positive errors (i.e., they indicate that malware may be present when, in fact, no malware is present).

Scanners examine memory, disk-boot sectors, executables, data files and command files for bit patterns that match known malware. Scanners need to be updated periodically to remain effective.

Active monitors interpret command line and read-only memory (ROM) basic input/output system (BIOS) calls, looking for malware-like actions. Active monitors can be problematic because they cannot distinguish between a user request and a program or malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

Integrity cyclic redundancy check (CRC) checkers compute a binary number on a known malware-free program that is then stored in a database file. On subsequent scans, when that program is called to execute, it checks for changes to the files as compared to the database and reports possible infection if changes have occurred. A match means no infection; a mismatch means a change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred (i.e., it is often too late to save files). Also, CRC checkers can only detect subsequent changes to files because they assume files are malware-free in the first place. Therefore, they are ineffective against new files that are malware-infected and that are not recorded in the database. Integrity checkers take advantage of the fact that executable programs and boot sectors do not change often, if at all.

Behavior blockers focus on detecting potentially abnormal behavior, such as writing to the boot sector or the master boot record or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware-based antimalware mechanisms are based on this concept.

Immunizers defend against malware by appending sections of themselves to files—somewhat in the same way that file malware appends itself. Immunizers continuously check the file for changes and report changes as possible malware behavior. Other types of immunizers focus on a specific virus and work by giving the malware the impression that it has already infected the computer. This method is not always practical because it is not possible to immunize files against all known malware.

Once malware has been detected by antimalware software, an eradication program can be used to wipe the malware from the hard disk. Sometimes eradication programs can kill the malware without having to delete the infected program or data file, while other times those infected files must be deleted. Other programs, sometimes called inoculators, do not allow a program to be run if it contains malware.

Antimalware Software Implementation Strategies

Organizations have to develop malware implementation strategies to effectively control and prevent the spread of malware throughout the IS infrastructure. An important means of controlling the spread of malware is to detect it at its point of entry—before it can cause damage. This includes everything from networks, server platforms and end-user workstations.

The user server or workstation level could include screening of software and data as it enters the machine. Antimalware programs can be set to perform:

- Scheduled malware scans (e.g., daily, weekly, etc.)
- Manual/on-demand scans, if the malware scan is requested by the user

 ©ISACA. All Rights Reserved.

- Continuous/on-the-fly scanning, with files scanned as they are processed. At the corporate network level, in cases of interconnected networks, malware scanning software is used as an integral part of firewall technologies and referred to as malware walls. Malware walls scan incoming traffic with the intent of detecting and removing malware before it enters the protected network.

Malware walls normally work at three levels:

1. SMTP protection, to scan inbound and outbound SMTP traffic for malware in coordination with the mail server
2. HTTP protection, to prevent malware-infected files from being downloaded and to offer protection against malicious Java and ActiveX programs
3. FTP protection, to prevent infected files from being downloaded

Malware walls are updated automatically with new malware signatures on a scheduled or on an as-needed basis when new malware emerges. Malware walls enable organizations to log malware incidents and deal with them in accordance with preset rules. This does not preclude the need for malware-detection software because the malware wall only addresses one channel through which malware enters the network.

For malware scanners to be acceptable and viable, their feature sets should include:

- Reliability and quality in the detection of malware
- Resident memory, which is a continuous checking facility
- Efficiency, such as a reasonable working speed and use of resources

5.11.5 Ransomware

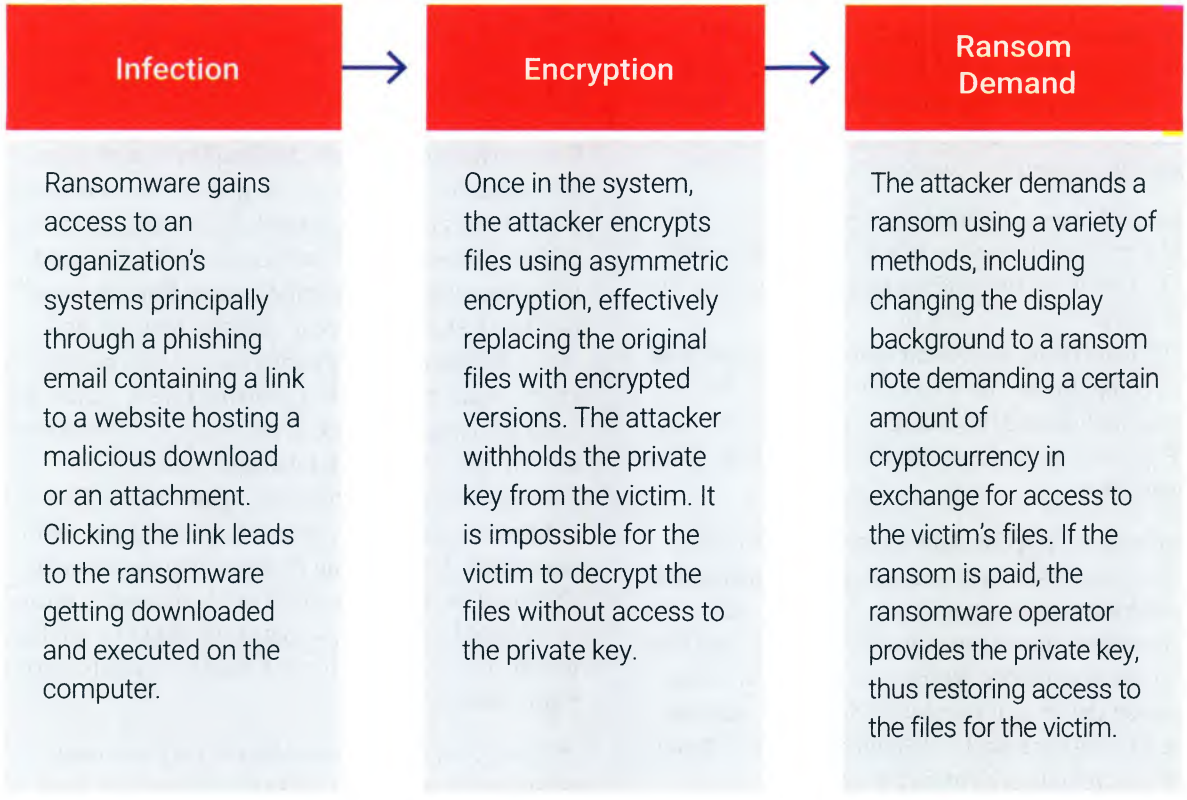
Ransomware is malware that employs encryption techniques to hold a victim's information at ransom. It works by accessing a target system and encrypting critical data so the user cannot access it. A ransom is then demanded to provide access. Ransomware[48] is often designed to spread across a network and target database and file servers to quickly paralyze an entire organization. It is a growing threat, generating huge amounts of money in payments to cybercriminals and inflicting significant damages and expenses on businesses and governmental organizations. Examples of ransomware include WannaCry and Maze. With ransomware, in addition to requesting a ransom to decrypt data, the threat actor might demand a ransom to withhold the release of sensitive data to a public forum. This is sometimes referred to as double extortion ransomware.

While the implementation details vary from one ransomware variant to another, all share the same core three stages as shown in **figure 5.59**.

[48] National Institute of Standards and Technology, *NIST IR 8374: Ransomware Risk Management: A Cybersecurity Framework Profile*, USA, 2022, *https://csrc.nist.gov/pubs/ir/8374/final*

©ISACA. All Rights Reserved.

Figure 5.59—Stages of a Ransomware Attack



Best practices to secure an organization against ransomware include:

- **Use secure networks**—Employees should avoid public Wi-Fi networks, as most of them are not secure. Criminals can snoop on Internet usage. Instead, consider installing a VPN, which provides the organization with a secure connection to the Internet anywhere the employees will be.
- **Continuous data backups**—Automated, protected data backups enable an organization to recover from an attack with a minimum of data loss and without paying a ransom. Maintaining regular backups of data as a routine process is a very important practice to prevent loss of data and help organizations recover from ransomware attacks.
- **Secure data backups**—Backup data should not be accessible for modification or deletion from the systems where the data resides. Ransomware will look for data backups and encrypt or delete them so they cannot be recovered (immutability). Organizations should use backup systems that do not allow direct access to backup files.
- **Effective patch management**—Attackers typically target the latest unpatched exploits in the patches made available and then target systems that are not yet patched. It is critical that organizations ensure that all systems have the latest patches applied to reduce the number of potential vulnerabilities for an attacker to exploit.
- **Strong authentication**—Accessing services like Remote Desktop Protocol (RDP) with stolen user credentials is a favorite technique of ransomware attackers. The use of strong user authentication can make it harder for an attacker to use a guessed or stolen password.
- **Minimal attack surface**—With the high potential cost of a ransomware infection, prevention is the best ransomware mitigation strategy. Prevention can be achieved by reducing the attack surface through use of antiransomware solutions.
- **Antiransomware solution**—The need to encrypt all of a user's files means that ransomware has a unique fingerprint when running on a system. Antiransomware solutions are built to identify those fingerprints.

Mitigating Active Ransomware Infections

Many successful ransomware attacks are only detected after data encryption is complete and a ransom note has been displayed on the infected computer's screen. At that

point, the encrypted files are likely unrecoverable, but it is advisable to immediately:

- **Quarantine the machine**—Some ransomware variants attempt to spread to connected drives and other machines in the organizational network. The organization can limit the spread by disabling access to other potential targets.
- **Contain the spread**—A ransomware attack often spreads quickly in the network and across networks. Immediate isolation of the infected device may not be very effective, as the ransomware can still be inside the networks. All devices behaving suspiciously should be disconnected from the network. Disconnecting the entire network (not just suspicious devices or systems) may eventually limit the ransomware's scope.
- **Do not switch off the system**—Encryption of files due to ransomware malicious actions may cause instability in the organization's systems. Switching off the systems during ransomware spread and lead to loss of volatile memory. Therefore, all systems should be kept on to preserve volatile memory and increase probability of recovery.
- **Create a backup**—There are some ransomware variants that can be decrypted without paying ransoms. The organization should just make a copy of the encrypted files and store them on secure removable media in case the ransomware solution becomes available without a ransom payment.
- **Check for decryptors**—Some organizations working to fight ransomware keep decryptors of various types of ransomware. The organization should just check to see if it can find a free decryptor available. It if is available, it should be run on the encrypted file to check if it can decrypt it.
- **Locate patient zero**—Patient zero in information security refers to an organization that is alerted to a suspected security breach. The reason for locating patient zero is to discover the initial point of attack in order to isolate the source of the attack. Ransomware tracking is easier when the source is identified. The organization should check all notifications and alerts that come from its defensive technology infrastructure.
- **Wipe and restore**—It is good practice to restore the system under attack from a clean backup or operating system installation as it ensures that the ransomware is completely removed from the system and/or device.
- **Report to authorities**—Ransomware is against the law in many jurisdictions and should be reported to law enforcement agents as soon as possible. In addition, ransomware attacks may have compliance implications.

Ethical Considerations for Ransomware

Theoretically, most law enforcement agencies urge organizations not to pay ransomware attackers, as it is considered criminal and encourages attackers to create more ransomware. However, this advice is rarely followed. Most organizations conduct a cost-benefit analysis of the price of a ransom against the value of the encrypted data and plan for potential payment. In addition to funding criminal activities, paying ransoms has other downsides. Attackers may fail to provide a decryption key after the organization makes the ransom payment, or the decryption key provided may not work.

5.12 Security Testing Tools and Techniques

Security testing is a process that is performed to reveal flaws and vulnerabilities in information systems. IS auditors should underscore the importance of security testing to avoid loss of customer confidence, disturbances to organization systems and related compliance complications in the organization. The results of security testing should lead to improvement in the systems' security architectures.

5.12.1 Objectives of Security Testing

The main objectives of security testing are:

- **Identification of assets**—Security testing pinpoints assets that need to be protected, such as software applications and other computing infrastructure. It determines whether they are protected from malicious actors.
- **Identification of threats and vulnerabilities**—Security testing identifies threats that can cause damage to systems and weaknesses that can be exploited by threat actors.
- **Identification of risk**—Another objective of security testing is to evaluate the risk that specific threats or vulnerabilities pose to the organization. Risk is determined from an evaluation of the severity of a threat or the vulnerability, likelihood and impact of exploitation.
- **Performance of remediation**—In addition to an evaluation of systems, which is a passive exercise, security testing is proactive in nature. It provides insights on remediating vulnerabilities and ensuring they are addressed.

©ISACA. All Rights Reserved.

- **Evaluation of the strength of assets and controls**—Security testing helps the organization to evaluate the security strength of its IS infrastructure and the controls in place to address risk.
- **Adherence to security principles**—A further objective of security testing is to ensure that an organization's IS infrastructure adheres to the security principles of confidentiality, integrity, authentication, authorization, availability and nonrepudiation.

5.12.2 Security Assessments and Security Audits

The IS auditor should be able to distinguish between security assessments and security audit as used in the information security fraternity. This enables a common understanding of the terms and what is generally expected from each procedure.

- **Security assessments**—A security risk assessment is a method of identifying, evaluating and prioritizing potential vulnerabilities and threats and their possible impacts to determine whether and how to implement security controls. An assessment can be both quantitative and qualitative. After the assessment, the team decides on the controls to be implemented. Security assessments can be performed at any time and cover any part of the organization's IS infrastructure. The main objectives of security risk assessments include:
  - Identify assets and their value and create risk profiles for each asset.
  - Assess asset criticality and sensitivity and rank and prioritize assets.
  - Identify vulnerabilities and threats to assets.
  - Quantify the probability and business impact of potential threats.
  - Provide an economic balance between the impact of a threat and the cost of a countermeasure.
  - Enable management to make informed decisions on the organization's security efforts.
  - Indicate areas in which employees require awareness and training to deal with security threats.
  - Apply mitigating security controls to reduce risk to an acceptable level.
- **Security audits**—A security audit is a process of reviewing an organization's security practices against a recognized and published standard or framework. It involves reviewing security audit logs within IS systems to ensure they can effectively support information security goals. It should be clear to the IS auditor that a security audit does not typically test information security in an organization but just indicates the extent of compliance with standards. Some audits are simply carried out internally for self-reporting purposes, while others may involve the use of a third party or consultant. An organization may be audited for compliance with security standards such as Payment Card Industry Data Security Standard (PCI DSS), ISO/IEC 27002 or Health Insurance Portability and Accountability Act (HIPAA). The goal is to measure an organization's level of compliance with a particular security standard.

5.12.3 Vulnerability Assessments

IS auditors can use different techniques to identify potential threats, measure the likelihood of exploitation and gauge the overall IS threats facing the organization's IS infrastructure. The results of the assessments are used to address security weaknesses and minimize security risk. One of the most common techniques is vulnerability assessment. Also known as vulnerability scanning, a vulnerability assessment is undertaken for the purpose of identifying vulnerabilities in a target system. It is typically carried out by trustworthy information security experts with a high level of skills and extensive information security experience. IS auditors should consider the results of vulnerability assessments in their procedures or carry out some tests themselves. As the environment changes, new vulnerabilities can arise, and the result may not be up to date. The goals of vulnerability assessments are:

- Evaluate the security posture of the organization.
- Identify, evaluate and prioritize vulnerabilities.
- Assess the reaction of the information security environment to vulnerabilities and attacks.
- Learn about the vulnerabilities currently present.
- Identify ways vulnerabilities can be exploited by attackers.
- Decide on controls to implement to address the vulnerabilities.

5.12.4 Penetration Tests

Penetration tests, intrusion tests and ethical hacking are procedures in which an IS auditor uses the same techniques as a hacker. These are effective methods of identifying the real-time risk to an information processing environment. During penetration testing, an auditor attempts to circumvent the security features of a system and exploits the vulnerabilities to gain access that would otherwise be unauthorized. An IS auditor who is part of the team intending to carry out a penetration test should first make sure prior permission has been obtained from management before undertaking the penetration

test; otherwise, the whole test may be considered illegal. In penetration testing, the tester (commonly called the pen tester) identifies one or more vulnerabilities and then proceeds to exploit them by simulating attacks on a network using a set of procedures, tools and technologies that attackers would typically use to bypass an organization's security defenses to detect weaknesses and assess the organization's resilience to attacks. There are two methods generally used to conduct penetration testing activities in organizations:

1. **Manual penetration testing**—This type of penetration testing is conducted by humans who are experts in information security. It typically involves the application of tools that must be run manually, with the results provided at specified points. The results combine insights and can vary each time depending on the type of tool used and the kind of attack vector targeted. Manual penetration testing is generally time-consuming and cumbersome for the tester. The benefit of manual penetration testing is that it provides a comprehensive assessment of the entire attack surface. There also is a real possibility of discovering hidden vulnerabilities that cannot be discovered by automated penetration testing tools.
2. **Automated penetration testing**—Automated penetration testing involves the application of tools that require very little to no human interaction. Anyone, including learners, can perform it as everything involved in the testing is automated. The only requirement is for the tester to have knowledge about the test configuration. Once the test is appropriately configured, all the tools will be available, and the results will be provided in the form of a report at the end of the test. Automated penetration testing provides fixed results because only a fixed set of predefined tests are run, and only the associated attack vectors are tested. Automated penetration testing is faster and more efficient than manual penetration testing. The results are not very reliable, however, as only a portion of the attack surface is subject to testing. An IS auditor should keep in mind that the results of automated penetration testing will ordinarily need to be analyzed manually.

Scope can vary based on the agreed-on terms, conditions and other requirements. From an audit risk perspective, the audit scope should clearly address:

- Precise IP addresses/ranges to be tested
- Restricted hosts (i.e., hosts not to be tested)
- Acceptable testing techniques (e.g., social engineering, DoS/DDoS, SQL injections, etc.)
- Management acceptance of proposed methodology
- Timing of attack simulation (e.g., business hours, off hours, etc.)
- IP addresses of the source of attack simulation (to identify between approved simulated attack and actual attack)
- Point of contact for both the penetration tester/auditor and the targeted system owner/administrator
- Handling of information collected by the penetration tester/auditor (e.g., nondisclosure agreement [NDA] or reference to standard rules of engagement)
- Warning notification from penetration tester/auditor before the simulation begins to avoid false alarms to law enforcement bodies

Phases of Penetration testing

The phases of penetration testing appear in **figure 5.60** and the corresponding procedures in **figure 5.61**. Penetration testing is intended to mimic an experienced attacker intruding on a live site. It should only be performed by experienced and qualified professionals who are aware of the risk of undertaking such work and capable of limiting the damage resulting from a successful break-in on a live site (e.g., avoidance of DoS attacks).

©ISACA. All Rights Reserved.

Figure 5.60—Penetration Testing Phases

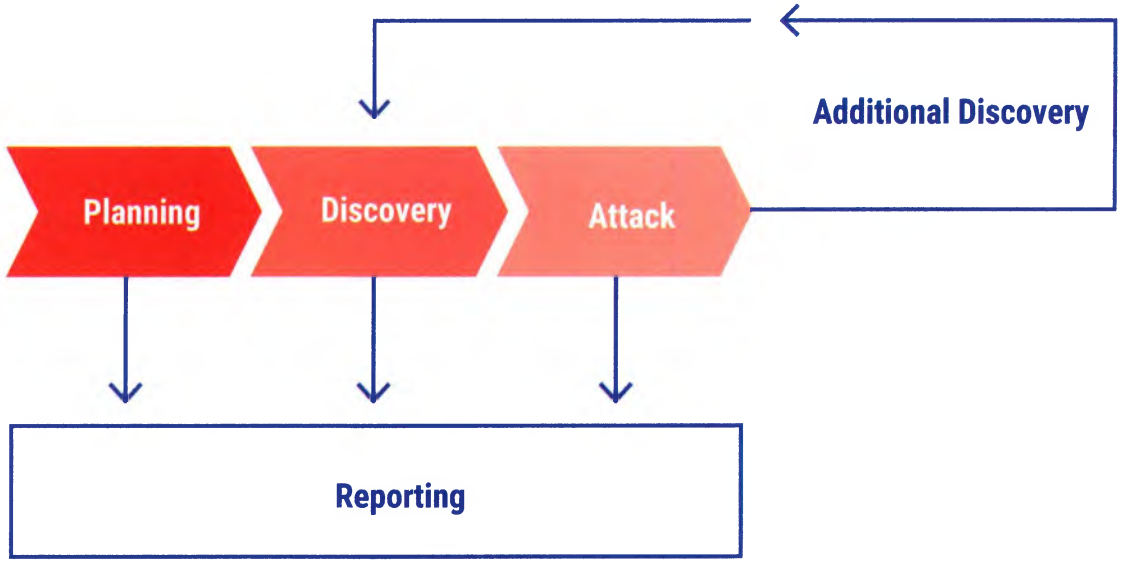


Figure 5.61—Penetration Testing Phases and Procedures

Planning	• Rules of engagement • Management approval/finalization • Testing methodology adopted • Intrusive or nonintrusive testing • Goals/objectives identified and agreed upon • Timelines/deadlines agreed upon • Milestones identified • Assignment time-tracking technique understood and communicated • Deliverables agreed upon • Tools collected/installed/tested in a test environment

 ©ISACA. All Rights Reserved.

Figure 5.61—Penetration Testing Phases and Procedures (cont.)

Reconnaissance/discovery	• Network mapping • Domain Name System (DNS) interrogation • WHOIS queries • Searching target's website for information • Searching target's related data on search engines • Searching target's related data and employees on social media (reveals system-related details) • Searching resume/curriculum vitae of target's current and formal employees (reveals system-related details) • Packet capture/sniffing (during internal testing only) • Host detection (Internet Control Message Protocol [ICMP], DNS, WHOIS, PingSweep, Transmission Control Protocol [TCP]/User Datagram Protocol [UDP] Sweep, etc.) • Service detection (port scanning, stealth scanning, error/banner detection, etc.) • Network topology detection (ICMP, etc.) • OS detection (TCP stack analysis, etc.) • Website mapping • Web page analysis • Unused pages/scripts • Broken links • Hidden links/files accessible • Application logic/use • Points of input error page banner grabbing • Vulnerability classification (based on using available search engines or custom-built repositories using previously collected information) Some of the attack techniques are: • Directory browsing • Show code • Error injection • Type and bound checks on input
Attacks	• Special character injection (meta-characters, escape characters, etc.) • Cookie/session IDs analysis • Authentication circumvention • Long input • System functions (shell escapes, etc.) • Logic altération (Structured Query Language [SQL] injection, etc.) • Cookie/session IDs manipulation • Internet service exploits (bind, mdac, unicode, apache-http, statd, sadmind, etc.) • OS exploits • Network exploits (SYN flooding, ICMP redirects, DNS poisoning, etc.) Once an attack is successful, it typically follows these subprocedures of an attack phase: • **Privilege escalation**—If only a user-level access was gained, then the tester will attempt to obtain super-level access (i.e., root on Unix/Linux and administrator on Windows). • **Information gathering from inside**—The attacker will probe further systems on the network to efficiently utilize the compromised system as a launch pad and thereby attempt to gain access to trusted/high-risk systems. • **Installation of further attack tools inside the system**—The attacker may require installation of additional tools and penetration testing software to gain further access to the resources, trusted or high-risk systems.

©ISACA. All Rights Reserved.

Figure 5.61—Penetration Testing Phases and Procedures (cont.)

Reporting	This phase simultaneously occurs with the other three phases. In the planning phase, rules of engagement, written consent and test plans are developed, discussed and reported. In the discovery phase, written logs are kept and periodic reports on the status of assignment are reported to management, as appropriate. Following the attack phase, the vulnerabilities and weaknesses discovered are reported with a risk rating based on probability derived from ease of exploitation and impact derived from attack results or official advisories and resources from the vendor. In addition, the recommendations contain steps to mitigate the risk and to effectively rectify the weaknesses.

There are several types of penetration tests depending on the scope, objective and nature of the test. Common types of penetration tests are:

- **External testing**—Refers to attacks and control circumvention attempts on the target's network perimeter from outside the target's system (i.e., usually the Internet).
- **Internal testing**—Refers to attacks and control circumvention attempts on the target from within the perimeter. The objective is to identify what would occur if the external network perimeter were successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on the network.
- **Blind testing**—Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such testing is expensive, because penetration testers have to research the target and profile it based on publicly available information only.
- **Double blind testing**—Refers to an extension of blind testing because the administrator and security staff at the target are also not aware of the test. Such testing can effectively evaluate the incident handling and response capability of the target.
- **Targeted testing**—Refers to attacks and control circumvention attempts on the target, while both the target's IT team and penetration testers are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they may be provided with a limited-privilege user account as a starting point to identify privilege-escalation possibilities in the system.

Potential risk associated with penetration testing includes:

- Penetration testing does not provide assurance that all vulnerabilities are discovered, and it may fail to discover significant vulnerabilities.
- Miscommunication may result in the test objectives not being achieved.
- Testing activities may inadvertently trigger escalation procedures that were not appropriately planned.
- Sensitive information may be disclosed, heightening the target's exposure level.
- Penetration testers who have not been subjected to proper background and qualification checks may damage the information assets or misuse the information gained for personal benefit.

Penetration testing techniques are becoming more popular for testing the reliability of firewall access controls. The IS auditor should be extremely careful if attempting to break into a live production system because, if successful, the IS auditor may cause the system to fail. Permission for the use of such techniques should always be obtained from top-level senior management. Permission from top-level senior management is also required to determine what tests can be performed without informing the staff who are responsible for the monitoring and reporting of security violations. (If any are aware that the attack will take place, they are likely to be more vigilant than usual.)

Vulnerability Assessments Versus Penetration Testing

Vulnerability assessments and penetration tests are interrelated. In most cases penetration testing depends on vulnerability assessment. Vulnerability assessment should be completed before initiating a penetration test. This assessment enables the penetration tester to understand any possible unexploited vulnerabilities that may currently be present in the system and exploit them. A subsequent penetration test will then confirm the extent to which such vulnerabilities can be exploited. Despite this interrelatedness, there are some differences between vulnerability scanning and penetration testing as depicted in **figure 5.62**.

 ©ISACA. All Rights Reserved.

Figure 5.62—Comparison of Vulnerability Assessment and Penetration Testing

	Vulnerability Assessment	Penetration Testing
Goal	To uncover known vulnerabilities in the organization	To uncover and exploit vulnerabilities to show how criminals may leverage vulnerabilities to move laterally and deeply in the environment
Frequency	More frequent; at least quarterly or after changes in networks or network equipment	Less frequent; typically once or twice a year or after every significant change in Internet-facing equipment
Scope	Wide and broad; basically, scanning the surface	Focused and deep in scope
Performers	Automated tools with human in-house oversight; does not require high skills levels	Experienced hackers with high skills levels; typically external independent experts
Outcome	Produces a list of known vulnerabilities that could be exploited	Produces a prioritized list of unknown exploitable vulnerabilities, methodologies to exploit such vulnerabilities, narrative walkthroughs of attack scenarios and recommendations for remediation
Insight	Prioritizes remediation and application of patches	Ordinarily follows a risk-based approach with remediation and patching
Value	Understanding of a basic level of security posture; possible detection of compromised systems	Understanding of all facets of the security posture; identification and reduction of vulnerabilities
Reporting	Typically comprehensive providing baselines of existing vulnerabilities and changes since the last reporting period	Typically concise, identifying the systems subject to compromise

Penetration Testing Versus Ethical Hacking

Some of the major differences between ethical hacking and penetration testing[49] are:

- Ethical hacking is much broader in scope than penetration testing, with no restrictions.
- Penetration testing tests the security of a specific aspect of an IS according to a documented scope provided while ethical hacking tests an entire system using multiple attack vectors.
- Penetration testing is a once-off engagement of limited duration while ethical hacking is continuous in nature.
- Penetration testing results are not very detailed while ethical hacking produces in-depth and comprehensive results.
- Penetration testers require robust knowledge of the domains under test. Ethical hackers mimic an attacker's footsteps; hence tactics, techniques and procedures are key.
- Penetration testers bear no responsibility for the client's security configuration and incident handling. Ethical hackers assist the client's information security teams to improve the information security posture of the organization.
- Penetration testers are required to be proficient writers of accurate reports while ethical hackers have no need to be skilled in report writing as they are often not mandated to produce reports for their clients.

5.12.5 Threat Readiness/Information Security Teams

The IS auditor should be aware of the various information security teams in an organization. **Figure 5.63** summarizes the major differences between these security teams.

[49] EC-Council, "CEH vs. PenTest+," *https://www.eccouncil.org/ceh-vs-pentest/*

Figure 5.63—Comparison of Information Security Teams

	Blue Team	Red Team	Purple Team
Objective	Detect and mitigate cyberattacks	Test resilience against real attacks	Improve security posture
Scope	Organizationwide	Organizationwide	Predetermined systems, processes and employees
Testing Method	No specific methods employed	Simulation	Efficient improvement of security posture
Tested controls	No controls tested	Detective and responsive	Detective and preventive
Tools	Endpoint detection and response (EDR), Security information and event management (SIEM)	Sophisticated, stealthy tools	Sophisticated, stealthy tools and detection software
Positioning	Continuous	Periodic	Periodic

5.12.6 Security Testing Techniques

Security testing is a process intended to reveal flaws in the security mechanisms of an IS. It is typically carried out to determine the level of protection the security controls provide with a view to providing mitigating controls when necessary. The aim of security testing is to ensure that existing security controls are working effectively. Some of the common testing techniques are:

- **Static application security testing (SAST)**—SAST relies upon static analysis. This approach is also known as white box testing. It simulates a developer's testing methodology with the tester aware of all the underlying technologies. The tester also has access to the code, frameworks, libraries, binaries, algorithms and implementations. The source code is analyzed without running the application. Using this method, security vulnerabilities can be found during the earlier phases of the SDLC and are fixed before the application enters the testing phase. However, SAST cannot detect runtime vulnerabilities.
- **Dynamic application security testing (DAST)**—DAST relies upon dynamic analysis. This approach is also called black box testing. It simulates an attacker's testing methodology. In DAST, the application is executed and analyzed, and the tester has no access to source code and only needs running applications to test. Security vulnerabilities are found during the later phase in the SDLC and generally get fixed in the next cycle except for the critical vulnerabilities.
- **Interactive application security testing (IAST)**—IAST combines SAST and DAST approaches to address their respective drawbacks and is sometimes known as grey-box testing. It is a more focused approach to application testing, which uses information present inside the application while running and requires the tester to perform analysis in real-time and during any phase of the development process. IAST also covers a broader set of testing rules than either SAST or DAST.
- **Mobile application security testing (MAST)**—MAST is a testing combination of static testing, dynamic testing, and forensics analysis. MAST performs some of the same functions as traditional static and dynamic analyzers but enables mobile code to be run through many analyzers. MAST tools are equipped with features that focus on issues specific to mobile applications, such as rooting of the device, spoofed Wi-Fi connections, handling, and validation of certificates.
- **Software Composition Analysis (SCA)**—The key function of SCA tools is to identify open-source components with vulnerabilities and potential security and compliance threats. The goal of SCA is to provide channels for IS security teams to remediate problems before they have an impact on the organization. A good SCA solution should incorporate notifications and alerts to determine areas in the code library which are affected and suggest security fixes if necessary.

5.12.7 Security Operations Center

A security operations center (SOC) is a team of IT security professionals that constantly monitors an organization's entire IT infrastructure to catch security events in real time and address them effectively. The team can be in-house or outsourced. It unifies, aggerates and coordinates an organization's security tools, practices and response to security incidents. This leads to

 ©ISACA. All Rights Reserved.

improved preventative measures and security policies, faster threat detection and faster, more effective, and more cost-effective response to security threats. The SOC also improves customer confidence and simplify and strengthen an organization's compliance with industry, national and global privacy regulations.

Common activities of the SOC include:

- **Asset inventory management**—The SOC should maintain an exhaustive inventory of all assets that needs to be protected, inside or outside the data center. This inventory includes applications, databases, servers, cloud services, endpoints, and similar infrastructure.
- **Security research**—The SOC should be current on the latest security solutions and technologies and the latest threat intelligence. This information can be gathered from social media, industry sources and other sources.
- **Events monitoring**—A SOC monitors the entire extended IT infrastructure from applications to servers, system software, computing devices and cloud workloads for signs of known exploits and for any suspicious activity. Threat data are typically analyzed to find ways to improve the organization's security posture.
- **Investigating and triaging potential incidents**—SOC teams typically receive huge volumes of event alerts. However, not all such alerts point to real incidents. Similarly, not all real incidents are created equal. Therefore, once an alert is received, it should be analyzed to determine if it points to a real attack. Once an incident is identified, the SOC team should triage and prioritize it to optimize resource utilization in the organization.
- **Security infrastructure management**—The SOC should manage the overall security infrastructure of the organization. This involves the selection, operation, and maintenance of the organization's information security technologies. Such tools and technologies that are used to protect data and information such as firewalls, antivirus/antimalware/antiransomware tools, monitoring software, and similar technologies.
- **Information security testing**—The SOC should periodically perform vulnerability assessments and penetration tests with the objective of fine tuning the security infrastructure, such as security policies and security technologies. IRPs are also based on the results of these tests. During these tests, the SOC team also ensures the security infrastructure complies with regulations such as GDPR and PCI DSS.
- **Patch management**—The SOC team should regularly perform preventative maintenance such as applying software patches and upgrades, to organizational systems while continually information security technologies such as updating firewalls, allow- and denylists, and security policies and procedures.
- **Incident response**—The SOC team should aim to for incident containment, restoration and recovery. In incident containment, the SOC team contains incidents through such activities as disconnecting networks and devices, isolating compromised infrastructure and rerouting traffic. Once an incident is contained, and the threat eradicated. The next stage involves restoring systems to the pre-incident phase which includes cutting over to backup systems.
- **Post-mortem and refinement**—To prevent a recurrence of similar events, the SOC makes use of new intelligence gained from the incidents to better address security threats and vulnerabilities, update security processes and policies, select new information security technologies and revise the IRP.

Full Network Assessment Reviews

Upon completion of penetration testing, comprehensive review of all network system vulnerabilities should occur to determine whether threats to CIA have been identified. Reviews that should occur include:

- Security policy and procedures should be reviewed to determine good practices are in place.
- The network and firewall configuration should be evaluated to ensure they have been designed to support the security of the services being provided (e.g., screening routers, dual/ multihomed host, screened subnet and DMZ proxy servers).
- The logical access controls should be evaluated to ensure that they support SoD (e.g., development vs. operation, security administration vs. audit).
- Networks should have been segmented by trust levels, using appropriately configured routers.
- Determine if:
  - Intrusion detection software is in place
  - Filtering is being performed
  - Encryption is being used (Consider VPNs/ tunneling, digital signatures for email.)
  - Strong forms of authentication are being used (Consider use of smart cards and biometrics for authentication to firewalls, to internal software/ hardware within the network and to external hardware/software.)
  - Firewalls have been configured properly (Consider removal of all unnecessary software, addition

©ISACA. All Rights Reserved.

of security and auditing software, removal of unnecessary logon IDs, disabling of unused services.)
- The application- or circuit-level gateways in use are running proxy servers for all legitimate services (e.g., teletype network [Telnet], HTTP and FTP)
- Virus scanning is being used
- Periodic penetration testing is being completed
- Audit logging is being undertaken for all key systems (e.g., firewalls, application gateways and routers) and audit logs are copied to secure file systems (Consider the use of security information and event management [SIEM] software.)
- The security administrators are keeping up to date with the latest known vulnerabilities via the organizations' vendors, their local and international CERT and vulnerability databases (e.g., the National Vulnerability Database operated by NIST).

5.12.8 Security Testing Audit Procedures

Specific procedures can be helpful to an IS auditor undertaking a security testing audit in an organization.

Terminal Identification

The IS auditor can work with the network manager to get a listing of terminal addresses and locations. This list can then be used to inventory the terminals, noting any incorrectly logged, missing or additional terminals. The IS auditor should select a sample of terminals to ensure they are identified in the network diagram.

Terminal Cards and Keys

The IS auditor can take a sample of cards or keys and attempt to gain access beyond what is usually authorized. Also, the IS auditor will want to know if the security administrator followed up on any unsuccessful attempted violations.

Logon IDs and Passwords

To test confidentiality, the IS auditor can attempt to guess the password of a sample of employees' logon IDs (although this is not necessarily a test). This should be done discreetly to avoid upsetting employees. The IS auditor should tour end-user and programmer work areas looking for passwords taped to the side of terminals or the inside of desk drawers. Another source of confidential information is the wastebasket. The IS auditor might consider going through the office wastebasket looking for confidential information and passwords. Users could be asked to give their passwords to the IS auditor. Unless specifically authorized for a particular situation and supported by the security policy, users should never disclose their password. Another way to test password strength is to analyze global configuration settings for password strength in the system application and compare them with the organization's security policy.

To test encryption, the IS auditor should work with the security administrator to attempt to view the internal password table. If viewing is possible, the contents should be unreadable. Being able to view encrypted passwords can still be dangerous. Although passwords on some systems are impossible to decipher, an individual who is able to obtain the encryption program can encrypt common passwords and look for matches. This method was used to break into Unix computers prior to the development of shadow password files. Application logs should be reviewed to ensure that passwords and logon IDs are not recorded in a clear form.

To test access authorization, the IS auditor should review a sample of access authorization documents to determine if proper authority was provided and if authorization was granted on a need-to-know basis. Conversely, the IS auditor should get a computer-generated report of computer access rules, take a sample to determine if the access is on a need-to-know basis, and attempt to match a sample of rules to authorizing documents. If no written authorization is found, this indicates a breakdown in control and may warrant further review to determine the exposures and implications.

Account settings for minimizing unauthorized access should be available from most access control software or from the OS. The IS auditor can perform manual tests to verify that these settings actually are working:
- To test periodic change requirements, the IS auditor can draw on personal experiences using the system and interview a sample of users to determine if they are forced to change their password after the prescribed time interval.
- To test for disabling or deleting inactive logon IDs and passwords, the IS auditor should obtain a computer-generated list of active logon IDs. On a sample basis, the IS auditor should match this list to current employees, looking for logon IDs assigned to employees or consultants who are no longer with the company.
- To test for password syntax, the IS auditor should attempt to create passwords in a format that is invalid, such as too short, too long, repeated from the

 ©ISACA. All Rights Reserved.

previous password, incorrect mix of alpha or numeric characters, or the use of inappropriate characters.
- To test for automatic logoff of unattended terminals, the IS auditor should log on to several terminals. The IS auditor should then simply wait for the terminals to disconnect after the established time interval. Before beginning this test, the IS auditor should verify with the security administrator that this automatic logoff feature applies to all terminals.
- To test for automatic deactivation of terminals after unsuccessful access attempts, the IS auditor should attempt to log on, purposefully entering the wrong password several times. The logon ID should deactivate after the established number of invalid passwords is entered. The IS auditor will be interested in how the security administrator reactivates the logon ID. If a simple telephone call to the security administrator with no verification of identification results in reactivation, then this function is not controlled properly.
- To test for masking of passwords on terminals, the IS auditor should log on to a terminal and observe if the password is displayed when entered.

Controls Over Production Resources

Computer access controls should extend beyond application data and transactions. There are numerous high-level utilities, macro or job control libraries, control libraries and system software parameters for which access control should be particularly strong. Access to these libraries would provide the ability to bypass other access controls.

The IS auditor should work with the system software analyst and operations manager to determine if access is on a need-to-know basis for all sensitive production resources. Working with the security administrator, the IS auditor should determine who can access these resources and what can be done with the access.

Logging and Reporting of Computer Access Violations

To test the reporting of access violations, the IS auditor should attempt to access computer transactions or data for which access is not authorized. The attempts should be unsuccessful and identified in security reports. This test should be coordinated with the data owner and security administrator to avoid violation of security regulations.

Follow-Up Access Violations

To test the effectiveness and timeliness of the security administrator and data owner's responses to reported violation attempts, the IS auditor should select a sample of security reports and look for evidence of follow-up and investigation of access violations. If such evidence cannot be found, the IS auditor should conduct further interviews to determine why this situation exists.

Bypassing Security and Compensating Controls

This is a technical area of review. As a result, the IS auditor should work with the system software analyst, network manager, operations manager and security administrator to determine ways to bypass security. This typically includes bypass label processing (BLP), special system maintenance logon IDs, OS exits, installation utilities and input/output (I/O) devices. Working with the security administrator, the IS auditor should determine who can access these resources and what can be done with this access. The IS auditor should determine if access is on a need-to-know/have basis or if compensating detective controls exist.

There should be restrictions and procedures for monitoring access to computer features that bypass security. Generally, only system software programmers should have access to:
- **BLP**—BLP bypasses the computer reading of the file label. Because most access control rules are based on file names (labels), BLP can bypass access control programs.
- **System exits**—This system software feature permits the user to perform complex system maintenance, which may be tailored to a specific environment or company. System exits often exist outside the computer security system and their use is thus not restricted or reported.
- **Special system logon IDs**—These logon IDs often are provided by vendors. The names can be determined easily because they are the same for all similar computer systems (i.e., system). Passwords should be changed immediately upon installation to secure the systems.

Because many of these bypassing security features can be exploited by technically sophisticated intruders, the IS auditor should also ensure that:
- All uses of these features are logged, reported and investigated by the security administrator or system software manager.
- Unnecessary bypass security features are deactivated.

©ISACA. All Rights Reserved.

- If possible, the bypass security features are subject to additional logical access controls.

5.13 Security Monitoring Logs, Tools and Techniques

Monitoring, detection and logging are integral parts of security. With potential for attacks and data loss, it is necessary to monitor data and information flowing into and out of an organization. There are several methods and tools an organization can use to detect and log potential problems.

5.13.1 Information Security Monitoring

Information security monitoring is the process of reviewing information to allow for the detection of malicious activities by users, attempted system intrusions and system failures. It can assist in reconstructing events, providing evidence for prosecution and creating reports for forensic analysis. Log analysis refers to a form of monitoring in which the logged information is systematically analyzed for trends, indications and patterns to detect potential security issues. Monitoring provides several benefits for an organization including:

- **Enforces accountability**—Monitoring and reviewing audit trail logs ensures that users can be held accountable for their actions and activities.
- **Promotes positive behavior**—When users are aware that their activities are being logged, they are less likely to attempt to circumvent security controls or to perform any unauthorized actions for fear of being discovered.
- **Encourages compliance culture**—Legislation, regulations and internal policies typically require specific monitoring and accountability practices.
- **Supports investigations**—Monitoring audit trails enables investigators to reconstruct events after their occurrence. A close examination of audit trails can reveal all the conditions and system states leading up to the event, during the event, and after the event. If NTP is implemented, time stamps remain consistent throughout the environment.
- **Identifies security problems**—Monitoring provides important information about events such as system failures, OS bugs, software errors and malicious attacks. Some log files can capture the contents of memory when an application or system crashes. All such information can pinpoint problems in the organization's systems and networks.

5.13.2 Intrusion Detection Systems

An IDS is an important element of securing networks and complements firewall implementations. An IDS works with routers and firewalls by monitoring network use anomalies. It protects an enterprise's IS resources from external and internal misuse.

An IDS operates continuously on the system, running in the background and notifying administrators when it detects a perceived threat. Broad categories of IDSs include:

- **Network-based IDSs**—They identify attacks within the monitored network and issue a warning to the operator. If a network-based IDS is placed between the Internet and the firewall, it will detect all the attack attempts, whether or not they enter the firewall. If the IDS is placed between a firewall and the corporate network, it will detect attacks that enter the firewall (it will detect intruders). The IDS is not a substitute for a firewall, but it complements the function of a firewall.
- **Host-based IDSs**—They are configured for a specific environment and will monitor various internal resources of the OS to warn of a possible attack. They can detect the modification of executable programs, detect the deletion of files and issue a warning when an attempt is made to use a privileged command.

Components of an IDS are:

- Sensors that are responsible for collecting data, such as network packets, log files and system call traces
- Analyzers that receive input from sensors and determine intrusive activity
- Administration console
- User interface

Types of IDSs include:

- **Signature-based**—These IDS systems protect against detected intrusion patterns. Identified intrusive patterns are stored as signatures.
- **Statistical-based**—These systems need a comprehensive definition of the known and expected behavior of systems.
- **Neural networks**—An IDS with this feature monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but with added self-learning functionality.

Signature-based IDSs cannot detect all types of intrusions due to the limitations of the detection rules. Statistical-based systems may report many events that are outside the defined normal activity but are normal activities on

 ©ISACA. All Rights Reserved.

the network. A combination of signature- and statistical-based models provides better protection.

Features

The features available in an IDS include:
- Intrusion detection
- Gathering evidence on intrusive activity
- Automated response (i.e., termination of connection, alarm messaging)
- Security policy
- Interface with system tools
- Security policy management

Limitations

An IDS cannot help with:
- Weaknesses in the policy definition
- Application-level vulnerabilities
- Back doors into applications
- Weaknesses in I&A schemes

Policy

An IDS policy should establish the action to be taken by security personnel in the event an intruder is detected.

Actions may include:
- **Terminate the access**—If there is a significant risk to the organization's data or systems, immediate termination is the usual procedure.
- **Trace the access**—If the risk to the data is low, the activity is not immediately threatening, or analysis of the entry point and attack method is desirable, the IDS can be used to trace the origin of the intrusion. This can be used to determine and correct any system weaknesses and to collect evidence of the attack, which may be used in a subsequent court action.

In either case, the action required should be determined by management in advance and incorporated in a policy. This will save time when an intrusion is detected and may impact the possible data loss.

5.13.3 Intrusion Prevention Systems

IPSs are closely related to IDSs and are designed not only to detect attacks, but also to prevent the intended victim hosts from being affected by the attacks. Whereas an IDS alerts or warns of an attack, requiring security personnel to act, an IPS will try to stop the attack. For example, an IPS can disconnect an originating network or user session by blocking access to the target from the originating user account and/or IP address. Some IPSs can also reconfigure other security controls, such as a firewall or router, to block an attack. The intrusion prevention approach can be effective in limiting damage or disruption to systems that are attacked. However, as with an IDS, the IPS must be properly configured and tuned to be effective. Threshold settings that are too high or too low will lead to limited effectiveness of the IPS. Some concerns have been raised that the IPS itself may constitute a threat, because a clever attacker could send commands to many hosts protected by an IPS to cause them to become dysfunctional. This attack could be catastrophic in environments where continuity of service is critical. Types of IPSs are shown in **figure 5.64**.

Figure 5.64—Types of Intrusion Prevention Systems (IPS)

Type of IPS	Description
Host-based IPS (HIPS)	Information security software that is located on individual clients and servers. It monitors events and thwarts attacks at the device level.
Network-based IPS (NIPS)	Deployed within the enterprise network infrastructure. It monitors all the data in the complete network and thwarts threats before they can reach their targets.
Wireless IPS (WIPS)	A network security device that monitors radio waves for unauthorized access points (APs). It automatically takes countermeasures to prevent them from causing damage to enterprise systems.

In contrast to IDSs, which rely on signature files to identify an attack as it happens (or after), an IPS predicts an attack before it can take effect. It does this by monitoring key areas of a computer system and looking for bad behavior, such as worms, Trojans, spyware, malware and hackers. It complements firewall, antivirus and antispyware tools to provide complete protection from emerging threats. It is able to block new (zero-day) threats that bypass traditional security measures because it is not reliant on identifying and distributing threat signatures or patches. **Figure 5.65** provides a comparison of IDS and IPS.

©ISACA. All Rights Reserved.

Figure 5.65—Comparison of IDS and IPS

	Intrusion Detection System (IDS)	Intrusion Prevention System (IPS)
Scope	IDS operates as a monitoring tool and is built for detection and surveillance and will take minimal action by itself when a threat is detected.	IPS is a control-based solution that either accepts or rejects network packets based on predetermined rulesets.
Interrelatedness	An IDS cannot do the job of an IPS.	An IPS can do the job of an IDS.
Extent	Any detected threats or anomalies are flagged and sent to human security personnel for further action.	Once a threat is detected, IPS stops the flow of malicious traffic. It can shut down the threat and prevent the malicious packets from reaching their target while alerting security personnel.
Location	IDS operates across the organizational network, monitoring and analyzing traffic in real time.	IPS typically operates in the same network location as a firewall, intercepting traffic at the juncture where the internal network meets the Internet at large.
Range	Packets anywhere on the network are scanned for indicators of compromise.	IPS is limited compared to IDS. IPS can rely on IDS to increase its range of surveillance.
Level of human intervention	An IDS is not capable of implementing a predetermined plan of action and addressing identified threats independently. If another solution, such as IPS, is not implemented, IDS would typically require a dedicated human resource to deal with any malicious traffic detected.	IPS is highly proactive in nature and leverages either a database of the latest threat signatures or a machine learning-powered behavior model to detect and prevent security violations before they cause damage.
Configuration	IDS is generally set to operate inline.	In a network, IPS is placed behind the firewall and generally configured to operate either as an end host or in the inline mode.

Honeypots and Honeynets

A honeypot is a software application that pretends to be a vulnerable server on the Internet and is not set up to actively protect against break-ins. A honeypot acts as a decoy system that lures hackers. The more a honeypot is targeted by an intruder, the more valuable it becomes. Although a honeypot is technically related to IDSs and firewalls, it does not actively protect networks.

There are two basic types of honeypots:
1. **High-interaction**—Gives hackers a real environment to attack
2. **Low-interaction**—Emulates production environments and provides limited information

A honeynet is a set of multiple linked honeypots that simulate a larger network installation. Hackers infiltrate the honeynet, which allows investigators to observe the hackers' actions using a combination of surveillance technologies. An IDS triggers a virtual alarm whenever an attacker breaches the security of networked computers. A stealthy keystroke logger watches everything the intruder types. A separate firewall cuts off the machines from the Internet anytime an intruder tries to attack another system from the honeynet.

All traffic on honeypots or honeynets is assumed to be suspicious because the systems are not meant for internal use. The information collected about these attacks is used proactively to update vulnerabilities on an enterprise's live network.

If a honeypot is designed to be accessible from the Internet, there is a risk that external monitoring services that create lists of untrusted sites may report the organization's system as vulnerable, without knowing that the vulnerabilities belong to the honeypot and not to the system itself. Such independent reviews made public can affect the organization's reputation. Therefore, prior to implementing a honeypot in the network, careful judgment should be exercised.

 ©ISACA. All Rights Reserved.

Best Practices for IDS/IPS Implementation

Best practices for implementing IDS/IPS include:

- **Perform an asset inventory**—An asset inventory is critical in the implementation of an IDS/IPS solution as it determines the placement of the technological solutions.
- **Establish an IDS/IPS policy**—There must be an organizational IDS/IPS policy and standards to ensure compliance with the policy. The policy should be updated in line with changes in the threat environment.
- **Set a baseline**—Baselining sets the normal network behavior in the organization and is critical for IDS/IPS deployment.
- **Ensure the IDS/IPS is properly placed**—The proper placement of the IDS/IPS is an important consideration for its effective functioning. It is advisable to start with the highest point of visibility and proceed down the network. Depending on the available resources, the organization should consider having multiple IDS/IPS installations to cover intra-host traffic.
- **Ensure the IDS/IPS is properly tuned**—IDS/IPS tuning is an ongoing process that requires constant iteration depending on network complexity. It involves updating rules as new signatures are released and as changes occur in the network.
- **Develop logging systems**—Since an IDS can generate large amounts of data, logging systems should be chosen that allow the gathering of large amounts of data, backup and recovery procedures and storage facilities. Hardware and software may need to be ordered during this phase.
- **Order of deployment**—This should be done immediately to start gathering data. Again, a network-based IDS should be deployed first as an industry and recommended standard. The approach should be three tiers, starting at the furthest extension of the security parameter, then DMZ and other devices. Host-based IDS deployment should follow network-based, as an industry standard. It could actually be done at the same time as network-based, but the emphasis should be placed on network-based first.
- **Incident response**—An IRP must be developed to ensure a standard is in place once a malicious attempt is made on company systems. This should include a written procedure and next steps in the notification chain.

5.13.4 Audit Logging in Monitoring System Access

Most access control software has security features that enable a security administrator to automatically log and report all levels of access attempts. For example, access control software can log computer activity initiated through a logon ID or computer terminal. This information provides management with an audit trail to monitor activities of a suspicious nature, such as an attacker attempting brute force attacks on a privileged logon ID. Also, keystroke logging can be turned on for users who have sensitive access privileges. What is logged is determined by the action of the organization. Issues include what is logged, who/what has access to the logs and how long logs are retained (record-retention item).

Access Rights to System Logs

Access rights to system logs for security administrators to perform logging and monitoring activities should be strictly controlled.

Computer security managers and system administrators/managers should have access for review purposes; however, security and/or administration personnel who maintain logical access functions may not need to access audit logs.

It is particularly important to ensure the integrity of audit trail data against modification. This can be done using digital signatures, write-once devices or a SIEM system. Audit trail files need to be protected because intruders may try to modify them to cover their tracks. Audit trail records should be protected by strong access controls to help prevent unauthorized access. The integrity of audit trail information may be particularly important when legal issues arise, such as the use of audit trails as legal evidence. (This would require daily printing and signing of logs.) Questions regarding legal issues should be directed to the appropriate legal counsel.

The confidentiality of audit trail information may be protected if the audit trail is recording information about users that may be disclosure-sensitive, such as transaction data containing personal information (e.g., before and after records of modification to income tax data). Strong access controls and encryption can be particularly effective in preserving confidentiality.

Media logging is used to support accountability. Logs can include control numbers (or other tracking data) such as the times and dates of transfers, names and signatures of individuals involved, and other relevant information.

©ISACA. All Rights Reserved.

Periodic spot checks or audits may be conducted to determine that no controlled items have been lost and that all are in the custody of individuals named in control logs. Automated media-tracking systems may be helpful for maintaining inventories of tape and disk libraries.

A periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours. Certain reports are generated for security recorded in activity logs.

Tools for Audit Trail (Logs) Analysis

Many types of tools have been developed to help reduce the amount of information contained in audit records and to delineate useful information from the raw data.

On most systems, audit trail software can create large files, which can be extremely difficult to analyze manually. The use of automated tools is likely to be the difference between unused audit trail data and an effective review. Some of the types of tools include:

- **Audit reduction tools**—They are pre-processors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. (This alone may cut the number of records in the audit trail in half.) These tools generally remove records generated by specified classes of events—for example, records generated by nightly backups.
- **Trend/variance-detection tools**—They look for anomalies in user or system behavior. It is possible to construct more sophisticated processors that monitor usage trends and detect major variations. For example, if a user typically logs in at 09:00 but appears at 04:30 one morning, this may indicate a security problem that needs to be investigated.
- **Attack-signature-detection tools**—They look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt.
- **SIEM systems**—These tools capture audit trails or logs and perform real-time analysis on them. They can aggregate audit trails and logs from many different sources. This data can then be correlated and alerts provided if required. Some SIEM systems can also be configured to perform automated tasks based upon the alerts (e.g., launching a vulnerability scan or commanding the firewall to close a certain port).

Cost Considerations

Audit trails involve many costs that factor into IT's determination as to how much logging is enough. First, some system overhead is incurred while recording the audit trail. Additional costs will be incurred to store and process the records. The more detailed the records, the more overhead is required. In some systems, logging every event could cause the system to lock up or slow to the point when response time would be measured in minutes. This is not acceptable if IT is properly aligned with the needs of the business.

Another cost involves human and machine time required when performing the analysis. This can be minimized by using tools. Many simple analyzers can be constructed quickly and inexpensively from system utilities, but they are limited to audit reduction and the identification of particularly sensitive events. More complex tools, such as SIEM systems, will be more expensive both to purchase and to implement.

The final cost of audit trails is the cost of investigating unexpected and anomalous events. If the system is identifying too many events as suspicious, administrators may spend undue time reconstructing events and questioning personnel. The frequency of the security administrator's review of computer access reports should be commensurate with the sensitivity of the computerized information being protected. The IS auditor should ensure that the logs cannot be tampered with or altered without leaving an audit trail.

When reviewing or performing security access follow-up, the IS auditor should look for:

- Patterns or trends that indicate abuse of access privileges, such as concentration on a sensitive application
- Violations (such as attempting computer file access that is not authorized) and/or use of incorrect passwords

When a violation is identified:

- The person who identified the violator should refer the problem to the security administrator for investigation.
- The security administrator and responsible management should work together to investigate and determine the severity of the violation. Generally, most violations are accidental.
- If a violation attempt is serious, executive management should be notified, not law enforcement officials. Executive management normally is responsible for notifying law enforcement officials. Involvement of external agencies may result in

adverse publicity that is ultimately more damaging than the original violation; therefore, the decision to involve external agencies should be left to executive management.
- Procedures should be in place to manage public relations and the press.
- To facilitate proper handling of access violations, written guidelines should identify various types and levels of violations and how they will be addressed. This effectively provides direction for judging the seriousness of a violation.
- Disciplinary action should be a formal process that is applied consistently. It may involve a reprimand, probation or immediate termination. The procedures should be legally and ethically sound to reduce the risk of legal action against the company.
- Corrective measures should include a review of the computer access rules, not only for the perpetrator but for interested parties. Excessive or inappropriate access rules should be eliminated.

5.13.5 Protecting Log Data

Personnel within the organization can use logs to recreate events leading up to and during an incident, but only if the logs have not been modified. If attackers can modify the logs, they can erase their activity, effectively affecting the value of the data. The files do not contain accurate information and may not be admissible as evidence in the prosecution of attackers. It is therefore important for the IS auditor to evaluate whether the organization has appropriate procedures in place to protect log files against unauthorized access and modification.

Some of the methods commonly used to enhance the protection of log data include:[50]
- **Centralize log storage**—It is common to store copies of logs on a central system to protect it. Even if an attack modifies or corrupts the original files, personnel can still use the copy to view the events and continue carrying out assigned tasks.
- **Implement access controls**—An organization can protect log files by assigning permissions to limit access. Generally, users should not have any access to log files unless some level of access is necessary for creating log entries. If access is required, users should have append-only privileges and no read access if possible.
- **Restrict logging of sensitive data**—Logging should be configured in such a way that the solution does not record information that is not required or would present a substantial risk if accessed by unauthorized individuals, such as passwords.
- **Establish log policies**—Organizations should establish strict policies mandating backups of log files. Additionally, log policies should define log retention times. For example, an organization may craft a policy that allows keeping archived log files for certain periods.
- **Implement secure log transfer**—It is recommended that an organization implement secure mechanisms for transporting log data from the system to the centralized log management servers. Secure protocols that can be used include IPsec and TLS.
- **Implement secure storage media**—The storage media where logs are stored need to be physically protected. This entails keeping the media in a secure location and also monitoring access to the secure area. In addition, proper environmental controls should be in place, such as temperature and humidity controls.
- **Protect archived log files**—This could include creating and securing message digests for the files, encrypting log files and providing adequate physical protection for archival media. Secure the processes that generate the log entries. Unauthorized parties should not be able to manipulate log source processes, executable files, configuration files or other components of the log sources that could impact logging.
- **Implement log disposal controls**—The organization should ensure that logs are destroyed safely when they are no longer required. This is mainly due to the lapse of time when the logs were considered relevant. Log disposal generally entails the destruction of media where log data is stored. The organization should ensure that the media destruction methods applied destroy the data completely and permanently to avoid instances of data remanence.

5.13.6 Security Information and Event Management

Security incidents are often made up of a series of events that occur throughout a network. By correlating data, the SIEM can take many isolated events and combine them to create one single relevant security incident. These systems use either rule-based or statistical correlation. Rule-based correlations create situation-specific rules that establish a pattern of events. Statistical correlation uses algorithms to calculate threat levels incurred by relevant events on various IT assets. There are a

[50] National Institute of Standards and Technology, *Special Publication 800-92: Guide to Computer Security Log Management*, USA, 2006, *https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf*

©ISACA. All Rights Reserved.

variety of SIEM solutions available that provide real-time monitoring, correlation of events, notifications, and console views.

SIEM is an umbrella term for centralized information security software packages that combine the following two technologies:

- **Security information management (SIM)**—The SIM component collects data from log files for analysis and reporting on past security threats and events. SIM systems are an extension of the broader log management discipline, and they automate the collection of log data from various security tools and systems and provide the information to the IS security team.
- **SEM**—SEM works in similar fashion to SIM, the only difference being that instead of focusing on historic log data, it works in real-time mode to identify relevant security events. It conducts real-time system monitoring, notifies security administrators about important issues and establishes correlations between security events as they happen.

SIEM typically supports two ways of collecting logs from log generators, agentless and agent-based. Using agentless aggregation, the SIEM server receives data from the individual hosts that generate logs without any requirements for installing special software on those hosts. SIEM collects logs from the hosts by authenticating to each host and retrieving its logs on a regular basis. In some cases, the hosts push their logs to the SIEM server by way of authentication. The agent-based method entails installing an agent program on the log-generating host that performs event filtering and aggregation and log normalization for onward transmission to the SIEM server. This happens on a real-time basis. Another common practice is to install multiple agents on the same server depending on the variety of logs to be collected.

Benefits of SIEM

SIEM is generally a reliable security solution that assists in security programs, supporting the operations, compliance and risk groups with valuable security information for an organization. The solution is scalable and able to support growing security needs. SIEM is simple to understand and easy to use and the automation helps increase efficiency. Additional benefits of SIEM include:

- **Enhances analytics**—A SIEM system is designed to support and facilitate data collection, analysis, response and remediation processes and procedures. It collects huge volumes of event types and configuration data. SIEM solutions that incorporate next-generation technologies such as ML and AI are able to investigate more sophisticated and complex attacks as they arise. The SIEM analytics engine inspects packet captures, gaining insight into information assets, IP addresses and protocols to reveal malicious files or data exfiltration activities.
- **Enhances regulatory compliance**—SIEM solutions enable centralized compliance auditing and reporting across an entire business infrastructure. Advanced automation streamlines the collection and analysis of system logs and security events to reduce internal resource utilization while meeting strict compliance reporting standards. The use of SIEM helps companies comply with a variety of industry information security management regulations.
- **Improves speed in addressing security concerns**—Modern next-generation SIEM solutions integrate with powerful security orchestration, automation and response (SOAR) capabilities, saving time and resources for teams managing information security. These technologies use deep ML to automatically adapt to systems behavior and address threat identification and incident response protocols quicker than employees.
- **Supports investigations**—SIEM solutions are ideal for conducting digital forensic investigations as they allow organizations to efficiently collect and analyze log data from all digital assets in one place. This provides information security professionals with the ability to recreate past incidents or analyze new ones to investigate suspicious activities.
- **Improves threat intelligence**—Being able to incorporate either proprietary or open-source intelligence feeds into the SIEM solution is essential to recognize and combat modern-day vulnerabilities and attack signatures. SIEM active monitoring solutions across the organization's entire infrastructure significantly reduce the lead time required to identify and react to potential network threats and vulnerabilities. SIEM assists in strengthening the security posture of the organization as it scales.
- **Provides insight into past events**—Every user or tracker leaves behind a virtual trail in a network's log data. SIEM systems are designed to use log data to generate insight into past attacks and events. A SIEM system not only detects an attack that has happened, but also allows the information security team to view how and why it happened.
- **Provides real-time detection of attacks**—SIEM addresses this problem by detecting attack activity

and assessing it against past behavior on the network. A SIEM system has the ability to distinguish between legitimate use and a malicious attack. This helps to increase a system's incident protection and avoid damage to systems and virtual property.

- **Reduces security staffing**—With the ever-increasing variety and volume of threats, the ability to staff security operations teams continues to be a concern. A single SIEM server can streamline workflow using multi-source log data to generate a single report that addresses all relevant logged security events. An analyst-centric user experience offers increased flexibility, ease of customization and faster responses to investigators. Enterprises continue to seek external service support or managed services for their SIEMs. Businesses with limited cybersecurity resources find SIEM's threat management attractive to larger clients or partners.

Features of SIEM

A SIEM is composed of several features, and it is up to the organization to ensure the features adopted address its needs for information and event management. The core features needed for a SIEM system are:

- **Policies**—A SIEM solution provides default rules, alerts, reports and dashboards that can be tuned and customized to suit the organization's specific security requirements. Generally, it contains a profile for defining the behavior of the organization's systems, both under normal conditions and security incident conditions.
- **Security knowledge base**—This database contains information regarding known security vulnerabilities, interpretation of log messages and alerts, and similar technical data. The security knowledge base can be customized as required.
- **Log data management**—Log data management is a critical component of a SIEM system as it needs to pool log info from a variety of data sources across an organization's entire network. Logs data is analyzed in real time, allowing IS security teams to automatically manage log and network flow data from a centralized location.
- **Event correlation and analytics**—SIEM solutions have functionalities to consolidate, parse and analyze log files. Security events are typically grouped together and correlation rules applied. Correlation combines individual data events to produce meaningful security information. The final stage involves quantifying the data and comparing it to previous data.
- **Notifications and alerts**—The SIEM system can recognize patterns of malicious behavior and raise notifications and alerts to the user. The data is then analyzed by the IS security analyst for the purposes of defining new criteria for future alerts. This strengthens the organization's defenses against emerging threats.
- **Network visibility**—By inspecting packet captures and enhancing visibility into network flows, the SIEM analytics engine obtains crucial security insights into IS infrastructure. This assists security professionals to reveal malicious files or data exfiltration that takes place across the network.
- **Security incident monitoring**—SIEM typically detects and tracks security events in real time. The security incident monitoring functionality is often combined with robust workflow features for improved efficiency.
- **Compliance reporting**—In highly regulated industries, a SIEM with extensive compliance reporting features is considered crucial. In general, most SIEM systems have some kind of a compliance report system that generates reports that assist organizations in conforming to applicable compliance requirements.

SIEM Implementation Best Practices

The IS auditor should provide expert advice to the management of an organization that seeks to implement a SIEM solution. Before or after an organization has acquired and implemented a SIEM solution, the IS auditor should advise management on the best practices for successful implementation. Some of the best practices in SIEM implementation are:

- **Set implementation scope**—The organization should start by fully understanding the scope of the proposed SIEM implementation. It should define the benefits that are expected from the implementation and identify appropriate use cases. SIEM should be selected and implemented based on information security goals, compliance requirements and the threat landscape of the organization.
- **Provide a holistic posture**—For successful SIEM implementation, the organization should design and apply predefined data correlation rules across all systems and networks. These rules should be extended to cloud deployments. Data that the SIEM collects should be aggregated and displayed visually to avoid missing critical events.
- **Identify all compliance requirements**—It is important for the organization to identify all compliance requirements and ensure the SIEM

©ISACA. All Rights Reserved.

solution is configured to report on them in real time to provide the organization with a better understanding of its risk posture. Meeting compliance requirements is an important benefit to most organizations using SIEM.

- **Classify all digital assets**—The organization should prepare an inventory and classification system for all digital assets stored across its IS infrastructure. This simplifies the management of log data and the monitoring of security activities.
- **Fine-tune SIEM configurations**—Fine-tuning SIEM configurations assists in reducing the number of false-positives in security alerts. The IS auditor should note that the SIEM software ordinarily presents its own set of preconfigured correlation rules. The organization's IS security team should then fine-tune the SIEM software in line with the security requirements of the organization.
- **Implement IRP**—An IRP is a requirement in the effective resolution of security incidents. It should be in place specifying such procedures as SIEM alert handling and the resolution of incidents documented. This improves efficiency and effectiveness in responding to security incidents.
- **Automate and integrate**—For accurate detection and resolution of events, the organization should automate the SIEM solution and add technologies like AI and SOAR. Some SIEM software includes automated functions, such as automated security incident analysis and automated IR.
- **Assign a SIEM administrator**—SIEM administrator is a crucial role in information security, as it ensures the proper maintenance of a SIEM implementation. The organization may evaluate the possibility of investing in a managed security service provider (MSSP) to handle its SIEM deployments, as an MSSP is better equipped to handle the complexities of SIEM implementations.
- **Monitor access controls**—A SIEM solution should monitor various aspects of critical resources such as privileged and administrative access, remote login attempts and system failure. It should be able to defend network boundaries using such technologies as firewalls, routers, ports and wireless APs.
- **Test the SIEM**—The organization should subject its SIEM to testing. This involves conducting test runs on the SIEM implementation and assessing how the technology reacts. This is critical, as it can lead to improvements in alert metrics and reconfiguration of the IS infrastructure.

5.13.7 Security Monitoring Tools

Security monitoring tools refer to technologies that are employed by information security professionals to monitor, detect and analyze activities taking place in the organization's systems and networks that can potentially indicate security events or incidents. Monitoring tools automatically provide warnings and alerts to enable information security teams to respond quickly and protect the organization from possible intrusion. To effectively discover threats, security monitoring tools often collect data and provide metrics across systems. They also perform extended functions such as traffic analysis for the purposes of identifying traffic flow patterns. Security monitoring tools provide network visualizations and leverage threat intelligence to generate charts and graphs for ease of analysis. The end result is improvement in threat investigations, discovery of malicious actions and activities, and assistance in troubleshooting security challenges.

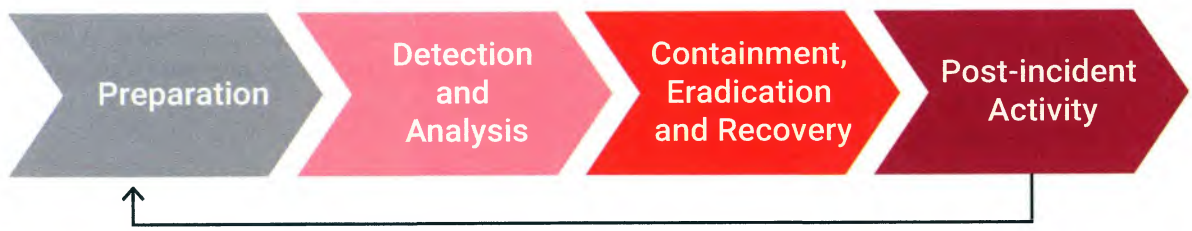
5.14 Security Incident Response Management

Incident management is the management of incidents that are potentially damaging to an organization. In information security, it is critical for the IS auditor to grasp the fact that not all incidents are computer-related; for example, a burglary at the office is also an incident. To minimize damage from security incidents and to recover and to learn from such incidents, a formal incident response capability should be established.

5.14.1 Incident Response Process

Figure 5.66 outlines the incident response process.

Figure 5.66—Incident Response Process



Source: Cichonski, P.; T. Millar; T. Grance; K. Scarfone; *Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*, National Institute of Standards and Technology (NIST), *https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf*

The phases of incident response are:

- **Preparation**—Incident preparation establishes an incident response capability so that the organization is ready to respond to incidents and prevents incidents by ensuring that systems, networks and applications are afforded sufficient security. Incident prevention is typically considered a fundamental component of an incident response program. Preventing problems is usually less costly and more effective than reacting to them. Preventive practices include patch management, systems hardening and configuring the network perimeter. Correct planning and implementation decisions are key to establishing a successful incident response program. Tasks that should be performed during the preparation phase include:
  - **Defining an incident**—The organization should develop its own definition of the term "incident" and clearly specify events that would constitute incidents. The definition assists in standardizing incidents in the organization and reducing false-positives in the form of alerts and/or notifications. It also demarcates incidents from security problems and events.
  - **Creating an incident response policy**—The policy should define what events are considered incidents, establish the organizational structure for incident response, define roles and responsibilities and list the organization's incident reporting requirements.
  - **Developing incident response procedures**—Based on the incident response policy, standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists and forms used by the incident response team. SOPs should be comprehensive and detailed to ensure that the organization's priorities are properly reflected in response operations.
  - **Establishing communication guidelines**—During the incident response process, the organization may need to communicate with outside parties, including other incident response teams, law enforcement, media, vendors and external victims. Organizations should have predetermined communication guidelines so that only the appropriate information is shared with the right parties.
  - **Defining incident response activities**—Although the focus of an incident response team is performing incident response, most teams offer additional services. These include security advisory distribution, vulnerability assessment, intrusion detection and education and awareness.
  - **Selecting an incident response team**—The organization should select the team structure and staffing model best suited to its needs. When contemplating the best team structure and staffing model, an organization should consider factors such as size of the organization, the geographic diversity of major computing resources, the need for 24/7 availability, cost and staff expertise. Members of the team should receive proper training and development.
  - **Establishing and maintaining notification mechanisms**—Organizations should establish, document, maintain and exercise on-hour and off-hour contact and notification mechanisms for various individuals and groups within the organization (e.g., chief information officer [CIO], chief information security officer [CISO], IT support, business continuity planning, etc.) and outside the organization (e.g., incident response organizations, counterparts at other organizations).

©ISACA. All Rights Reserved.

- **Detection and analysis**—It is critical to detect incidents quickly because they often become more damaging as time passes. It is important to have robust monitoring and intrusion detection solutions in place, such as security cameras, motion detectors, smoke alarms and other sensors. The incident response process is most challenged by accurately detecting and assessing possible incidents. Determining whether an incident has occurred—and, if so, the type, extent and magnitude of the problem—is difficult. Incidents can be detected through things like automated detection capabilities including IDSs/IPSs, antivirus software and log analyzers. Incidents may also be detected through manual means such as user reports.
- **Containment, eradication and recovery**—It is important to contain an incident before it spreads to avoid overwhelming resources and increasing damage by:
  - **Containment**—Most incidents require containment. The essential part of containment is decision-making, such as shutting down a system, disconnecting it from the network or disabling certain system functions. Organizations should create separate containment strategies for each major type of incident. Containment strategies should be documented clearly to facilitate quick and effective decision-making.
  - **Eradication**—After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malicious code and disabling breached user accounts. For some incidents, eradication is either unnecessary or is performed during recovery.
  - **Recovery**—In recovery, administrators restore systems to normal operation and (if applicable) harden systems to prevent similar incidents. Recovery may involve such actions as:
    - Restoring systems from clean backups
    - Rebuilding systems from scratch
    - Replacing compromised files with clean versions
    - Installing patches
    - Changing passwords
    - Tightening network perimeter security (e.g., firewall rule sets)
- **Postincident activity**—After an incident has been handled, the organization should hold a lessons-learned process to review the effectiveness of the incident handling process. The information accumulated from all lessons-learned meetings and the data collected while handling each incident should be used to identify systemic security weaknesses and deficiencies in policies and procedures. Improvements to existing security controls and practices can then be proffered. The results can be referred to in handling future incidents and in training and awareness programs.

5.14.2 Computer Security Incident Response Team

A computer security incident response team (CSIRT) is a team that is established with clear lines of reporting. Responsibilities for standby support also should be established. When an incident occurs, the response team has the following primary responsibilities:

- Determine the amount and scope of damage that was realized because of the incident.
- Determine whether there was information compromise during the incident.
- Implement necessary recovery procedures to restore security and recover from incident-related damages.
- Supervise the implementation of any additional security measures necessary to strengthen the security posture and prevent repeat incidents.

Organizational CSIRT will act as an efficient detective and corrective control. Additionally, with its members' participation and involvement in security awareness programs, exercises and workshops, it can demonstrate a preventive control. It should also disseminate security alerts—such as recent threats, security guidelines and security updates—to users and assist them in understanding the security risk of errors and omissions. Organizational CSIRT should act as single point of contact for all incidents and issues related to information security and should respond to abuse reports pertaining to the network of its constituency.

An IS auditor should ensure that the CSIRT is actively involved with users to assist them in the mitigation of risk arising from security failures and also to prevent security incidents. Auditors should ensure that there is a formal, documented plan and that it contains vulnerabilities identification, reporting and incident response procedures to common security-related threats/issues, such as:

- Virus outbreak
- Web defacement
- Abuse notification
- Unauthorized access
- Security attack alerts from IPSs/IDSs
- Hardware/software theft

- System root compromises
- Physical security breach
- Malware
- Defamatory media information
- Forensic investigations

Additionally, automated IDSs should be in place to notify administrators in real time of a potential incident and define a process for determining the severity of incidents and steps to take in high-risk situations.

5.14.3 Incident Response Plan

An IRP is put in place to deal with incidents and potential security incidents that an organization encounters. The greatest benefit of having an IRP is that it allows the organization to treat a security incident scene and take initiatives such as cordoning off the area and determining the extent of the attack. The reason for that is to reveal all the relevant evidence and correlations with the crime and quickly initiate remediation processes. The IS auditor may be required to provide assurance and advice on the effectiveness of the IRP in the organization. Some best practices for developing an IRP are:

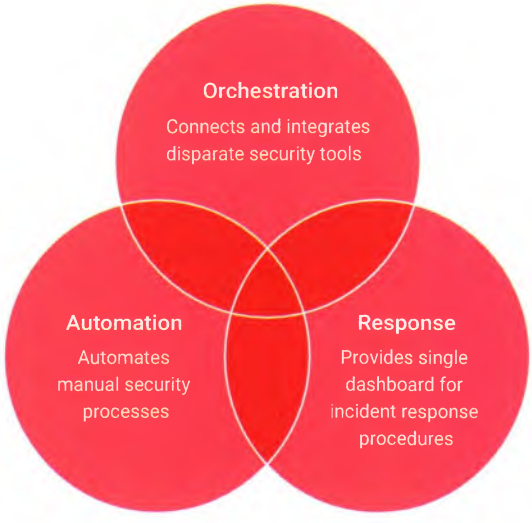
- **Automate repetitive tasks**—The organization should combine all the tools and steps involved in incident response (IR) and strive to automate all the repetitive tasks. Automation frees information security teams from some activities and allows them to focus on more-strategic security initiatives. This also reduces the IS security labor budget.
- **Leverage templates and playbooks**—Agile playbooks and templates can be customized or come preconfigured to automate multistep responses. These should adapt to the incident response information in real time, including guiding information security analysts by outlining specific roles, responsibilities and deadlines.
- **Centralize IR initiatives—A** centralized IR approach entails gathering information from all relevant security tools and technologies to create a resource and data pool that is accessible from a single place. This ensures a more coordinated and effective response to security incidents.
- **Test the plan**—This includes conducting exercises that review the best practices and various security situations to evaluate the effectiveness of the IRP. The organization can use the results from tests and drills to calibrate its IRP for real-world incidents. Testing should cover the information security team's ability to discover and contain a security incident before it spreads across organizational systems.
- **Invest in IR training and development**—The importance of security training and development in IR cannot be overemphasized. The organization should train and develop its information security personnel to address talent gaps that may exist. The information security environment is ever-evolving, and employees should be knowledgeable about the deployment and operation of advances in security technologies, such as advanced analytics, playbooks and similar capabilities.
- **Standardize incident response**—It is important for the organization to standardize responses to assist in reducing the extent of training required while allowing new recruits to easily grasp concepts.
- **Obtain executive buy-in**—Executive buy-in is a key requirement in the establishment, operation and maintenance of the IRP. The executive team should understand the importance of IR in the organization and support it by providing the necessary resources, including human and financial resources. The executives are the ones who approve the IRP and are ultimately responsible for its effective operations.
- **Confirm roles and responsibilities**—Roles and responsibilities in incident response should be clearly defined and ensure that all members of the organization accept their roles and responsibilities. Reserves should always be available to serve as backups if the critical personnel are unavailable or unreachable. The IS auditor may test this by interviewing relevant staff to gauge understanding of their roles and responsibilities.
- **Document critical assets**—Information assets in an organization should not be treated equally when it comes to IR. The organization should rank and document its assets in terms of criticality. This allows the organization to assess the impact of incidents on its critical assets and adjust the speed and depth of its response accordingly. Determining criticality of information depends on several factors, such as compliance requirements, sensitivity of the information, and its value.
- **Establish a crisis communications plan**—Communication is a very critical element of IR and should be included in the IRP. The communications plan specifies how teams should communicate during an incident while addressing procedural aspects such as appointing a spokesperson. It is a best practice to draft core communications and have them approved in advance. These documents should be instantly retrievable in case of incidents to avoid the tendency to seek communications approvals in the middle of a security incident.

©ISACA. All Rights Reserved.

5.14.4 Security Orchestration, Automation and Response

SOAR is a collection of technologies that allow the organization to gather inputs monitored by the security operations team and incorporate automated responses to the resolution of security events. It combines SOAR in a single platform. SOAR typically provides a top-to-bottom threat management system in which threats are identified and response strategies are then implemented. A single centralized console to coordinate all security aspects of an organization is a major feature of SOAR. The IS auditor should advise that the whole system be automated for operational efficiency. SOAR's components of orchestration, automation and response effectively work together to simplify the work of the organization's security teams. The components of SOAR are depicted in **figure 5.67**.

Figure 5.67—Components of SOAR



The components of SOAR are:

- **Orchestration**—This refers to a method of connecting security tools and integrating a series of interdependent and disparate security systems within an organization. It forms the connected layer that streamlines security processes and drives automation in the organization. Orchestration ensures that the organization's security tools, both manual and automated, are working in harmony to address security issues.
- **Automation**—The automation component sets SOAR apart from other security systems. With SOAR, manual intervention is eliminated due to its cumbersome and time-consuming nature. Various security management tasks—such as managing user access and query logs, triaging potential threats, and containing security issues—are automated in SOAR. Automation can also be applied in the orchestration stage.
- **Response**—Orchestration and automation provide the basis for the response capabilities the SOAR system leverages. With SOAR, an organization can manage, plan and coordinate its responses to identified security threats. As a result of the automation feature of SOAR, the risk of human error is eliminated, leading to more accurate responses to security events.

Benefits of SOAR

Some of the benefits of SOAR include:

- **Promotes security visibility**—A SOAR solution provides visibility into the entire organization's IS infrastructure. It comes with several dashboards, metrics functionalities and reporting capabilities that give insight into the organization's systems. SOAR enables the organization to easily handle multiple security events at the same time while minimizing response time.
- **Reduces security costs**—The growing number, type and sophisticated nature of information security threats present significant funding challenges to many organizations, sometimes requiring the purchase of technologies and the hiring of many information security experts, which leads to higher security costs. With the implementation of SOAR, information security is streamlined and automated, thereby reducing overall security costs.
- **Improves security efficiency**—The use of SOAR in an organization leads to efficiency improvements through significant time-saving and enhanced productivity. Information security teams in an organization no longer spend hours dealing with security events as the processes are automated.
- **Improves security effectiveness**—Organizations that implement a SOAR solution can benefit from accurate security interventions as they happen in real time. The security effectiveness of SOAR leads to fewer errors and less time spent addressing security problems.
- **Promotes security flexibility**—A SOAR solution is very flexible and can be implemented to suit the organization's specific and changing requirements. SOAR can be implemented in existing organizational setups without any need for system redesign, which is often a costly and time-consuming process.
- **Enhances collaboration**—SOAR can address various types of security threats from a central position,

allowing IS security personnel who normally work in different teams to collaborate on successfully installing and automating the SOAR system. This can lead to uniformity of security protocols and innovative security approaches in the organization.
- **Streamlines security operations**—SOAR streamlines security operations in an organization in a variety of ways. An organization can use a solution with a plugin library for the frequently used technologies and prebuilt workflows for common security use cases. This allows the organization to connect the entire security technology stack and ensure automation across security processes. It is also easy to customize orchestrations and workflows.

The IS auditor should proactively advise management on the differences between the capabilities of a SOAR solution and those of a SIEM as these are often confused with each other. Both SOAR and SIEM detect security issues, collect data about the nature of the problems identified and deal with notifications. However, there are some differences between the technologies:
- **Investigations**—SOAR collects data and provide alerts to IS security teams using a centralized platform similar to SIEM. However, while SIEM only sends alerts to IS security analysts, SOAR extends security further by adding automation and response. Therefore, SOAR can predict similar security threats to the organization before they happen.
- **Aggregation**—While both SIEM and SOAR aggregate data, SOAR reaches further to a more diverse collection of data sources. For example, SIEM can collect data from logs or events coming from the usual components in the organization's IT infrastructure. SOAR ordinarily absorbs SIEM data and adds information from other sources, such as endpoint security software, cloud security alerts and IoT device alerts.

5.15 Evidence Collection and Forensics

Computer crimes are not reported in most cases because they are not detected. In many cases when computer crimes are detected, enterprises hesitate to report them because they generate a large amount of negative publicity that can affect business. In such cases, the management of the affected enterprise seeks to fix the vulnerabilities exploited to carry out the crime and resume operations. In addition, in many countries, laws are directed toward protecting physical property. It is very difficult to use such laws against computer crime. Even in jurisdictions where the laws have been updated, the investigation procedures are not always widely known, and the necessary hardware and software tools are not always available to collect digital evidence.

In the aftermath of a computer crime, it is very important that proper procedures be used to collect evidence from the crime scene. If proper procedures are not followed, data could be damaged, and even if the perpetrator is eventually identified, the evidence may not be useful to the prosecution. Therefore, after a computer crime, the environment and evidence must be left unaltered and specialist law enforcement officials must be called in. If the incident is to be handled in-house, the enterprise must have a suitably qualified and experienced incident response team.

5.15.1 Types of Investigations

Types of investigations vary depending on the incidents under investigation, and each type of investigation has special considerations that have to be taken into account by the IS auditor. **Figure 5.68** explains typical computer investigations prevalent in the corporate world.

©ISACA. All Rights Reserved.

Figure 5.68—Types of Investigations

Type of Investigation	Description
Administrative investigation	The main purpose of an administrative investigation is to provide appropriate authorities with all relevant information so they can determine the proper course of action in an objective manner. Administrative investigations are often tied to HR scenarios, such as when a manager has been accused of improprieties.
Criminal investigation	This type of investigation is undertaken when there is knowledge or suspicion that a crime has been committed. The organization typically works with a law enforcement agency to convict the alleged perpetrator. It is common to gather evidence for a court of law and to be required to share the evidence with the defense. Therefore, the information systems (IS) auditor should advise the organization on the need to gather and handle information using methods that ensure the evidence can be used in court. In criminal cases, a suspect must be proven guilty beyond a reasonable doubt. There is often a different standard of proof in a civil case.
Civil investigation	In a civil case, one person or entity sues another person or entity; for example, one organization might sue another for a trademark violation or intellectual property (IP) theft. A civil case typically seeks monetary damages, not incarceration or a criminal record. The burden of proof is less in a civil case than in a criminal case with the requirement being merely to show a preponderance of evidence.
Regulatory investigation	A regulatory investigation is conducted by a regulating body, such as the US Securities and Exchange Commission, against an organization suspected of infracting specific regulations. In such cases, the organization is required to comply with the investigation by providing all relevant evidence.
Industry standards investigation	An industry standards investigation is carried out to determine whether an organization is adhering to a specific industry standard or set of standards. Because industry standards represent well-understood and widely implemented best practices, many organizations strive to adhere to them even when they are not required to do so. This helps to reduce security, operational and other risk while enhancing reputation in the marketplace.
Forensic investigation	A computer forensic investigation scientifically gathers and preserves criminal or potentially criminal evidence from the organization's IS environment in a way that is suitable for presentation in a court of law. Its objective is to perform a structured investigation and maintain a documented chain of evidence in preparation for legal proceedings. Forensic investigators examine things like blood or other fluids, fingerprints, residues, hard drives and so forth to establish how a criminal act was carried out.

5.15.2 Types of Computer Forensics

An IS auditor may be required or asked to be involved in a forensic analysis in progress to provide expert opinion or to ensure the correct interpretation of information gathered. Computer forensics includes activities that involve the exploration and application of methods to gather, process, interpret and use digital evidence that helps to substantiate whether an incident took place, providing validation that an attack actually occurred and gathering digital evidence that can later be used in judicial proceedings. Any electronic document or data can be used as digital evidence, provided there is sufficient manual or electronic proof that the contents of digital evidence are in their original state and have not been tampered with or modified during the process of collection and analysis.

Some common types of computer forensics include:

- **Database forensics**—Database forensics refers to the retrieval and examination of data and associated metadata residing in databases. The database forensics investigator should have unrestricted access to the organization's databases for the success of the database forensics process.
- **Email forensics**—This refers to the retrieval and analysis of email content. Email content consists of messages, contacts, schedules and similar information found on an email platform. To effectively carry out an email forensics examination, the email forensics investigator requires access to the email of the threat actor and the organization under threat.
- **Mobile forensics**—The retrieval and forensic examination of information from mobile devices is known as mobile forensics. Information from mobile phones include messages, photos, videos, contacts

 ©ISACA. All Rights Reserved.

and other information. The investigator may need to seize the device from the suspect to carry out the examination.

- **Memory forensics**—Memory forensics involves the retrieval and examination of data stored on a computer's memory and/or cache. This is commonly referred to as data in process and the technique commonly used in the investigation is known as live analysis.
- **Network forensics**—In network analysis, the network forensics investigator uses tools to monitor network traffic to identify indications of abnormal behavior within the network. Typical network forensic activities include capturing, recording and analyzing events that have occurred within the network to establish the source and trajectory of network attacks.
- **Malware forensics**—Malware forensics involves the examination of programming code to identify malicious programs such as viruses, ransomware or Trojan horses. It involves analysis of the programs' payloads to identify abnormal behavior that may indicate the presence of malware.

5.15.3 Phases of Computer Forensics

The organization should follow the defined stages in computer forensics regardless of the type of computer forensics it is engaged in. The IS auditor needs to ensure that the phases adopted are being followed by the computer forensics investigators or, if the IS auditor is requested to undertake a computer forensic investigation, the auditor should follow the defined procedures as well. The stages of computer forensics are:[51]

- **First response**—Immediately after a security incident is reported, the computer forensics team gets involved. The actions the team carries out are known as the first response, and such actions depend on the nature of the incident.
- **Search and seizure**—The computer forensics team searches the devices that were involved in the suspected crime. The purpose at this stage is to collect data for evidentiary purposes. The seizure is to ensure that the suspected criminals cannot continue the attacks or extract information from the devices.
- **Evidence collection**—At this stage, forensic investigators collect data using forensic methods. They handle evidence carefully using specified methods of evidence handling. Evidence at this stage consists of any information that is available that might form part of the body of evidence of an incident after examination.
- **Evidence security**—Computer forensic investigators should store evidence in a safe environment to reduce contamination. It is important to note that when evidence is stored in a secure place, it can be authenticated and proved to be accurate and accessible.
- **Data acquisition**—During this stage, the computer forensic investigation team retrieves electronically stored information (ESI) from the seized devices. Professionals must use proper procedures to avoid altering data and affecting the integrity of the evidence. Data acquisition enables the organization to gain insight into the suspected criminal incident.
- **Data analysis**—During this stage, members of the computer forensics team identify and examine the authenticated ESI to obtain evidential data suitable for use in court. Sophisticated methods such as extraction, processing, modeling and interpretation are applied to transform collected data into useful evidence.
- **Evidence assessment**—Once ESI is identified as evidence, computer forensic investigators assess it against the security incident reported. This phase is concerned with relating the data gathered directly to the incident case.
- **Documentation and reporting**—This is a post-investigation phase that is carried out once the initial criminal investigation is done. Members of the computer forensics team report and document data and acceptable evidence in accordance with applicable legal requirements.
- **Expert witness testimony**—An expert witness refers to a professional who works in a field related to the case. The witness affirms that the data is useful and can constitute evidence.

5.15.4 Audit Considerations

The IS auditor should consider key elements of computer forensics during audit planning.

Data Protection

To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocols to inform appropriate parties that electronic evidence will be sought and to refrain from destroying it by any means.

Infrastructure and processes for incident response and handling should be in place to permit an effective

[51] EC Council, "What Is Digital Forensics," *https://www.eccouncil.org/cybersecurity/what-is-digital-forensics/*

©ISACA. All Rights Reserved.

response and forensic investigation if an event or incident occurs.

Data Acquisition

All information and data required should be transferred to a controlled location. This includes all types of electronic media, such as fixed disk drives and removable media. Each device must be checked to ensure that it is write-protected. This may be achieved by using a device known as a write-blocker.

It is also possible to get data and information from witnesses or related parties via recorded statements.

By examining volatile data, investigators can determine what is currently happening on a system. This kind of data includes open ports, open files, active processes, user logons and other data present in RAM. This information is typically lost when the infected computer is shut down.

Imaging

Imaging is a process that allows one to obtain a bit-for-bit copy of data to avoid damaging original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files, and other information from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

With appropriate tools, it is sometimes possible to recover destroyed information (erased even by reformatting) from the disk's surface.

Extraction

This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and other media if any images were created.

The extraction process could include different sources, such as system logs, firewall logs, IDS logs, audit trails and network management information.

Interrogation

Interrogation is used to obtain prior indicators or relationships, including telephone numbers, IP addresses and names of individuals, from extracted data.

Ingestion/Normalization

This process converts the information extracted to a format that can be understood by investigators. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tools. It is possible to create relationships from data by extrapolation, using techniques such as fusion, correlation, graphing, mapping or time lining, which could be used in the construction of the investigation's hypothesis.

Reporting

The information obtained from computer forensics has limited value when it is not collected and reported in the proper way. There are two types of reporting: one for IT with technical details and one for management without technical details. Both are critical. The company must be fully aware of the incident and be kept up to date as the investigation proceeds. Capture everything possible, including dates, times and pertinent details.

When IS auditors write the forensic audit reports, they must include why the system was reviewed, how the computer data was reviewed and what conclusions were made from the analysis.

Goals the report should achieve include:[52]

- Accurately describe the details of an incident
- Be understandable to decision-makers
- Be able to withstand a barrage of legal scrutiny
- Be unambiguous and not open to misinterpretation
- Be easily referenced
- Contain all information required to explain conclusions reached
- Offer valid conclusions, opinions or recommendations when needed
- Be created in a timely manner

The report should also identify the organization, sample reports and restrictions on circulation (if any) and include any reservations or qualifications that the IS auditor has with respect to the assignment.

5.15.5 Computer Forensic Techniques

Computer forensic investigators use a variety of techniques and examine the copies of compromised devices and applications. They analyze all the hidden files and unallocated disk spaces to identify all files that could be encrypted or deleted. The forensics evidence obtained from the process is documented as findings and verified with the original device information. This

[52] Luttgens, J.; M. Pepe; K. Mandia; *Incident Response & Computer Forensics, 3rd Edition*, McGraw Hill, USA, 2014

is carried out in preparation for legal proceedings. The IS auditor should understand the techniques and be able to offer the necessary advice to the team throughout the forensic investigation process. Some of the common computer forensics techniques include:

- **Deleted file recovery**—This technique involves recovering and restoring files that supposedly would have been deleted by a malicious employee, threat actor or malware. It involves searching the entire system and associated memory for fragments of files that were deleted at an endpoint. Deleted file recovery is also known as file carving or data carving.
- **Reverse steganography**—Reverse steganography is a technique in which computer forensic investigators search the hashes of the file contents to identify if there are any changes in the file and whether it was manipulated. This technique is typically effective, as threat actors often leave important information inside an image or other digital file. With reverse steganography the computer forensics investigator can identify changes in the underlying hashes.
- **Cross-drive analysis**—The cross-drive analysis technique involves analyzing data across multiple system drives through methods such as correlation and cross-referencing to compare suspicious events and detect anomalies. The comparison is meant to detect similarities and provide context of the investigation, a process also referred to as anomaly detection. Cross-drive analysis preserves information relevant to a particular forensic computer investigation.
- **Live analysis**—Live analysis analyzes the computer's volatile data (RAM and cache) while the computer is in process. The technique can identify causes of abnormal system traffic. It is also common among organizations to send the computer to a forensic laboratory for the extraction of volatile data from the computer. This is often preferred as it helps to maintain the chain of custody.
- **Stochastic forensics**—This technique involves computer forensics investigators analyzing and reconstructing past digital activity without the application of digital artifacts. Artifacts are the unintended alterations to data that arise from digital processes including hints related to digital crime. Examples of such hints include alterations to file attributes during data theft. Computer forensics investigators often apply stochastic forensics in data breaches involving insiders. The reason is that malicious insiders do not normally leave behind digital artifacts.

5.15.6 Computer Forensics Tools

IS auditors may be requested to assist in the forensic audit process or provide assurance. Some of the forensic auditing tools the IS auditor should understand well, as they improve the efficiency and effectiveness of the forensic investigation process, are:

- **Acquisition tools**—One of the primary activities that a forensic auditor should carry out is the gathering of digital evidence. This stage in the forensic investigation process is known as the acquisition process. It is critical that evidence be collected using trusted tools because the evidence may later be used in a court action. Some of the most trusted tools include SafeBank, which is used to create a mirror-image, or bit-stream backup files, of storage devices like hard drives.
- **Digital evidence bags (DEBs)**—A DEB is a tool that is typically used by IS crime scene forensic investigators. It is basically a plastic evidence bag that assists in securing physical evidence, thereby ensuring that the chain of custody is maintained. It provides IS auditors with a reliable container for storing digital evidence until it is needed. A digital evidence bag consists of a tag file, index file and bag file. A tag file contains important metadata about the evidence, including information related to the investigation and chain of custody. An index file contains information related to the data itself, including its source and format and the device used to capture the data. The bag file is the actual evidence/data typically provided as bits streams or logical files although it can also come in various other forms.
- **Analysis tools**—The analysis process is quite extensive, and speed, accuracy and efficiency are of paramount importance. The initial tools that a computer forensic investigator uses to examine digital evidence for clues are basic file listing and documentation software packages. These packages typically examine a bit-stream image and produce a listing of programs and files that were present on the original device. Software used to hide, protect, encrypt or delete files from investigators is often preferred. Examples include TrueCrypt, which is an encryption tool, and Hide and Seek, which is a steganography tool.
- **File recovery tools**—File recovery tools are crucial in a forensic investigation as malicious users often think they can cover their tracks by deleting files from their computer, and that the information will be gone forever. Rather, all deleted files become part of the storage media free space that can be used to store new files. When using file recovery tools, IS

©ISACA. All Rights Reserved.

auditors should examine such aspects as the file's characteristics, the last time the file was viewed and when it was deleted. After a list of suspicious files is generated, a tool such as Encase can be employed to open the files for further investigation.

5.15.7 Chain of Custody

Evidence of a computer crime exists in the form of log files, file time stamps, contents of memory, etc. Rebooting the system or accessing files could result in such evidence being lost, corrupted or overwritten. Therefore, one of the first steps taken should be copying one or more images of the attacked system. Memory content should also be dumped to a file before rebooting the system. Any further analysis must be performed on an image of the system and on copies of the memory dumped—not on the original system. In addition to protecting the evidence, it is important to preserve the chain of custody.

Chain of custody refers to documenting, in detail, how evidence is handled and maintained, including its ownership, transfer and modification. This is necessary to satisfy legal requirements that mandate a high level of confidence regarding the integrity of evidence. It is very important to preserve evidence in any situation. Organizations typically are not well equipped to deal with intrusions and electronic crimes from an operational and procedural perspective, and they respond only when an intrusion has occurred and a risk has been realized. Evidence loses its integrity and value in legal proceedings if it is not preserved and subjected to a documented chain of custody. This happens when an incident is inappropriately managed and responded to in an ad hoc manner.

For evidence to be admissible in a court of law, the chain of custody needs to be maintained professionally. The chain of evidence contains information regarding:

- Who had access to the evidence (chronological)
- The procedures followed in working with the evidence (e.g., disk duplication, virtual memory dump)
- Proving that the analysis is based on copies that are identical to the original evidence (e.g., documentation, checksums or timestamps)

It is important to use industry-specified good practices, proven tools and due diligence to provide reasonable assurance of the quality of evidence.

It is also important to demonstrate integrity and reliability of evidence for it to be acceptable to law enforcement authorities. For example, if the IS auditor boots a computer suspected of containing stored information that might represent evidence in a court case, the auditor cannot later deny that having written data to the hard drive because the boot sequence writes a record to the drive. This is the reason specialist tools are used to make a true copy of the drive, which is then used in the investigation.

5.15.8 Best Practices to Secure Digital Evidence

A digital investigation involving potential computer crimes has rules and processes that ensure that the collected evidence is admissible in court. Best practices for securing digital evidence are:

- **Prevent contamination**—Computer forensics should preserve the crime scene and maintain the integrity of the data and the environment. This enables other investigators to be able to perform their own analyses and come to the same conclusions, as they have the same data. The IS forensics investigator should take images of the memory and storage and examine the contents without modifying the originals. The imaging should produce a bit-for-bit duplicate of an evidence file that will serve as the work copy. It is advisable to never work on the original data, as doing so often leads to the deletion and contamination of valuable metadata.
- **Have a clear chain of custody**—In computer forensics jurisprudence, it is essential to prove the integrity of evidence by maintaining audit logs. The chain of custody will assist in proving the authenticity of evidence, as it provides a complete record of who accessed the file at what time, and the sequence of activities performed on the evidence by any authenticated user. It is critical for the IS auditor to verify the transfer of media and digital evidence between every person and agency that comes in contact with it. Gaps in records typically prevent evidence from being admitted in court should there be any need for legal action.
- **Implement tamper detection**—The process of imaging generates cryptographic hash values that verify the integrity and authenticity of digital evidence by providing proof that digital evidence is the same as the original since upload. If any alteration is made to the evidence, the system generates a new hash value that does not match the original one. Hence, through hash values, any sort of alteration is detected, and the integrity of digital evidence is preserved.
- **Secure storage devices**—If digital evidence is stored on a laptop or any other device, it is critical to first

protect the device. This is achieved by incorporating password processes during logon. Password-protected screen savers can be included to prevent anyone from accessing the device. Offsite storage of the device should be considered, especially if evidence management is long term.

- **Keep mobile devices digitally isolated**—Wireless devices should be kept digitally isolated in an isolation chamber, kept off Wi-Fi and wired network connections and switched to airplane mode to prevent reception of calls. Turning off the phone preserves cell tower location information and call logs, and prevents the phone from being used, which could change the data on the phone. Devices should be placed in a Faraday bag made of antistatic packaging, such as paper bags or envelopes and cardboard boxes. Plastic should be avoided as it can convey static electricity and allow a buildup of condensation or humidity. The devices should initially be examined in isolation to prevent connections to any networks and to keep evidence in pristine condition.
- **Encrypt the hard drive**—If there are any heightened concerns about security after the implementation of passwords, the organization can go a step further to encrypt the hard drive. However, full disk encryption is not always recommended as the best option for device protection.
- **Involve forensic experts**—Normally, it is important for personnel handling evidence to know when to stop working with evidence and to allow forensic experts to take over. Following best practices allows regular security officers, IT technicians and office workers to assist with evidence collection processes. However, the process of preserving and analyzing evidence usually requires increased levels of forensic expertise.
- **Avoid changing device power status**—It is advisable to leave devices in their current power state as long as possible during evidence identification and collection. If a device is on, it is recommended to leave it on and vice versa. Battery-powered devices should be left in their current state as long as possible. When they are turned off, batteries should be removed immediately. Some phones have an automatic timer to turn on the phone for updates, which could compromise data, so battery removal is considered optimal.
- **Monitor evidence transactions**—Employees should periodically sign out evidence for reporting or for legal consultation. Recording of evidence transactions is essential for maintaining a proper chain of custody. This can be difficult for organizations that have no designated personnel to manage evidence. Therefore, IS security personnel may be called upon to manage evidence.
- **Install write-blocking software**—Installing write-blocking software prevents changes to data on a device or media while it is under examination. The write-blocker tool typically permits read-only access to the device or media, thereby maintaining the integrity of the data.
- **Incorporate other evidence**—It should be clear to the IS auditor supporting a forensic investigation that files on a computer or other device are not the only evidence that can be gathered. The analyst may have to work beyond the hardware to find evidence that resides on the Internet, including chat rooms, instant messaging, websites and other networks of participants or information. By using the system of Internet addresses, email header information, time stamps on messaging and other encrypted data, the analyst can piece together strings of interactions that provide a picture of activity.

©ISACA. All Rights Reserved.

Page intentionally left blank

 ©ISACA. All Rights Reserved.

Case Study

Spectertainment is a company dedicated to the production and distribution of video clips specializing in jazz music. Born in the Internet era, the company has actively supported the use of laptops and tablets, so staff easily work remotely. They can access the company databases through the Internet and provide online information to customers. The decision to support remote work has resulted in an increase in productivity and high morale among employees who are allowed to work up to two days a week from home. Based on written procedures and a training course, employees learn security procedures to avoid the risk of unauthorized access to company data. Employees' access to the company data includes using logon IDs and passwords to the application server through a VPN. Initial passwords are assigned by the security administrator. When the employee logs on for the first time, the system forces a password change to improve confidentiality. Management is currently considering ways to improve security protection for remote access by employees.

Spectertainment asks its IS auditor to review its new VPN implementation to accommodate the increase in remote work. The auditor discovers that many employees are using personal devices to connect to the VPN either while engaged in their remote work or when traveling. There is a remote access policy in place, but it does not specify requirements for personal devices.

1. Which of the following would be of **MOST** concern to an IS auditor reviewing a VPN implementation? Computers on the network that are located:

   A. on the enterprise's internal network.
   B. at the backup site.
   C. in employees' homes.
   D. at the enterprise's remote offices.

2. Which of the following levels provides a higher degree of protection in applying access control software to avoid unauthorized access risk?

   A. Network and OS level
   B. Application level
   C. Database level
   D. Log file level

3. When an employee notifies the company of a forgotten password, what should be done **FIRST** by the security administrator?

   A. Allow the system to randomly generate a new password.
   B. Verify the user's identification through a challenge/response system.
   C. Provide the employee with the default password and explain that it should be changed as soon as possible.
   D. Ask the employee to move to the administrator terminal to generate a new password to ensure confidentiality.

4. Which of the following policies should Spectertainment ensure are in place to address its finding that employees are using personal devices to connect to the VPN?

   A. Remote access policy
   B. Acceptable use policy
   C. Change control policy
   D. Access control policy

5. Why would Spectertainment choose to support the use of personal devices rather than prohibiting this practice? (Select all that apply.)

   A. Increased employee productivity
   B. Ease of terminating employee access if necessary
   C. Increased cost savings
   D. Improved security awareness

Answers on page 546

©ISACA. All Rights Reserved.

Chapter 5 Answer Key

Case Study

1. A. On an enterprise's internal network, security policies and controls should be in place to detect and halt an outside attack that uses an internal machine as a staging platform. Therefore, this would not be the biggest concern to the IS audit.
   B. Computers at the backup site are subject to the corporate security policy and therefore are not high-risk computers.
   C. VPN offers a secure connection between the remote PC and the corporate network. VPN does not, however, protect the remote PC from outside attack (such as from the Internet). If the remote PC is compromised, a malicious actor can use the entry point of the compromised remote PC to enter the corporate network (lateral movement).
   D. Computers on the network that are at the enterprise's remote offices, perhaps with IS and security employees who have different ideas about security, are riskier than computers in the main office or backup site, but obviously less risky than home computers.

2. **A. The greatest degree of protection in applying access control software against internal and external users' unauthorized access is at the network and platform/OS levels. These systems are also referred to as general support systems, and they make up the primary infrastructure on which applications and database systems will reside.**
   B. The application level is part of the infrastructure made up by the general support systems, supported by the network and OS level.
   C. The database level is part of the infrastructure made up by the general support systems, supported by the network and OS level.
   D. The log file level is part of the infrastructure made up by the general support systems, supported by the network and OS level.

3. A. When an employee reports a forgotten password, the security administrator should start a password process generation procedure only after verifying the user's identification using a challenge/response system or similar procedure.
   B. A challenge/response system or similar procedure should be the first step in verifying a user's identity. To verify, it is advised that the security administrator should return the user's call after verifying their extension or calling their supervisor for verification.
   C. Before an employee is provided with a default password, the individual's identity should be verified using a challenge/response system or similar procedure.
   D. Before any further action is taken, the user's identity must be verified. A new password should not be generated until it is confirmed, regardless of the security of the terminal.

4. A. Spectertainment has a remote access policy in place that outlines the approved methods for remotely connecting to internal resources but does not address the use of personal devices.
   B. An acceptable use policy outlines what employees agree to when using and accessing organizational assets. It would confirm whether the use of personal devices is allowed and may also include a Bring Your Own Device (BYOD) policy to further codify their use.
   C. Change control policies are required when making changes to IT systems. While some changes may need to be submitted based on any changes needed to support BYOD, it is not the most important control.
   D. Access control policies are required to ensure employees understand how to access systems. While changes to the access control policy may need to be made to support BYOD, it is not the most important control.

5. **A. BYOD policies have shown increased productivity and employee satisfaction.**
   B. BYOD use can make it more difficult to terminate employee access.
   C. Since employees are using their own devices, BYOD can help organizations increase their cost savings.
   D. The use of BYOD does not indicate that employees have increased awareness of the security risk posed by their use of their personal devices for work.

 ©ISACA. All Rights Reserved.

Appendix A: CISA Exam General Information

ISACA is a professional membership association composed of individuals interested in information systems (IS) audit, assurance, control, security and governance. The CISA Certification Working Group is responsible for establishing policies for the CISA certification program and developing the exam.

Note

Because information regarding the CISA examination may change, please refer to *https://www.isaca.org/credentialing* for the most current information.

The CISA designation is awarded to individuals who have met the following requirements:

1. Attaining a passing score on the CISA exam
2. Submitting verified evidence of IS auditing, control, assurance or security experience
3. Abiding by the *Code of Professional Ethics*
4. Abiding by the continuing professional education policy
5. Abiding by the IS Auditing Standards as adopted by ISACA

Successful Completion of the CISA Exam

The exam is open to all individuals who wish to take it. For optimal performance on the exam, ISACA suggests that test takers gain three years of experience in IS auditing prior to taking the exam.

Successful exam candidates must apply for certification, demonstrate that they have met all requirements and receive approval from ISACA in order to become certified.

Experience in IS Auditing, Control and Security

A minimum of five years of professional IS auditing, control, assurance and security work experience is required for certification. Please refer to the *ISACA Certification Exam Candidate Guide*, available at *https://www.isaca.org/credentialing/exam-candidate-guides*, for information about experience waivers.

Experience must have been gained within the 10-year period preceding the application date for certification or within five years from the date of initially passing the exam. A completed application for certification must be submitted within five years from the passing date of the CISA exam. All experience must be independently verified with employers.

Description of the Exam

The CISA Certification Working Group oversees the development of the exam and ensures the currency of its content. Questions for the CISA exam are developed through a multitiered process that is designed to enhance the ultimate quality of the exam.

The purpose of the exam is to evaluate a candidate's knowledge and experience in conducting IS audits and reviews. The exam consists of 150 multiple-choice questions, administered during a four-hour session.

Registration for the CISA Exam

The CISA exam is administered on a continuous basis at qualifying test sites and via live online proctoring. Consult the *ISACA Certification Exam Candidate Guide*, available at *https://www.isaca.org/credentialing/exam-candidate-guides*, for specific information, including exam registration, scheduling, languages and important key information for exam day. Exam registrations can be made online at *https://www.isaca.org/credentialing/cisa/#register*.

CISA Program Accreditation Renewed Under ISO/IEC 17024:2012

The American National Standards Institute (ANSI) has voted to continue the accreditation for the CISA, CISM, CGEIT, CRISC and CDPSE certifications under *ISO/IEC 17024:2012 Conformity assessment –*

©ISACA. All Rights Reserved.

general requirements for bodies operating certification of persons. ANSI, a private nonprofit organization, accredits other organizations to serve as third-party product, system and personnel certifiers.

ISO/IEC 17024 specifies the requirements to be followed by organizations certifying individuals against specific requirements. ANSI describes ISO/IEC 17024 as "expected to play a prominent role in facilitating global standardization of the certification community, increasing mobility among countries, enhancing public safety and protecting consumers."

ANSI's accreditation:

- Promotes the unique qualifications and expertise that ISACA's certifications provide
- Protects the integrity of the certifications and provides legal defensibility
- Enhances consumer and public confidence in the certifications and the people who hold them
- Facilitates mobility across borders or industries

Accreditation by ANSI signifies that ISACA's procedures meet the ANSI essential requirements for openness, balance, consensus and due process. With this accreditation, ISACA anticipates that significant opportunities for CISAs, CISMs, CGEITs and CRISCs will continue to open in the United States and around the world.

Scheduling the Exam

The CISA exam can be scheduled directly from your My ISACA profile. Please see the *ISACA Certification Exam Candidate Guide* at *https://www.isaca.org/credentialing/exam-candidate-guides* for complete instructions. Exams can be scheduled for any available time slot. Exams may be rescheduled a minimum of 48 hours prior to the originally scheduled appointment. If you are within 48 hours of your original appointment, you must take your exam or forfeit the exam registration fee.

Sitting for the Exam

Prior to the day of the exam:

- If testing at a testing center, locate the test center and confirm the start time.
- If testing via live online proctoring, test the computer that will be used to take the exam. Please refer to the Remote Proctoring Guide at *https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/general/remote-proctoring-guide.pdf* for detailed instructions.
- Plan to arrive 15 minutes prior to the exam start time.
- Plan to store personal belongings.
- Review the exam day rules.

You must present an acceptable form of identification (ID) to enter the testing center and to access the exam via online remote proctoring. Please see the *ISACA Certification Exam Candidate Guide* at *https://www.isaca.org/credentialing/exam-candidate-guides* for acceptable forms of ID.

You are prohibited from bringing the following items into the test center or having them in the room during online remote proctoring exams:

- Reference materials, paper, notepads or language dictionaries
- Calculators
- Any type of communication, surveillance or recording devices, such as:
  - Mobile phones
  - Tablets
  - Smart watches or glasses
  - Mobile devices
- Baggage of any kind, including handbags, purses or briefcases
- Weapons
- Tobacco products
- Food or beverages
- Visitors

If exam candidates are observed having any such communication, surveillance or recording devices during the exam administration, their exam will be voided, and they will be asked to immediately leave the exam site.

Personal items brought to the testing center must be stored in a locker or other designated area until the exam is completed and submitted.

Avoid activities that would invalidate your test score, such as:

- Creating a disturbance
- Giving or receiving help; using notes, papers or other aids
- Attempting to take the exam for someone else
- Possessing any communication, surveillance or recording device during the exam administration, including but not limited to cellphones, tablets, smart glasses, smart watches and other mobile devices
- Attempting to share test questions or answers or other information contained in the exam, including sharing test questions subsequent to the exam (as such are the confidential information of ISACA)
- Leaving the testing area without authorization (as returning to the testing room will be prohibited)

 ©ISACA. All Rights Reserved.

- Accessing items stored in the personal belongings area before completion of the exam

Budgeting Your Time

The exam is administered over a four-hour period. This allows a little over 1.5 minutes per question. Therefore, it is advisable that candidates pace themselves to complete the entire exam. To do so, candidates should complete an average of 38 questions per hour.

Grading the Exam

Candidate scores are reported as a scaled score. A scaled score is a conversion of a candidate's raw score on an exam to a common scale. ISACA uses and reports scores on a common scale from 200 to 800.

A candidate must receive a score of 450 or higher to pass the exam. A score of 450 represents a minimum consistent standard of knowledge as established by ISACA's CISA Certification Working Group. A candidate receiving a passing score may then apply for certification if all other requirements are met.

Passing the exam does not grant the CISA designation.

To become a CISA, each candidate must complete all requirements, including submitting an application and receiving approval for certification.

The CISA examination contains some questions that are included for research and analysis purposes only. These questions are not separately identified, but the candidate's final score will be based only on the common scored questions. There are various versions of each exam, but only the common questions are scored for candidate results.

A candidate receiving a score of less than 450 is not successful and can retake the exam by registering and paying the appropriate exam fee. To assist with future study, each candidate will receive a result letter that includes a score analysis by content area.

Candidates will receive a preliminary score on screen immediately following completion of the exam. **Their official score will be emailed to them and available online within 10 working days.** Question-level results cannot be provided.

To become CISA-certified, candidates must pass the CISA exam, must complete and submit an application for certification, and must receive confirmation from ISACA that the application is approved. The application is available on the ISACA website at *https://www.isaca.org/credentialing/cisa/get-cisa-certified*. After an application is approved, the candidate will be sent confirmation of the approval. The candidate is not CISA-certified and cannot use the CISA designation until the application is approved. A processing fee must accompany the CISA application for certification.

Candidates receiving a failing score on the exam may request a rescoring of their exam within 30 days following the release of the exam results. All requests must include the candidate's name, exam identification number and mailing address. A fee of US $75 must accompany the request.

©ISACA. All Rights Reserved.

Page intentionally left blank

Appendix B: CISA Job Practice

Knowledge Areas

Information System Auditing Process

A Planning

1. IS Audit Standards, Guidelines, Functions and Codes of Ethics
2. Types of Audits, Assessments and Reviews
3. Risk-Based Audit Planning
4. Types of Controls and Considerations

B Execution

1. Audit Project Management
2. Audit Testing and Sampling Methodology
3. Audit Evidence Collection Techniques
4. Audit Data Analytics
5. Reporting and Communication Techniques
6. Quality Assurance and Improvement of Audit Process

Governance and Management of IT

A IT Governance

1. Laws, Regulations and Industry Standards
2. Organizational Structure, IT Governance and IT Strategy
3. IT Policies, Standards, Procedures and Practices
4. Enterprise Architecture (EA) and Considerations
5. Enterprise Risk Management (ERM)
6. Privacy Program and Principles
7. Data Governance and Classification

B IT Management

1. IT Resource Management
2. IT Vendor Management
3. IT Performance Monitoring and Reporting
4. Quality Assurance and Quality Management of IT

©ISACA. All Rights Reserved.

Information Systems Acquisition, Development and Implementation

A Information Systems Acquisition and Development

1. Project Governance and Management
2. Business Case and Feasibility Analysis
3. System Development Methodologies
4. Control Identification and Design

B Information Systems Implementation

1. System Readiness and Implementation Testing
2. Implementation Configuration and Release Management
3. System Migration, Infrastructure Deployment and Data Conversion
4. Post-Implementation Review

Information Systems Operations and Business Resilience

A Information Systems Operations

1. IT Components
2. IT Asset Management
3. Job Scheduling and Production Process Automation
4. System Interfaces
5. Shadow IT and End-User Computing (EUC)
6. Systems Availability and Capacity Management
7. Problem and Incident Management
8. IT Change, Configuration and Patch Management
9. Operational Log Management
10. IT Service Level Management
11. Database Management

B Business Resilience

1. Business Impact Analysis (BIA)
2. System and Operational Resilience
3. Data Backup, Storage and Restoration
4. Business Continuity Plan (BCP)
5. Disaster Recovery Plans (DRP)

Protection of Information Assets

A Information Asset Security and Control

1. Information Asset Security Policies, Frameworks, Standards and Guidelines
2. Physical and Environmental Controls
3. Identity and Access Management
4. Network and End-Point Security
5. Data Loss Prevention (DLP)
6. Data Encryption
7. Public Key Infrastructure (PKI)

 ©ISACA. All Rights Reserved.

8. Cloud and Virtualized Environments
9. Mobile, Wireless and Internet-of-Things (IoT) Devices

B Security Event Management

1. Security Awareness Training and Programs
2. Information System Attack Methods and Techniques
3. Security Testing Tools and Techniques
4. Security Monitoring Logs, Tools and Techniques
5. Security Incident Response Management
6. Evidence Collection and Forensics

Secondary Classifications–Tasks

1. Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.
2. Conduct audits in accordance with IS audit standards and a risk-based IS audit strategy.
3. Apply project management methodologies to the audit process.
4. Communicate with stakeholders and collect feedback on audit progress, findings, results and recommendations.
5. Conduct post-audit follow-up to evaluate whether identified risk has been sufficiently addressed.
6. Use data analytics tools to enhance audit processes.
7. Evaluate the role and/or impact of automation and/or decision-making systems for an organization.
8. Evaluate audit processes as part of quality assurance and improvement programs.
9. Evaluate the IT strategy for alignment with the organization's strategies and objectives.
10. Evaluate the effectiveness of IT governance structure and IT organizational structure.
11. Evaluate the organization's management of IT policies and practices, including compliance with legal and regulatory requirements.
12. Evaluate IT resources and project management for alignment with the organization's strategies and objectives.
13. Evaluate the organization's enterprise risk management (ERM) program.
14. Determine whether the organization has defined ownership of IT risk, controls and standards.
15. Evaluate the monitoring and reporting of IT key performance indicators (KPIs) and IT key risk indicators (KRIs).
16. Evaluate the organization's ability to continue business operations.
17. Evaluate the organization's storage, backup and restoration policies and processes.
18. Evaluate whether the business cases related to information systems meet business objectives.
19. Evaluate whether IT vendor selection and contract management processes meet business, legal and regulatory requirements.
20. Evaluate supply chains for IT risk factors and integrity issues.
21. Evaluate controls at all stages of the information systems development life cycle.
22. Evaluate the readiness of information systems for implementation and migration into production.
23. Conduct post-implementation reviews of systems to determine whether project deliverables, controls and requirements are met.
24. Evaluate whether effective processes are in place to support end users.
25. Evaluate whether IT service management practices align with organizational requirements.
26. Conduct periodic review of information systems and enterprise architecture (EA) to determine alignment with organizational objectives.
27. Evaluate whether IT operations and maintenance practices support the organization's objectives.
28. Evaluate the organization's database management practices.
29. Evaluate the organization's data governance program.
30. Evaluate the organization's privacy program.
31. Evaluate data classification practices for alignment with the organization's data governance program, privacy program and applicable external requirements.
32. Evaluate the organization's problem and incident management program.

©ISACA. All Rights Reserved.

33. Evaluate the organization's change, configuration, release and patch management programs.
34. Evaluate the organization's log management program.
35. Evaluate the organization's policies and practices related to asset life cycle management.
36. Evaluate risk associated with shadow IT and end-user computing (EUC) to determine effectiveness of compensating controls.
37. Evaluate the organization's information security program.
38. Evaluate the organization's threat and vulnerability management program.
39. Use technical security testing to identify potential vulnerabilities.
40. Evaluate logical, physical and environmental controls to verify the confidentiality, integrity and availability of information assets.
41. Evaluate the organization's security awareness training program.
42. Provide guidance to the organization in order to improve the quality and control of information systems.
43. Evaluate potential opportunities and risk associated with emerging technologies, regulations and industry practices.

 ©ISACA. All Rights Reserved.

Glossary

A

Acceptable use policy (AUP)—A policy that establishes an agreement between users and the enterprise that defines, for all parties, the ranges of use that are approved before gaining access to a network or the Internet

Access control—The processes, rules and deployment mechanisms that control access to information systems, resources and physical access to premises

Access control list (ACL)—An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals

Scope Notes: Also referred to as access control table

Access control table—An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals

Access method—The technique used for selecting records in a file, one at a time, for processing, retrieval or storage. The access method is related to, but distinct from, the file organization, which determines how the records are stored.

Access rights—The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy

Administrative controls—The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies

Anonymous File Transfer Protocol (AFTP)—A method of downloading public files using the File Transfer Protocol (FTP). AFTP does not require users to identify themselves before accessing files from a particular server. In general, users enter the word "anonymous" when the host prompts for a username. Anything can be entered for the password, such as the user's email address or simply the word "guest." In many cases, an AFTP site will not prompt a user for a name and password.

Antivirus software—An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected.

Application—A computer program or set of programs that performs the processing of records for a specific function

Scope Notes: Applications contrast with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort.

Application controls—The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved

Application layer—The application layer provides services for an application program to ensure that effective communication with another application program in a network is possible in the Open Systems Interconnection (OSI) communications model

Application programming interface (API)—A set of routines, protocols and tools referred to as building blocks used in business application software development

Artificial intelligence (AI)—An advanced computer system that can simulate human capabilities, such as analysis, based on a predetermined set of rules

Asymmetric key (public key)—A cipher technique in which different cryptographic keys are used to encrypt and decrypt a message

Scope Notes: See public key encryption.

Audit evidence—The information used to support the audit opinion

Audit objective—The specific goal(s) of an audit

Scope Notes: These often center on substantiating the existence of internal controls to minimize business risk

Audit plan—1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion.

Scope Notes: Includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work. It also includes topics such as budget, resource

©ISACA. All Rights Reserved.

allocation, schedule dates, type of report and its intended audience and other general aspects of the work.
2. A high-level description of the audit work to be performed in a certain period of time

Audit program—A step-by-step set of audit procedures and instructions that should be performed to complete an audit

Audit risk—The risk of reaching an incorrect conclusion based upon audit findings

Scope Notes: The three components of audit risk are:

- Control risk
- Detection risk
- Inherent risk

Audit trail—A logical path linking a sequence of events, in the form of data, used to trace the transactions that have affected the contents of a record

Source : ISO

Authentication—The act of verifying the identity of a user, the user's eligibility to access computerized information

Scope Notes: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.

B

Backup—The files, equipment, data and procedures available for use in the event of a failure or loss, if the originals are destroyed or out of service

Balanced scorecard (BSC)—A coherent set of performance measures organized into four categories that include traditional financial measures and customer, internal business process and learning and growth perspectives. Developed by Robert S. Kaplan and David P. Norton.

Benchmarking—A systematic approach to comparing enterprise performance against peers and competitors in an effort to learn the best ways of conducting business

Scope Notes: Examples include benchmarking of quality, logistic efficiency and various other metrics.

Biometrics—A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint

Black box testing—A testing approach that focuses on the functionality of the application or product and does not require knowledge of the code intervals

Broadband—Multiple channels that are formed by dividing the transmission medium into discrete frequency segments

Scope Notes: Broadband generally requires the use of a modem.

Brouter—A device that performs the functions of both a bridge and a router

Scope Notes: A brouter operates at both the data link and network layers. It connects same data link type LAN segments as well as different data link ones, which is a significant advantage. Like a bridge, it forwards packets based on the data link layer address to a different network of the same type. Also, it processes and forwards messages to a different data link type network based on the network protocol address whenever required. When connecting same data link type networks, it is as fast as a bridge.

Bus—A common path or channel between hardware devices

Scope Notes: Can be located between internal computer components or between external computers in a communication network

Bus configuration—A configuration in which all devices (nodes) are linked along one communication line where transmissions are received by all attached nodes

Scope Notes: This architecture is reliable in very small networks, as well as easy to use and understand. This configuration requires the least amount of cable to connect the computers together and, therefore, is less expensive than other cabling arrangements. It is also easy to extend, and two cables can be easily joined with a connector to make a longer cable to allow more computers to join the network. A repeater can also be used to extend a bus configuration.

Business case—Documentation of the rationale for making a business investment that is used both to support a business decision on whether to proceed with the investment and as an operational tool to support management of the investment through its full economic life cycle

Business continuity plan (BCP)—A plan used by an enterprise to respond to the disruption of critical business processes (depends on the contingency plan for the restoration of critical systems)

Business impact analysis (BIA)—The process of evaluating the criticality and sensitivity of information

assets by determining the impact of losing the support of any resource to an enterprise. This establishes the escalation of a loss over time, identifies the minimum resources needed to recover and prioritizes the recovery of processes and the supporting system.

Scope Notes: This process captures income loss, unexpected expense, legal issues (regulatory compliance or contractual), interdependent processes and loss of public reputation or public confidence.

Business process reengineering (BPR)—The thorough analysis and significant redesign of business processes and management systems to establish a better-performing structure that is more responsive to the customer base and market conditions while yielding material cost savings

Business risk—The probability that a situation with uncertain frequency and magnitude of loss (or gain) could prevent the enterprise from meeting its business objectives

C

Capability Maturity Model Integration (CMMI)—An integrated model of best practices that enable businesses to improve performance by improving their processes. Product teams developed the model with global members from across the industry. The CMMI provides a best-practice framework for building, improving and sustaining process capability.

See CMMI product suite

Card swipe—A physical control technique that uses a secured card or ID to gain access to a highly sensitive location

Scope Notes: If built correctly, card swipes act as a preventive control over physical access to sensitive locations. After a card has been swiped, the application attached to the physical card swipe device logs all card users who try to access the secured location. In this way, the card swipe device prevents unauthorized access and logs all attempts to enter the secured location.

Central processing unit (CPU)—Computer hardware that houses the electronic circuits that control/direct all operations of a computer system

Certificate (Certification) authority (CA)—A trusted third party that serves authentication infrastructures or enterprises, registers entities and issues entities certificates

Certificate revocation list (CRL)—An instrument for checking the continued validity of the certificates for which the certification authority (CA) has responsibility

Scope Notes: The CRL details digital certificates that are no longer valid. The time gap between two updates is critical and poses a risk in digital certificate verification.

Certification practice statement (CPS)—A detailed set of rules governing the certificate authority's (CA) operations. It provides an understanding of the value and trustworthiness of certificates issued by a given CA.

Scope Notes: In terms of the controls an enterprise observes, this is the method used to validate the authenticity of certificate applicants and the CA's expectations of how its certificates may be used.

Chain of custody—The process of evidence handling (from collection to presentation) that is necessary to maintain the validity and integrity of evidence

Scope Notes: Includes documentation of who had access to the evidence and when and the ability to identify that the evidence is the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on verifying that evidence could not have been tampered with. This is accomplished by sealing off the evidence so it cannot be changed and providing a documentary record of custody to prove that the evidence was, at all times, under strict control and not subject to tampering.

Challenge/response token—A method of user authentication carried out through use of the Challenge Handshake Authentication Protocol (CHAP)

Scope Notes: When a user tries to log into the server using CHAP, the server sends the user a "challenge," which is a random value. The user enters a password, which is used as an encryption key to encrypt the "challenge" and return it to the server. The server is aware of the password. It, therefore, encrypts the "challenge" value and compares it with the value received from the user. If the values match, the user is authenticated. The challenge/response activity continues throughout the session, protecting it from password-sniffing attacks. In addition, CHAP is not vulnerable to "man-in-the-middle" attacks because the challenge value is a random value that changes on each access attempt.

Change management (CM)—A holistic and proactive approach to managing the transition from a current to a desired organizational state, focusing specifically on the critical human, or "soft," elements of change (ISACA)

©ISACA. All Rights Reserved.

Scope Notes: Includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives), organizational design, stakeholder management, human resources policies and procedures, executive coaching, change leadership training, team building and communication planning and execution.

Ciphertext—Information generated by an encryption algorithm to protect the plaintext that is unintelligible to the unauthorized reader

Circuit-switched network—A data transmission service that requires establishing a circuit-switched connection before data can be transferred from source data terminal equipment (DTE) to a sink DTE

Scope Notes: A circuit-switched data transmission service uses a connection network.

Circular routing—In open systems architecture, the logical path of a message in a communication network based on a series of gates at the physical network layer in the open systems interconnection (OSI) model

Client-server—A term used to broadly describe the relationship between the receiver and provider of a service. Generally, the client-server describes a networked system where front-end applications, like the client, make service requests to another networked system. Client-server relationships are defined primarily by software. In a local area network (LAN), the workstation is the client, and the file server is the server. However, client-server systems are inherently more complex than file-server systems. Two disparate programs must work in tandem, and there are many more decisions to make about separating data and processing between the client workstations and the database server. The database server encapsulates database files and indexes, restricts access, enforces security and provides applications with a consistent interface to data via a data dictionary.

Cloud computing—Convenient, scalable on-demand network access to a shared pool of resources that can be provisioned rapidly and released with minimal management effort or service provider interaction

Coaxial cable—A cable composed of an insulated wire that runs through the middle of each cable, a second wire that surrounds the insulation of the inner wire like a sheath and the outer insulation that wraps the second wire

Scope Notes: Has a greater transmission capacity than standard twisted-pair cables but has a limited range of effective distance

Cold site—An IS backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place

Scope Notes: The site is ready to receive the necessary replacement computer equipment in the event that the users have to move from the main computing location to the alternative computer facility.

Compensating control—An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions

Completely connected (mesh) configuration—A network topology in which devices are connected with many redundant interconnections between network nodes (primarily used for backbone networks)

Compliance testing—Control tests designed to obtain evidence on both the effectiveness of the controls and their operation during the audit period

Comprehensive audit—An audit designed to determine the accuracy of financial records and evaluate the internal controls of a function or department

Computer emergency response team (CERT)—A group of people integrated at the enterprise with clear lines of reporting and responsibilities for standby support in case of an information systems emergency. This group acts as an efficient corrective control and should also be the single point of contact for all incidents and issues related to information systems.

Computer forensics—The application of the scientific method to digital media to establish factual information for judicial review

Scope Notes: This process often involves investigating computer systems to determine whether they have been used for illegal or unauthorized activities. As a discipline, it combines elements of law and computer science to collect and analyze data from information systems (e.g., personal computers, networks, wireless communication and digital storage devices) in a way that makes it admissible as evidence in a court of law.

Computer-assisted audit technique (CAAT)—Any automated audit technique, such as generalized audit software (GAS), test data generators, computerized audit programs and specialized audit utilities

 ©ISACA. All Rights Reserved.

Configuration management (CM)—The control of changes to a set of configuration items over a system life cycle

Contingency planning—Process of developing advance arrangements and procedures that enable an enterprise to respond to an event that might occur by chance or unforeseen circumstances

Continuous auditing approach—Allows IS auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer

Control objective—A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process

Control practice—Key control mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business

Control risk—Risk that assets are lost/compromised or that financial statements are materially misstated, due to lack of, or ineffective, design and/or implementation of internal controls

Cookie—A web browser message used for the purpose of identifying users and possibly preparing customized web pages for them

Scope Notes: The first time a cookie is set, a user may be required to go through a registration process. Subsequent to this, whenever the cookie's message is sent to the server, a customized view based on that user's preferences can be produced. The browser's implementation of cookies has, however, brought several security concerns, allowing breaches of security and the theft of personal information (e.g., user passwords that validate the user identity and enable restricted web services).

Corrective control—A control designed to correct errors, omissions, unauthorized uses and intrusions, once they are detected

Countermeasure—The reduction of threats or vulnerabilities through any direct process

Critical success factor (CSF)—The most important issue or action for management to achieve control over and within its IT processes

D

Data custodian—Individual(s) and department(s) responsible for the storage and safeguarding of computerized data

Data Encryption Standard (DES)—A legacy algorithm for encoding binary data that was deprecated in 2006. DES and its variants were replaced by the Advanced Encryption Standard (AES).

Data leakage—Unauthorized transmission of data from an organization, either electronically or physically

Data owner—Individual(s) who has responsibility for the integrity, accurate reporting and use of computerized data

Data security—The controls that seek to maintain confidentiality, integrity and availability of information

Database—A collection of data, often with controlled redundancy, organized according to a schema to serve one or more applications. The data are stored so that they can be used by different programs without considering the data structure or organization. A common approach is used to add new data and modify and retrieve existing data.

Database administrator (DBA)—An individual or department responsible for the security and information classification of the shared data stored on a database system. This responsibility includes the design, definition and maintenance of the database.

Database management system (DBMS)—A software system that controls the organization, storage and retrieval of data in a database

Decision support systems (DSS)—An interactive system that provides the user with easy access to decision models and data to support semistructured decision-making tasks

Decryption—A technique used to recover the original plaintext from the ciphertext so that it is intelligible to the reader. The decryption is a reverse process of the encryption.

Decryption key—A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption

Degauss—The application of variable levels of alternating current for the purpose of demagnetizing magnetic recording media.

Scope Notes: The process involves increasing the alternating current field gradually from zero to some maximum value and back to zero, leaving a very low residue of magnetic induction on the media. Degauss loosely means to erase.

©ISACA. All Rights Reserved.

Detective control—Controls designed to detect and report when errors, omissions and unauthorized uses or entries occur

Digital certificate—An electronic credential that permits an entity to exchange information securely via the Internet using the public key infrastructure (PKI)

Digital signature—An electronic identification of a person or entity using a public key algorithm that serves as a way for the recipient to verify the identity of the sender, integrity of the data and proof of transaction

Disaster recovery plan (DRP)—A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster

Discovery sampling—A form of attribute sampling that is used to determine a specified probability of finding at least one example of an occurrence (attribute) in a population.

Discretionary access control (DAC)—Logical access control filters that may be configured or modified by the users or data owners

Domain name system (DNS)—A hierarchical database distributed across the Internet, which allows names to be resolved into IP addresses (and vice versa) to locate services, such as web and email servers

Domain name system (DNS) poisoning—Corrupts the table of an Internet server's DNS, replacing an Internet address with the address of a vagrant or scoundrel address

Scope Notes: If a web user looks for the page with that address, the request is redirected by the scoundrel entry in the table to a different address. Cache poisoning differs from another form of DNS poisoning in which the attacker spoofs valid email accounts and floods the in-boxes of administrative and technical contacts. Cache poisoning is related to URL poisoning or location poisoning, in which an Internet user's behavior is tracked by adding an identification number to the location line of the browser that can be recorded as the user visits successive pages on the site. It is also called DNS cache poisoning or cache poisoning.

Dry-pipe fire extinguisher system—A sprinkler system that does not have water in the pipes during idle usage, unlike a fully charged fire extinguisher system that has water in the pipes at all times

Scope Notes: The dry-pipe system is activated at the time of the fire alarm and water is emitted to the pipes from a water reservoir for discharge to the location of the fire.

Dynamic Host Configuration Protocol (DHCP)—A protocol used by networked computers (clients) to obtain IP addresses from DHCP servers, and parameters such as default gateways, subnet masks and domain name system (DNS) server IP addresses

Scope Notes: The DHCP server ensures that all IP addresses are unique (e.g., no IP address is assigned to a second client while the first client's assignment is valid [its lease has not expired]). Thus, IP address pool management is done by the server and not by a human network administrator.

E

Ecommerce—The processes by which enterprises conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology.

Scope Notes: Ecommerce encompasses both business-to-business (B2B) and business-to-consumer (B2C) ecommerce models, but does not include existing non-Internet ecommerce methods based on private networks such as electronic data interchange (EDI) and Society for Worldwide Interbank Financial Telecommunication (SWIFT).

Electronic data interchange (EDI)—The electronic transmission of transactions (information) between two enterprises. EDI promotes a more efficient paperless environment. EDI transmissions can replace the use of standard documents, including invoices or purchase orders.

Electronic funds transfer (EFT)—The exchange of money via telecommunications. EFT refers to any financial transaction that originates at a terminal and transfers a sum of money from one account to another.

Email/interpersonal messaging—An individual using a terminal, PC or an application can access a network to send an unstructured message to another individual or group of people

Embedded audit module (EAM)—Integral part of an application system that is designed to identify and report specific transactions or other information based on pre-determined criteria. Identification of reportable items occurs as part of real-time processing. Reporting may be real-time online or may use store and forward methods. Also known as integrated test facility or continuous auditing module.

Encryption—The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext).

Encryption key—A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext

End-user computing—The ability of end users to design and implement their own information system utilizing computer software products.

Enterprise resource planning (ERP)—A packaged business software system that allows an enterprise to automate and integrate the majority of its business processes; to share common data and practices across the entire enterprise; and to produce and access information in a real-time environment

Ethernet—A popular network protocol and cabling scheme that uses a bus topology and carrier sense multiple access/collision detection (CSMA/CD) to prevent network failures or collisions when two devices try to access the network at the same time

Evidence—Information that an auditor gathers in the course of performing an IS audit; relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support

Scope Notes: Audit perspective

Exception reports—An exception report is generated by a program that identifies transactions or data that appear to be incorrect.

Scope Notes: Exception reports may be outside a predetermined range or may not conform to specified criteria.

eXtensible Markup Language (XML)—Promulgated through the World Wide Web Consortium, XML is a web-based application development technique that allows designers to create their own customized tags, thus, enabling the definition, transmission, validation and interpretation of data between applications and enterprises.

Extranet—A private network that resides on the Internet and allows a company to securely share business information with customers, suppliers or other businesses as well as to execute electronic transactions.

Scope Notes: Different from an Intranet in that it is located beyond the company's firewall. Therefore, an extranet relies on the use of securely issued digital certificates (or alternative methods of user authentication) and encryption of messages. A virtual private network (VPN) and tunneling are often used to implement extranets, to ensure security and privacy.

F

Fallback procedures—A plan of action or set of procedures to be performed if a system implementation, upgrade or modification does not work as intended.

Scope Notes: May involve restoring the system to its state prior to the implementation or change. Fallback procedures are needed to ensure that normal business processes continue in the event of failure and should always be considered in system migration or implementation.

False authorization—Also called false acceptance, occurs when an unauthorized person is identified as an authorized person by the biometric system.

False enrollment—Occurs when an unauthorized person manages to enroll into the biometric system.

Scope Notes: Enrollment is the initial process of acquiring a biometric feature and saving it as a personal reference on a smart card, a PC or in a central database.

Feasibility study—Analysis of the known or anticipated need for a product, system or component to assess the degree to which the requirements, designs or plans can be implemented

Fiber-optic cable—Glass fibers that transmit binary signals over a telecommunications network.

Scope Notes: Fiber-optic systems have low transmission losses as compared to twisted-pair cables. They do not radiate energy or conduct electricity. They are free from corruption and lightning-induced interference, and they reduce the risk of wiretaps.

File Transfer Protocol (FTP)—A protocol used to transfer files over a Transmission Control Protocol/ Internet Protocol (TCP/IP) network (Internet, UNIX, etc.)

Financial audit—An audit designed to determine the accuracy of financial records and information.

Firewall—A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet

Firmware—The combination of a hardware device, e.g., an IC, and computer instructions and data that reside as read only software on that device. Such

©ISACA. All Rights Reserved.

software cannot be modified by the computer during processing.

Fourth-generation language (4GL)—High-level, user-friendly, nonprocedural computer language used to program and/or read and process computer files.

Frame relay—A packet-switched wide-area-network (WAN) technology that provides faster performance than older packet-switched WAN technologies.

Scope Notes: Best suited for data and image transfers. Because of its variable-length packet architecture, it is not the most efficient technology for real-time voice and video. In a frame-relay network, end nodes establish a connection via a permanent virtual circuit (PVC).

Function point analysis (FPA)—A technique used to determine the size of a development task, based on the number of function points

Scope Notes: Function points are factors such as inputs, outputs, inquiries and logical internal sites.

G

Gateway—A physical or logical device on a network that serves as an entrance to another network (e.g., router, firewall or software)

Generalized audit software (GAS)—Multipurpose audit software that can be used for general processes, such as record selection, matching, recalculation and reporting

Governance—The method by which an enterprise evaluates stakeholder needs, conditions and options to determine balanced, agreed-upon enterprise objectives to be achieved. It involves setting direction through prioritization, decision making and monitoring performance and compliance against the agreed-upon direction and objectives.

H

Hacker—An individual who attempts to gain unauthorized access to a computer system

Handprint scanner—A biometric device used to authenticate a user through palm scans

Hash total—The total of any numeric data field in a document or computer file. This total is checked against a control total of the same field to facilitate the accuracy of processing.

Help desk—A service offered via telephone/Internet by an enterprise to its clients or employees that provides information, assistance and troubleshooting advice regarding software, hardware or networks

Scope Notes: A help desk is staffed by people who can either resolve the problem on their own or escalate the problem to specialized personnel. A help desk is often equipped with dedicated customer relationship management (CRM) software that logs the problems and tracks them until they are solved.

Hierarchical database—A database structured in a tree/root or parent/child relationship.

Scope Notes: Each parent can have many children, but each child may have only one parent.

Honeypot—A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner so that their actions do not affect production systems

Hot site—A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster

Hypertext Markup Language (HTML)—A language designed for the creation of web pages with hypertext and other information to be displayed in a web browser; used to structure information–denoting certain text such as headings, paragraphs and lists–and can be used to describe, to some degree, the appearance and semantics of a document

I

Incident—A violation or imminent threat of violation of computer security policies, acceptable use policies, guidelines or standard security practices

Incident response—The response of an enterprise to a disaster or other significant event that may significantly affect the enterprise, its people or its ability to function productively. Incident response may include evacuation of a facility, initiating a disaster recovery plan (DRP), performing a damage assessment or any other measures necessary to bring an enterprise to a more stable status.

Information processing facility (IPF)—The computer room and support areas.

Information systems (IS)—The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies

Scope Notes: Information systems are distinct from information technology (IT) in that an information

system has an IT component that interacts with the process components.

Inherent risk—The level of risk or exposure that does not account for the actions management has taken or might take (e.g., implementing controls)

Instant messaging (IM)—An online mechanism or a form of real-time communication between two or more people based on typed text and multimedia data

Scope Notes: Text is conveyed via computers or another electronic device (e.g., cellular phone or handheld device) and connected over a network, such as the Internet.

Integrated services digital network (ISDN)—A public end-to-end digital telecommunications network with signaling, switching and transport capabilities that support a wide range of services accessed by standardized interfaces with integrated customer control

Scope Notes: The standard allows transmission of digital voice, video and data over 64-kbps lines.

Integrated test facilities (ITF)—A testing methodology in which test data are processed in production systems

Scope Notes: The data usually represent a set of fictitious entities such as departments, customers or products. Output reports are verified to confirm the correctness of the processing.

Integrity—The guarding against improper information modification or destruction. This includes ensuring information nonrepudiation and authenticity.

Internal controls—The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected

IP Security (IPSec)—A set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets

IT steering committee—An executive-management-level committee that assists in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects, and focuses on implementation aspects.

IT strategic plan—A long-term plan (i.e., three- to five-year horizon) in which business and IT management cooperatively describe how IT resources will contribute to the enterprise's strategic objectives (goals).

K

Key goal indicator (KGI)—A measure that tells management, after the fact, whether an IT process has achieved its business requirements; usually expressed in terms of information criteria.

Key performance indicator (KPI)—A type of performance measurement

L

Leased line—A communication line permanently assigned to connect two points, as opposed to a dial-up line that is only available and open when a connection is made by dialing the target machine or network. Also known as a dedicated line.

Licensing agreement—A contract that establishes the terms and conditions under which a piece of software is being licensed (i.e., made legally available for use) from the software developer (owner) to the user.

Local area network (LAN)—Communication network that serves several users within a specified limited geographic area

Log—To record details of information or events in an organized record-keeping system, usually sequenced in the order in which they occurred

Logical access controls—The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files

Logon—The act of connecting to the computer, which typically requires entry of a user ID and password into a computer terminal.

M

Malware—Short for malicious software. Designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Examples of malware include computer viruses, worms, Trojan horses, spyware and adware.

Mandatory access control (MAC)—Logical access control filters used to validate access credentials that cannot be controlled or modified by normal users or data owners

Media access control (MAC)—Lower sublayer of the OSI Model Data Link layer

Middleware—Another term for an application programmer interface (API). It refers to the interfaces that allow programmers to access lower- or higher-level

©ISACA. All Rights Reserved.

services by providing an intermediary layer that includes function calls to the services.

Mobile site—The use of a mobile/temporary facility to serve as a business resumption location. The facility can usually be delivered to any site and can house information technology and staff.

N

Network—A system of interconnected computers and the communication equipment used to connect them.

Network administrator—Responsible for planning, implementing and maintaining the telecommunications infrastructure; also may be responsible for voice networks.

Scope Notes: For smaller enterprises, the network administrator may also maintain a local area network (LAN) and assist end users.

Network attached storage (NAS)—Utilizes dedicated storage devices that centralize storage of data.

Scope Notes: NA storage devices generally do not provide traditional file/print or application services.

Network interface card (NIC)—A communication card that when inserted into a computer, allows it to communicate with other computers on a network.

Scope Notes: Most NICs are designed for a particular type of network or protocol.

Nondisclosure agreement (NDA)—A legal contract between at least two parties that outlines confidential materials that the parties wish to share with one another for certain purposes, but wish to restrict from generalized use; a contract through which the parties agree not to disclose information covered by the agreement.

Scope Notes: Also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement. An NDA creates a confidential relationship between the parties to protect any type of trade secret. As such, an NDA can protect non-public business information. In the case of certain governmental entities, the confidentiality of information other than trade secrets may be subject to applicable statutory requirements, and in some cases may be required to be revealed to an outside party requesting the information. Generally, the governmental entity will include a provision in the contract to allow the seller to review a request for information that the seller identifies as confidential and the seller may appeal such a decision requiring disclosure. NDAs are commonly signed when two companies or individuals are considering doing business together and need to understand the processes used in one another's businesses solely for the purpose of evaluating the potential business relationship. NDAs can be "mutual," meaning that both parties are restricted in their use of the materials provided, or they can only restrict a single party. It is also possible for an employee to sign an NDA or NDA-like agreement with a company at the time of hiring; in fact, some employment agreements will include a clause restricting "confidential information" in general.

O

Operating system (OS)—A master control program that runs the computer and acts as a scheduler and traffic controller

Scope Notes: The operating system is the first program copied into the computer memory after the computer is turned on; it must reside in memory at all times. It is the software that interfaces between the computer hardware (disk, keyboard, mouse, network, modem and printer) and the application software (word processor, spreadsheet email) which also controls access to the devices, is partially responsible for security components and sets the standards for the application programs that run in it.

Operational audit—An audit designed to evaluate the various internal controls, economy and efficiency of a function or department.

Outsourcing—A formal agreement with a third party to perform IS or other business functions for an enterprise

P

Paper test—A walk-through of the steps of a regular test, but without actually performing the steps.

Scope Notes: Usually used in disaster recovery and contingency testing; team members review and become familiar with the plans and their specific roles and responsibilities

Password—A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system

Patch management—An area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system to maintain up-to-date software and often to address security risk

Scope Notes: Patch management tasks include maintaining current knowledge of available patches,

 ©ISACA. All Rights Reserved.

deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation and documenting all associated procedures, such as specific configurations required. A number of products are available to automate patch management tasks. Patches are sometimes ineffective and can sometimes cause more problems than they fix. Patch management experts suggest that system administrators take simple steps to avoid problems, such as performing backups and testing patches on noncritical systems prior to installations. Patch management can be viewed as part of change management.

Penetration testing—A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers

Phishing—A type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering

Scope Notes: Phishing attacks may take the form of masquerading as a lottery organization advising the recipient or the user's bank of a large win; in either case, the intent is to obtain account and personal identification number (PIN) details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.

Phreakers—Those who crack security, most frequently telephone and other communication networks.

Plaintext—Digital information, such as cleartext, that is intelligible to the reader.

Point-to-Point Protocol (PPP)—A protocol used for transmitting data between two ends of a connection.

Policy—A document that communicates required and prohibited activities and behaviors

Preventive control—An internal control that is used to avoid undesirable events, errors and other occurrences that an enterprise has determined could have a negative material effect on a process or end product.

Privacy—The right of an individual to trust that others will appropriately and respectfully use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes for which it was collected or derived

Private key cryptosystems—A cryptosystem that involves secret, private keys. The keys are also known as "symmetric ciphers" because the same key both encrypts message plaintext from the sender and decrypts resulting ciphertext for a recipient.

Procedure—A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.

Process—Generally, a collection of activities influenced by the enterprise's policies and procedures that takes inputs from a number of sources, (including other processes), manipulates the inputs and produces outputs.

Protocol—The rules by which a network operates and controls the flow and priority of transmissions

Public key cryptosystem—A cryptosystem that combines a widely distributed public key and a closely held, protected private key. A message that is encrypted by the public key can only be decrypted by the mathematically related counterpart private key. Conversely, only the public key can decrypt data that was encrypted by its corresponding private key.

Public key encryption—A cryptographic system that uses two keys: one is a public key, which is known to everyone, and the second is a private or secret key, which is only known to the recipient of the message. See also Asymmetric Key.

Public key infrastructure (PKI)—A series of processes and technologies for the association of cryptographic keys with the entity to whom those keys were issued

Q

Quality assurance (QA)—A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. (ISO/IEC 24765)

R

Reciprocal agreement—Emergency processing agreement between two or more enterprises with similar equipment or applications.

Scope Notes: Typically, participants of a reciprocal agreement promise to provide processing time to each other when an emergency arises.

Recovery point objective (RPO)—Determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.

©ISACA. All Rights Reserved.

Recovery strategy—An approach by an enterprise that will ensure its recovery and continuity in the face of a disaster or other major outage.

Scope Notes: Plans and methodologies are determined by the enterprise's strategy. There may be more than one methodology or solution for an enterprise's strategy. Examples of methodologies and solutions include: contracting for hot site or cold site, building an internal hot site or cold site, identifying an alternate work area, a consortium or reciprocal agreement, contracting for mobile recovery or crate and ship, and many others.

Recovery time objective (RTO)—The amount of time allowed for the recovery of a business function or resource after a disaster occurs

Registration authority (RA)—An authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it

Remote access service (RAS)—Refers to any combination of hardware and software to enable the remote access to tools or information that typically reside on a network of IT devices.

Scope Notes: Originally coined by Microsoft when referring to their built-in NT remote access tools, RAS was a service provided by Windows NT which allowed most of the services that would be available on a network to be accessed over a modem link. Over the years, many vendors have provided both hardware and software solutions to gain remote access to various types of networked information. In fact, most modern routers include a basic RAS capability that can be enabled for any dial-up interface.

Remote procedure call (RPC)—The traditional Internet service protocol widely used for many years on UNIX-based operating systems and supported by the Internet Engineering Task Force (IETF) that allows a program on one computer to execute a program on another (e.g., server).

Scope Notes: The primary benefit derived from its use is that a system developer need not develop specific procedures for the targeted computer system. For example, in a client-server arrangement, the client program sends a message to the server with appropriate arguments, and the server returns a message containing the results of the program executed. Common Object Request Broker Architecture (CORBA) and Distributed Component Object Model (DCOM) are two newer object-oriented methods for related RPC functionality.

Repeaters—A physical layer device that regenerates and propagates electrical signals between two network segments.

Scope Notes: Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) distorted by transmission loss due to reduction of signal strength during transmission (i.e., attenuation)

Request for proposal (RFP)—A document distributed to software vendors requesting them to submit a proposal to develop or provide a software product.

Ring topology—A type of local area network (LAN) architecture in which the cable forms a loop, with stations attached at intervals around the loop.

Scope Notes: In ring topology, signals transmitted around the ring take the form of messages. Each station receives the messages and each station determines, on the basis of an address, whether to accept or process a given message. However, after receiving a message, each station acts as a repeater, retransmitting the message at its original signal strength.

Risk—The combination of the likelihood of an event and its impact (ISACA)

Risk analysis—The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats.

Scope Notes: It often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of that event.

Risk appetite—The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission.

Risk assessment—A process used to identify and evaluate risk and its potential effects

Scope Notes: Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan. Risk assessments are also used to manage project delivery risk and project benefit risk.

Risk evaluation—The process of comparing the estimated risk against given risk criteria to determine the significance of the risk. [ISO/IEC Guide 73:2002].

Risk management—The coordinated activities to direct and control an enterprise with regard to risk

Scope Notes: In the International Standard, the term "control" is used as a synonym for "measure." (ISO/IEC Guide 73:2002)

Risk mitigation—The management of risk through the use of countermeasures and controls (ISACA)

Risk tolerance—The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives

Risk transfer—The process of assigning risk to another enterprise, usually through the purchase of an insurance policy or by outsourcing the service

Scope Notes: Also known as risk sharing

Risk treatment—The process of selection and implementation of measures to modify risk (ISO/IEC Guide 73:2002)

Router—A networking device that can send (route) data packets from one local area network (LAN) or wide area network (WAN) to another, based on addressing at the network layer (Layer 3) in the open systems interconnection (OSI) model

Scope Notes: Networks connected by routers can use different or similar networking protocols. Routers usually are capable of filtering packets based on parameters, such as source addresses, destination addresses, protocol and network applications (ports).

RSA (RSA)—A public key cryptosystem developed by R. Rivest, A. Shamir and L. Adleman used for both encryption and digital signatures

Scope Notes: The RSA has two different keys, the public encryption key and the secret decryption key. The strength of the RSA depends on the difficulty of the prime number factorization. For applications with high-level security, the number of the decryption key bits should be greater than 512 bits.

S

Secure Sockets Layer (SSL)—A protocol that is used to transmit private documents through the Internet

Scope Notes: The SSL protocol uses a private key to encrypt the data that are to be transferred through the SSL connection.

Segregation/separation of duties (SoD)—A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets.

Scope Notes: Segregation/separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

Service level agreement (SLA)—An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured

Simple Object Access Protocol (SOAP)—A platform-independent formatted protocol based on extensible markup language (XML) enabling applications to communicate with each other over the Internet.

Scope Notes: Use of SOAP may provide a significant security risk to web application operations because use of SOAP piggybacks onto a web-based document object model and is transmitted via HyperText Transfer Protocol (HTTP) (port 80) to penetrate server firewalls, which are usually configured to accept port 80 and port 21 File Transfer Protocol (FTP) requests. Web-based document models define how objects on a web page are associated with each other and how they can be manipulated while being sent from a server to a client browser. SOAP typically relies on XML for presentation formatting and also adds appropriate HTTP-based headers to send it. SOAP forms the foundation layer of the web services stack, providing a basic messaging framework on which more abstract layers can build. There are several different types of messaging patterns in SOAP, but by far the most common is the Remote Procedure Call (RPC) pattern, in which one network node (the client) sends a request message to another node (the server), and the server immediately sends a response message to the client.

Spyware—Software whose purpose is to monitor a computer user's actions (e.g., websites visited) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user

Standard—A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as International Organization for Standardization (ISO).

Star topology—A type of local area network (LAN) architecture that utilizes a central controller to which all nodes are directly connected.

Scope Notes: With star topology, all transmissions from one station to another pass through the central controller which is responsible for managing and controlling all

©ISACA. All Rights Reserved.

communication. The central controller often acts as a switching device.

Statistical sampling—A method of selecting a portion of a population, by means of mathematical calculations and probabilities, for the purpose of making scientifically and mathematically sound inferences regarding the characteristics of the entire population.

Storage area networks (SANs)—A variation of a local area network (LAN) that is dedicated for the express purpose of connecting storage devices to servers and other computing devices.

Scope Notes: SANs centralize the process for the storage and administration of data.

Structured Query Language (SQL)—A language used to interrogate and process data in a relational database. Originally developed for IBM mainframes, many implementations have been created for mini- and microcomputer database applications. SQL commands can be used to interactively work with a database or embedded with a programming language to interface with a database.

Switches—Typically associated as a data link layer device, switches enable local area network (LAN) segments to be created and interconnected, which has the added benefit of reducing collision domains in Ethernet-based networks.

System development life cycle (SDLC)—The phases deployed in the development or acquisition of a software system.

Scope Notes: SDLC is an approach used to plan, design, develop, test and implement an application system or a major modification to an application system. Typical phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review, but not the service delivery or benefits realization activities.

T

Threat—Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm

Scope Notes: A potential cause of an unwanted incident (ISO/IEC 13335)

Token ring topology—A type of local area network (LAN) ring topology in which a frame containing a specific format, called the token, is passed from one station to the next around the ring.

Scope Notes: When a station receives the token, it is allowed to transmit. The station can send as many frames as desired until a predefined time limit is reached. When a station either has no more frames to send or reaches the time limit, it transmits the token. Token passing prevents data collisions that can occur when two computers begin transmitting at the same time.

Transmission Control Protocol Internet Protocol (TCP/IP)—Provides the basis for the Internet; a set of communication protocols that encompass media access, packet transport, session communication, file transfer, electronic mail (email), terminal emulation, remote file access and network management

Trojan horse—Purposefully hidden malicious or damaging code within an authorized computer program

Twisted pair—A low-capacity transmission medium; a pair of small, insulated wires that are twisted around each other to minimize interference from other wires in the cable.

U

Uninterruptible power supply (UPS)—Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level.

Universal Serial BUS (USB)—An external bus standard that provides capabilities to transfer data at a rate of 12 Mbps.

Scope Notes: A USB port can connect up to 127 peripheral devices.

V

Variable sampling—A sampling technique used to estimate the average or total value of a population based on a sample; a statistical model used to project a quantitative characteristic, such as a monetary amount.

Voice-over Internet Protocol (VoIP)—Also called IP Telephony, Internet Telephony and Broadband Phone, a technology that makes it possible to have a voice conversation over the Internet or over any dedicated Internet Protocol (IP) network instead of over dedicated voice transmission lines

Vulnerability—A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

Vulnerability analysis—A process of identifying and classifying vulnerabilities

W

Warm site—Similar to a hot site but not fully equipped with all of the necessary hardware needed for recovery.

White box testing—A testing approach that uses knowledge of a program/module's underlying implementation and code intervals to verify its expected behavior.

Wi-Fi Protected Access (WPA)—A class of security protocols used to secure wireless (Wi-Fi) computer networks

Wide area network (WAN)—A computer network connecting multiple offices or buildings over a larger area

Wide area network (WAN) switch—A data link layer device used for implementing various WAN technologies such as asynchronous transfer mode, point-to-point frame relay solutions, and integrated services digital network (ISDN).

Scope Notes: WAN switches are typically associated with carrier networks providing dedicated WAN switching and router services to enterprises via T-1 or T-3 connections.

Wired Equivalent Privacy (WEP)—A scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks (also known as Wi-Fi networks).

Scope Notes: Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network (in particular, it does not protect users of the network from each other), hence the name. Several serious weaknesses were identified by cryptanalysts, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the weaknesses, WEP provides a level of security that can deter casual snooping.

Wiretapping—The practice of eavesdropping on information being transmitted over telecommunications links.

X

X.25 Interface—An interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode on some public data networks.

Glossary terms are provided for reference within the CISA Official Review Manual. Because term definitions may evolve due to the changing technological environment, the CISA candidate may also want to be familiar with ISACA's Glossary, which can be viewed at *www.isaca.org/glossary*.

©ISACA. All Rights Reserved.

Page intentionally left blank

Acronyms

The following is a list of common acronyms used throughout the CISA Review Manual. These may be defined in the text for clarity.

4GL	Fourth-generation language
ACL	Access control list
AES	Advanced Encryption Standard
AH	Authentication header
AI	Artificial intelligence
AICPA	American Institute of Certified Public Accountants
ALE	Annual loss expectancy
API	Application programming interface
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASIC	Application-specific integrated circuit
ATDM	Asynchronous time division multiplexing
ATM	Asynchronous Transfer Mode
ATM	Automated teller machine
B-to-B	Business-to-business
B-to-C	Business-to-consumer
B-to-E	Business-to-employee
B-to-G	Business-to-government
BCI	Business Continuity Institute
BCM	Business continuity management
BCP	Business continuity plan
BCP	Business continuity planning
BDA	Business dependency assessment
BI	Business intelligence
BIA	Business impact analysis
BIMS	Biometric Information Management and Security
BIOS	Basic Input/Output System
Bit	Binary digit
BLP	Bypass label process
BNS	Backbone network services
BPR	Business process reengineering
BRP	Business recovery (or resumption) plan
BSC	Balanced scorecard
C-to-G	Consumer-to-government
CA	Certificate authority
CAAT	Computer-assisted audit technique
CASE	Computer-aided software engineering
CCK	Complementary Code Keying
CCM	Constructive Cost Model
CCTV	Closed-circuit television
CDDF	Call Data Distribution Function
CDPD	Cellular Digital Packet Data
CEO	Chief executive officer
CERT	Computer emergency response team
CGI	Common gateway interface
CIA	Confidentiality, integrity and availability
CIAC	Computer Incident Advisory Capability
CICA	Canadian Institute of Chartered Accountants
CIM	Computer-integrated manufacturing
CIO	Chief information officer
CIS	Continuous and intermittent simulation
CISO	Chief information security officer
CMDB	Configuration management database
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CNC	Computerized Numeric Control
COCOMO2	Constructive Cost Model
CODASYL	Conference on Data Systems Language
COM	Component Object Model
COM/DCOM	Component Object Model/Distributed Component Object Model
COOP	Continuity of operations plan
CORBA	Common Object Request Broker Architecture
CoS	Class of service
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPM	Critical Path Methodology
CPO	Chief privacy officer
CPS	Certification practice statement
CPU	Central processing unit
CRC	Cyclic redundancy check
CRL	Certificate revocation list
CRM	Customer relationship management
CSA	Control self-assessment
CSF	Critical success factor
CSIRT	Computer security incident response team
CSMA/CA	Carrier sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier sense Multiple Access/Collision Detection
CSO	Chief security officer
CSU-DSU	Channel service unit/digital service unit
DAC	Discretionary access control
DASD	Direct access storage device
DBA	Database administrator
DBMS	Database management system
DCE	Data communications equipment
DCE	Distributed computing environment
DCOM	Distributed Component Object Model (Microsoft)
DCT	Discrete Cosine Transform
DD/DS	Data dictionary/directory system
DDL	Data Definition Language
DDN	Digital Divide Network
DDoS	Distributed denial of service
DECT	Digital Enhanced Cordless Telecommunications
DES	Data Encryption Standard
DFD	Data flow diagram
DHCP	Dynamic Host Configuration Protocol
DID	Direct inward dial
DIP	Document image processing
DLL	Dynamic link library
DMS	Disk management system
DMZ	Demilitarized zone
DNS	Domain name system
DoS	Denial of service
DRII	Disaster Recovery Institute International
DRM	Digital rights management

©ISACA. All Rights Reserved.

DRP	Disaster recovery plan
DRP	Disaster recovery planning
DSL	Digital subscriber lines
DSS	Decision support systems
DSSS	Direct Sequence Spread Spectrum
DTE	Data terminal equipment
DTR	Data terminal ready
DW	Data warehouse
EA	Enterprise architecture
EAC	Estimates at completion
EAI	Enterprise application integration
EAM	Embedded audit module
EAP	Extensible Authentication Protocol
EBCDIC	Extended Binary-coded for Decimal Interchange Code
EC	Electronic commerce
ECC	Elliptical Curve Cryptography
EDFA	Enterprise data flow architecture
EDI	Electronic data interchange
EER	Equal-error rate
EFT	Electronic funds transfer
EIGRP	Enhanced Interior Gateway Routing Protocol
EJB	Enterprise java beans
EMI	Electromagnetic interference
EMRT	Emergency response time
ERD	Entity relationship diagram
ERP	Enterprise resource planning
ESP	Encapsulating security payload
EVA	Earned value analysis
FAR	False-acceptance rate
FAT	File allocation table
FC	Fibre channels
FDDI	Fiber Distributed Data Interface
FDM	Frequency division multiplexing
FEA	Federal enterprise architecture
FEMA	Federal Emergency Management Association (USA)
FER	Failure-to-enroll rate
FERC	Federal Energy Regulatory Commission (USA)
FFIEC	Federal Financial Institutions Examination Council (USA)
FFT	Fast Fourier Transform
FHSS	Frequency-hopping spread spectrum
FIPS	Federal Information Processing Standards
FP	Function point
FPA	Function point analysis
FRAD	Frame relay assembler/disassembler
FRB	Federal Reserve Board (USA)
FRR	False-rejection rate
FTP	File Transfer Protocol
GAS	Generalized audit software
GID	Group ID
GIS	Geographic information systems
GPS	Global positioning system
GSM	Global system for mobile communications
GUI	Graphical user interface
HA	High availability
HD-DVD	High definition/high density-digital video disc
HDLC	High-level data link control
HIPAA	Health Insurance Portability and Accountability Act (USA)
HIPO	Hierarchy input-process-output
HMI	Human machine interfacing
HTML	Hypertext Markup Language
HTTP	Hypertext Transmission Protocol
HTTPS	Secured Hypertext Transmission Protocol
HW/SW	Hardware/software
I&A	Identification and authentication
I/O	Input/output
ICMP	Internet Control Message Protocol
ICT	Information and communication technologies
IDE	Integrated development environment
IDEF1X	Integration Definition for Information Modeling
IDS	Intrusion detection system
IETF	Internet Engineering Task Force
IMS	Integrated manufacturing systems
IP	Internet protocol
IPF	Information processing facility
IPL	Initial program load
IPMA	International Project Management Association
IPRs	Intellectual property rights
IPS	Intrusion prevention system
IPSec	IP Security
IPX	Internetwork Packet Exchange
IR	Infrared
IRC	Internet relay chat
IrDA	Infrared Data Association
IRM	Incident response management
IS	Information systems
IS/DRP	IS disaster recovery planning
ISAKMP/	Internet Security Association and Key Oakley Management Protocol/Oakley
ISAM	Indexed Sequential Access Method
ISDN	Integrated services digital network
ISO	International Organization for Standardization
ISP	Internet service provider
IT	Information technology
ITF	Integrated test facility
ITIL	Information Technology Infrastructure Library
ITSM	IT service management
ITT	Invitation to tender
ITU	International Telecommunications Union
IVR	Interactive voice response
JIT	Just in time
KB	Knowledge base
KGI	Key goal indicator
KPI	Key performance indicator
KRI	Key risk indicator
L2TP	Layer 2 Tunneling Protocol
LAN	Local area network
LCP	Link Control Protocol
M&A	Mergers and acquisition
MAC	Mandatory access control
MAC	Message Authentication Code
MAC	Address Media Access Control Address
MAN	Metropolitan area network
MAP	Manufacturing accounting and production

MIS	Management information system
MODEM	Modulator/demodulator
MOS	Maintenance out of service
MPLS	Multiprotocol label switching
MRP	Manufacturing resources planning
MSAUs	Multistation access units
MTBF	Mean time between failures
MTS	Microsoft's Transaction Server
MTTR	Mean time to repair
NAP	Network access point
NAS	Network access server
NAS	Network attached storage
NAT	Network address translation
NCP	Network Control Protocol
NDA	Nondisclosure agreement
NFPA	National Fire Protection Agency (USA)
NFS	Network File System
NIC	Network interface card
NIST	National Institute of Standards and Technology (USA)
NNTP	Network News Transfer Protocol
NSP	Name Server Protocol
NSP	Network service provider
NTFS	NT file system
NTP	Network Time Protocol
OBS	Object breakdown structure
OCSP	Online Certificate Status Protocol
ODC	On-demand computing
OECD	Organization for Economic Cooperation and Development
OEP	Occupant emergency plan
OLAP	Online analytical processing
OOSD	Object-oriented system development
ORB	Object request broker
OS	Operating system
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAD	Packet assembler/disassembler
PAN	Personal area network
PC	Personal computer/microcomputer
PCR	Program change request
PDCA	Plan-do-check-act
PDN	Public data network
PER	Package-enabled reengineering
PERT	Program Evaluation Review Technique
PICS	Platform for Internet Content Selection
PID	Process ID
PID	Project initiation document
PIN	Personal identification number
PKI	Public key infrastructure
PLC	Programmable logic controllers
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
POC	Proof of concept
POP	Proof of possession
POS	Point of sale (or Point-of-sale systems)
PPP	Point-to-point Protocol
PPPoE	Point-to-point Protocol Over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PR	Public relations
PRD	Project request document
PRINCE2	Projects in Controlled Environments 2
PROM	Programmable Read-only Memory
PSTN	Public switched telephone network
PVC	Permanent virtual circuit
QA	Quality assurance
QAT	Quality assurance testing
RA	Registration authority
RAD	Rapid application development
RAID	Redundant Array of Inexpensive Disks
RAM	Random access memory
RAS	Remote access service
RBAC	Role-based access control
RDBMS	Relational database management system
RF	Radio frequencies
RFI	Request for information
RFID	Radio frequency identification
RFP	Request for proposal
RIP	Routing Information Protocol
RMI	Remote method invocation
ROI	Return on investment
ROLAP	Relational online analytical processing
ROM	Read-only memory
RPC	Remote procedure call
RPO	Recovery point objective
RSN	Robust secure network
RST	Reset
RTO	Recovery time objective
RTU	Remote terminal unit
RW	Rewritable
S/HTTP	Secure Hypertext Transfer Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
SA	Security Association
SAN	Storage area network
SANS	SysAdmin, Audit, Network, Security
SAS	Statement on Auditing Standards
SCOR	Supply chain operations reference
SD/MMC	Secure digital multimedia card
SDLC	System development life cycle
SDO	Service delivery objective
SEC	Securities and Exchange Commission (USA)
SET	Secure electronic transactions
SIP	Service improvement plan
SLA	Service level agreement
SLIP	Serial Line Internet Protocol
SLM	Service level management
SLOC	Source lines of code
SMART	Specific, measurable, attainable, realistic, timely
SME	Subject matter expert
SMF	System management facility
SMTP	Simple Mail Transport Protocol
SNA	Systems network architecture
SNMP	Simple Network Management Protocol
SO	Security officer
SOA	Service-oriented architectures
SOAP	Simple Object Access Protocol
SOHO	Small office-home office
SOW	Statement of work
SPI	Security parameter index
SPOC	Single point of contact
SQL	Structured Query Language
SSH	Secure Shell
SSID	Service set identifier
SSL	Secure Sockets Layer
SSO	Single sign-on
SVC	Switched virtual circuits
SYSGEN	System generation

©ISACA. All Rights Reserved.

TACACS	Terminal Access Controller Access Control System
TCO	Total cost of ownership
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP/UDP	Transmission Control Protocol/User Datagram Protocol
TDM	Time-division multiplexing
TELNET	Teletype network
TES	Terminal emulation software
TFTP	Trivial File Transport Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport layer security
TP	monitors Transaction processing monitors
TQM	Total quality management
TR	Technical report
UAT	User acceptance testing
UBE	Unsolicited bulk email
UDDI	Universal description, discovery and integration
UDP	User Datagram Protocol
UID	User ID
UML	Unified Modeling Language
UPS	Uninterruptible power supply
URI	Uniform resource identifier
URL	Uniform resource locator
URN	Uniform resource name
USB	Universal Serial Bus
VLAN	Virtual local area network
VoIP	Voice-over IP
VPN	Virtual private network
WAN	Wide area network
WAP	Wireless Application Protocol
WBS	Work breakdown structure
WEP	Wired Equivalent Privacy
WLAN	Wireless local area network
WML	Wireless Markup Language
WORM	Write Once and Read Many
WP	Work package
WPA	Wi-Fi Protected Access
WPAN	Wireless personal area network
WSDL	Web Services Description Language
WWAN	Wireless wide area network
XBRL	Extensible Business Reporting Language
XML	Extensible Markup Language
XOR	Exclusive-OR
Xquery	XML query
XSL	Extensible Stylesheet Language

 ©ISACA. All Rights Reserved.


9781604209815.