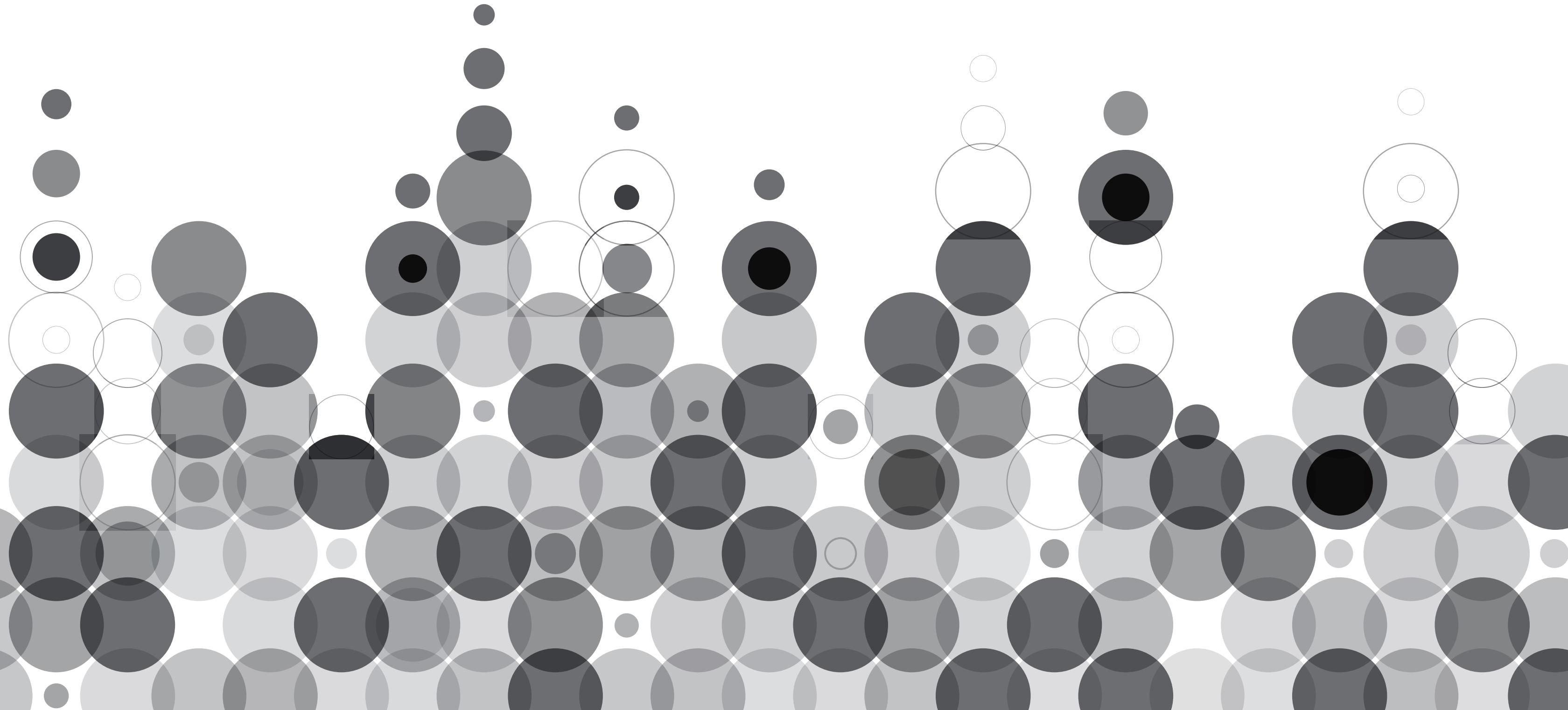
ISACA®
Trust in, and value from, information systems

26th Edition

CISA

Review Manual

CISA® Certified Information Systems Auditor®
An ISACA® Certification



ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

In addition, ISACA advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials.

Disclaimer

ISACA has designed and created *CISA® Review Manual 26th Edition* primarily as an educational resource to assist individuals preparing to take the CISA certification exam. It was produced independently from the CISA exam and the CISA Certification Working Group, 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 CISA exam.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

ISBN 978-1-60420-367-7
CISA® Review Manual 26th Edition
Printed in the United States of America

CISA REVIEW MANUAL 26TH EDITION

ISACA is pleased to offer the 26th edition of the *CISA® Review Manual*. The purpose of this manual is to provide CISA candidates with updated technical information and references to assist in preparation and study for the Certified Information Systems Auditor exam.

The content in the manual has been substantially updated. Most of the changes made were to recognize and map to the new task and knowledge statements that resulted from the new CISA job practice analysis. Further details regarding the new job practice can be found in the section titled NEW–CISA Job Practice and can be viewed at *www.isaca.org/cisajobpractice* and in the ISACA Exam Candidate Information Guide at *www.isaca.org/examguide*. **The exam is based on the task and knowledge statements in the job practice.** The development of the task and knowledge statements involved thousands of CISAs and other industry professionals worldwide who served as committee members, focus group participants, subject matter experts and survey respondents.

The *CISA® Review Manual* is updated to keep pace with rapid changes in the IS audit, control and security professions. As with previous manuals, the 26th 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 manual readers.

Your comments and suggestions regarding this manual are welcomed. After taking the exam, please take a moment to complete the online questionnaire *(www.isaca.org/studyaidsevaluation)*. Your observations will be invaluable for the preparation of the next edition of the *CISA® Review Manual*.

The sample questions contained in this manual are designed to depict the type of questions typically found on the CISA exam and to provide further clarity to the content presented in this manual. The CISA exam is a practice-based exam. Simply reading the reference material in this manual will not properly prepare candidates for the exam. The sample questions are included for guidance only. Scoring results do not indicate future individual exam success.

Certification has resulted in a positive impact on many careers, and the CISA designation is respected and acknowledged by organizations around the world. We wish you success with the CISA exam. Your commitment to pursue the leading certification in IS audit, assurance, control and security is exemplary.

ACKNOWLEDGMENTS

The 26th edition of the *CISA® 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 has become the hallmark of contributors to this manual. Their participation and insight are truly appreciated.

Special thanks go to Ian J. Cooke, CISA, CGEIT, CRISC, CFE, COBIT Foundation, CPTS, ITIL-F, Six Sigma Green Belt, An Post, Ireland, and Jeffrey L. Roth, CISA, CGEIT, CISSP-ISSEP, QSA, USA, who worked on the 26th edition of the *CISA® Review Manual*.

Expert Reviewers

Rajeev Andharia, CISA, CISSP, COBIT 5 Assessor & Implementation, ITIL Expert, PMP, Business Technology Partner Pte Ltd., Singapore
Sunil Bakshi, CISA, CISM, CGEIT, CRISC, National Institute of Bank Management, India
Ishwar Chandra, CISA, FCA, I C & Associates, India
James T. Enstrom, CISA, CRISC, CIA, Chicago Board Options Exchange, USA
Mohamed Gohar, CISA, CISM, Egypt
Florin-Mihai Iliescu, CISA, Info-Logica Silverline SRL, Romania
Binoy Koonammavu, CISA, CISM, CRISC, CISSP, ValueMentor Infosec Pvt. Ltd, India
Shruti Shrikant Kulkarni, CISA, CRISC, CISSP, CPISI, CCSK, ITIL V3 Expert, Monitise Group Ltd, United Kingdom
S. Krishna Kumar, CISA, CISM, CGEIT, India
Juan Carlos López, CISA, CGEIT, CRISC, COBIT Implementation, COBIT Certified Assessor, ITIL, PMP, Exacta Consulting, Ecuador
Balakrishnan Natarajan, CISA, CISM, Pivotal Software, Inc., USA
S. Peter Nota, CISA, CISM, CISSP, MBCS, PCI-ISA, Premier Farnell plc, United Kingdom
Derek J. Oliver, Ph.D., CISA, CISM, CRISC, DBA, Ravenswood Consultants Ltd., United Kingdom
Opeyemi Onifade, CISA, CISM, CGEIT, Afenoid Enterprise Limited, Nigeria
Manuel (Manolo) Palao, CISA, CISM, CGEIT, Accredited COBIT 5 Trainer, COBIT 5 Certified Assessor, P&T: S, SLU | Innovation & Technology Trends Institute (iTTi), Spain
Robert D. Prince, CISA, CISSP, USA
Beth Pumo, CISA, CISM, Kaiser Permanente, USA
Sree Krishna Rao, CISA, Ernst & Young LLP, United Kingdom
Markus Schiemer, CISA, CGEIT, CRISC, Microsoft Österreich GmbH, Austria
Hilary Shreter, CISA, PMP, USA
Katalin Szenes, Ph.D., CISA, CISM, CGEIT, CISSP, Obuda University, Hungary
Hui Zhu, CISA, CISM, CGEIT, BlueImpact Ltd., Canada
Tichaona Zororo, CISA, CISM, CRISC, CGEIT, Certified COBIT 5 Assessor, CIA, CRMA, EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

ISACA has begun planning the next edition of the *CISA® Review Manual*. Volunteer participation drives the success of the manual. If you are interested in becoming a member of the select group of professionals involved in this global project, we want to hear from you. Please email us at *studymaterials@isaca.org.*

NEW—CISA JOB PRACTICE

BEGINNING IN 2016, THE CISA EXAM WILL TEST THE NEW CISA JOB PRACTICE.

An international job practice analysis is conducted at least every five years or sooner to maintain the validity of the CISA certification program. A new job practice forms the basis of the CISA exam beginning in June 2016.

The primary focus of the job practice is the current tasks performed and the knowledge used by CISAs. By gathering evidence of the current work practice of CISAs, ISACA is able to ensure 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 2016 job practice reflects the areas of study to be tested and is compared below to the previous job practice. The complete CISA job practice can be found at *www.isaca.org/cisajobpractice.*

Previous CISA Job Practice	New 2016 CISA Job Practice
Domain 1: The Process of Auditing Information Systems (14%) Domain 2: Governance and Management of IT (14%) Domain 3: Information Systems Acquisition, Development and Implementation (19%) Domain 4: Information Systems Operations, Maintenance and Support (23%) Domain 5: Protection of Information Assets (30%)	Domain 1: The Process of Auditing Information Systems (21%) Domain 2: Governance and Management of IT (16%) Domain 3: Information Systems Acquisition, Development and Implementation (18%) Domain 4: Information Systems Operations, Maintenance and Service Management (20%) Domain 5: Protection of Information Assets (25%)

Page intentionally left blank

Table of Contents

About This Manual 17
Overview 17
Format of This Manual 17
Evaluation of This Manual 18
About the CISA Review Questions, Answers and Explanations Manual 18
CISA Online Review Course 18

Chapter 1:
The Process of Auditing Information Systems 19

Section One: Overview 20
Definition 20
Objectives 20
Task and Knowledge Statements 20
Tasks 20
Knowledge Statements 20
Suggested Resources for Further Study 28
Self-assessment Questions 29
Answers to Self-assessment Questions 30

Section Two: Content 32
1.1 Quick Reference 32
1.2 Management of the IS Audit Function 32
1.2.1 Organization of the IS Audit Function 32
1.2.2 IS Audit Resource Management 33
1.2.3 Audit Planning 33
Annual Planning 33
Individual Audit Assignments 33
1.2.4 Effect of Laws and Regulations on IS Audit Planning 34
1.3 ISACA IS Audit and Assurance Standards and Guidelines 35
1.3.1 ISACA Code of Professional Ethics 35
1.3.2 ISACA IS Audit and Assurance Standards 35
General 36
Performance 36
Reporting 37
1.3.3 ISACA IS Audit and Assurance Guidelines 37
General 38
Performance 39
Reporting 40
1.3.4 ISACA IS Audit and Assurance Tools and Techniques 40
1.3.5 Relationship Among Standards, Guidelines, and Tools and Techniques 40
1.3.6 ITAF™ 40
1.4 IS Controls 41
1.4.1 Risk Analysis 41
1.4.2 Internal Controls 42
1.4.3 IS Control Objectives 43
1.4.4 COBIT 5 44
1.4.5 General Controls 45
1.4.6 IS Specific Controls 45
1.5 Performing An IS Audit 45
1.5.1 Audit Objectives 46
1.5.2 Types of Audits 46
1.5.3 Audit Methodology 47

1.5.4 Risk-based Auditing 48
1.5.5 Audit Risk and Materiality 48
1.5.6 Risk Assessment and Treatment 49
Assessing Risk 49
Treating Risk 49
1.5.7 IS Audit Risk Assessment Techniques 50
1.5.8 Audit Programs 50
1.5.9 Fraud Detection 50
1.5.10 Compliance Versus Substantive Testing 51
1.5.11 Evidence 51
1.5.12 Interviewing and Observing Personnel in Performance of Their Duties 53
1.5.13 Sampling 54
1.5.14 Using the Services of Other Auditors and Experts 55
1.5.15 Computer-assisted Audit Techniques 56
CAATS as a Continuous Online Audit Approach 57
1.5.16 Evaluation of the Control Enviornment 57
Judging the Materiality of Findings 57
1.6 Communicating Audit Results 57
1.6.1 Audit Report Structure and Contents 58
1.6.2 Audit Documentation 59
1.6.3 Closing Findings 59
1.7 Control Self-assessment 60
1.7.1 Objectives of CSA 61
1.7.2 Benefits of CSA 61
1.7.3 Disadvantages of CSA 61
1.7.4 Auditor Role in CSA 61
1.7.5 Technology Drivers for CSA 61
1.7.6 Traditional Versus CSA Approach 61
1.8 The Evolving IS Audit Process 62
1.8.1 Integrated Auditing 62
1.8.2 Continuous Auditing 62
1.9 Case Studies 64
1.9.1 Case Study A 64
1.9.2 Case Study B 65
1.9.3 Case Study C 65
1.10 Answers to Case Study Questions 65
Answers to Case Study A Questions 65
Answers to Case Study B Questions 66
Answers to Case Study C Questions 66

Chapter 2:
Governance and Management of IT 67

Section One: Overview 68
Definition 68
Objectives 68
Task and Knowledge Statements 68
Tasks 68
Knowledge Statements 68
Suggested Resources for Further Study 80
Self-assessment Questions 81
Answers to Self-assessment Questions 82

Section Two: Content ... 84
2.1 Quick Reference ... 84
2.2 Corporate Governance ... 85
2.3 Governance of Enterprise IT ... 85
2.3.1 Good Practices for Governance of Enterpise IT ... 86
Governance of Enterprise IT and Management Frameworks ... 86
Audit Role in Governance of Enterprise IT ... 87
2.3.2 IT Governing Committees ... 88
2.3.3 IT Balanced Scorecard ... 88
2.3.4 Information Security Governance ... 89
Effective Information Security Governance ... 90
Roles and Responsibilities of Senior Management and Boards of Directors ... 91
Matrix of Outcomes and Responsibilities ... 91
2.3.5 Enterprise Architecture ... 92
2.4 Information Systems Strategy ... 93
2.4.1 Strategic Planning ... 93
2.4.2 IT Steering Committee ... 94
2.5 Maturity and Process Improvement Models ... 94
2.6 IT Investment and Allocation Practices ... 95
2.6.1 Value of IT ... 95
2.6.2 Implementing IT Portfolio Management ... 95
2.6.3 IT Portfolio Management Versus Balanced Scorecard ... 95
2.7 Policies and Procedures ... 95
2.7.1 Policies ... 96
Information Security Policy ... 96
2.7.2 Procedures ... 98
2.8 Risk Management ... 98
2.8.1 Developing a Risk Management Program ... 98
2.8.2 Risk Management Process ... 98
Step 1: Asset Identification ... 98
Step 2: Evaluation of Threats and Vulnerabilities to Assets ... 99
Step 3: Evaluation of the Impact ... 99
Step 4: Calculation of Risk ... 99
Step 5: Evaluation of and Response to Risk ... 99
2.8.3 Risk Analysis Methods ... 100
Qualitative Analysis Methods ... 100
Semiquantitative Analysis Methods ... 100
Quantitative Analysis Methods ... 100
2.9 Information Technology Management Practices ... 100
2.9.1 Human Resource Management ... 100
Hiring ... 100
Employee Handbook ... 101
Promotion Policies ... 101
Training ... 101
Scheduling and Time Reporting ... 101
Employee Performance Evaluations ... 101
Required Vacations ... 101
Termination Policies ... 101
2.9.2 Sourcing Practices ... 102
Outsourcing Practices and Strategies ... 102
Industry Standards/Benchmarking ... 104
Globalization Practices and Strategies ... 104
Cloud Computing ... 104
Outsourcing and Third-party Audit Reports ... 104
Governance in Outsourcing ... 106

Capacity and Growth Planning 107
Third-party Service Delivery Management 107
Service Improvement and User Satisfaction 108
2.9.3 Organizational Change Management 108
2.9.4 Financial Management Practices 109
IS Budgets 109
Software Development 109
2.9.5 Quality Management 109
2.9.6 Information Security Management 110
2.9.7 Performance Optimization 110
Critical Success Factors 110
Methodologies and Tools 110
Tools and Techniques 111
2.10 IT Organizational Structure and Responsibilities 111
2.10.1 IT Roles and Responsibilities 111
Vendor and Outsourcer Management 112
Infrastructure Operations and Maintenance 113
Media Management 113
Data Entry 113
Supervisory Control and Data Acquisition 113
Systems Administration 113
Security Administration 113
Quality Assurance 114
Database Administration 114
Systems Analyst 114
Security Architect 114
System Security Engineer 114
Applications Development and Maintenance 115
Infrastructure Development and Maintenance 115
Network Management 115
2.10.2 Segregation of Duties Within IT 115
2.10.3 Segregation of Duties Controls 116
Transaction Authorization 116
Custody of Assets 116
Access to Data 116
Compensating Controls for Lack of Segregation of Duties 117
2.11 Auditing IT Governance Structure and Implementation 117
2.11.1 Reviewing Documentation 117
2.11.2 Reviewing Contractual Commitments 118
2.12 Business Continuity Planning 118
2.12.1 IT Business Continuity Planning 119
2.12.2 Disasters and Other Disruptive Events 120
Pandemic Planning 120
Dealing With Damage to Image, Reputation or Brand 120
Unanticipated/Unforeseeable Events 121
2.12.3 Business Continuity Planning Process 121
2.12.4 Business Continuity Policy 121
2.12.5 Business Continuity Planning Incident Management 122
2.12.6 Business Impact Analysis 123
Classification of Operations and Criticality Analysis 125
2.12.7 Development of Business Continuity Plans 125
2.12.8 Other Issues in Plan Development 126
2.12.9 Components of a Business Continuity Plan 126
Key Decision-making Personnel 127
Backup of Required Supplies 127
Insurance 127

2.12.10 Plan Testing 128
Specifications 128
Test Execution 128
Documentation of Results 129
Results Analysis 129
Plan Maintenance 129
Business Continuity Management Good Practices 129
2.12.11 Summary of Business Continuity 130
2.13 Auditing Business Continuity 130
2.13.1 Reviewing the Business Continuity Plan 130
Review the Document 130
Review the Applications Covered by the Plan 130
Review the Business Continuity Teams 130
Plan Testing 131
2.13.2 Evaluation of Prior Test Results 131
2.13.3 Evaluation of Offsite Storage 131
2.13.4 Interviewing Key Personnel 131
2.13.5 Evaluation of Security at Offsite Facility 131
2.13.6 Reviewing Alternative Processing Contract 132
2.13.7 Reviewing Insurance Coverage 132
2.14 Case Studies 132
2.14.1 Case Study A 132
2.14.2 Case Study B 132
2.14.3 Case Study C 133
2.14.4 Case Study D 133
2.14.5 Case Study E 134
2.15 Answers to Case Study Questions 134
Answers to Case Study A Questions 134
Answers to Case Study B Questions 134
Answers to Case Study C Questions 135
Answers to Case Study D Questions 135
Answers to Case Study E Questions 135

Chapter 3:
Information Systems Acquisition, Development and Implementation 137

Section One: Overview 138
Definition 138
Objectives 138
Task and Knowledge Statements 138
Tasks 138
Knowledge Statements 138
Suggested Resources for Further Study 147
Self-assessment Questions 148
Answers to Self-assessment Questions 149

Section Two: Content 151
3.1 Quick Reference 151
3.2 Benefits Realization 151
3.2.1 Portfolio/Program Management 152
3.2.2 Business Case Development and Approval 153
3.2.3 Benefits Realization Techniques 154

3.3 Project Management Structure 155
3.3.1 General Aspects 155
3.3.2 Project Context and Environment........ 155
3.3.3 Project Organizational Forms 155
3.3.4 Project Communication and Culture 156
3.3.5 Project Objectives 156
3.3.6 Roles and Responsibilities of Groups and Individuals........ 158
3.4 Project Management Practices 159
3.4.1 Initiation of a Project 160
3.4.2 Project Planning........ 160
System Development Project Cost Estimation 160
Software Size Estimation 161
Function Point Analysis........ 161
FPA Feature Points 161
Cost Budgets........ 161
Software Cost Estimation 162
Scheduling and Establishing the Time Frame 162
Critical Path Methodology 162
Gantt Charts........ 162
Program Evaluation Review Technique 163
Timebox Management 164
3.4.3 Project Execution........ 164
3.4.4 Project Controlling 164
Management of Scope Changes 164
Management of Resource Usage........ 164
Management of Risk 164
3.4.5 Closing a Project........ 165
3.5 Business Application Development........ 165
3.5.1 Traditional SDLC Approach........ 166
3.5.2 Description Of Traditional SDLC Phases........ 168
Phase 1—Feasibility Study........ 168
Phase 2—Requirements Definition........ 168
Phase 3A—Software Selection and Acquisition 169
Phase 3B—Design........ 171
Phase 4A—Configuration 173
Phase 4B—Development........ 173
Phase 5—Final Testing and Implementation........ 176
Phase 6—Postimplementation Review........ 182
3.5.3 Integrated Resource Management Systems........ 182
3.5.4 Risk Associated With Software Development........ 182
3.6 Virtualization and Cloud Computing Environments 183
3.6.1 Virtualization 183
Key Risk Areas........ 184
Typical Controls 184
3.7 Business Application Systems 185
3.7.1 E-Commerce 185
E-Commerce Models........ 185
3.7.2 Electronic Data Interchange 188
General Requirements 188
Traditional EDI........ 188
Web-Based EDI 189
3.7.3 EDI Risk and Controls 189

3.7.4 Controls in The EDI Environment 189
Receipt of Inbound Transactions 190
Outbound Transactions 190
Auditing EDI 191
3.7.5 Email 191
Security Issues of Email 192
Standards for Email Security 192
3.7.6 Point-of-sale Systems 193
3.7.7 Electronic Banking 193
Risk Management Challenges in E-banking 193
Risk Management Controls for E-banking 193
3.7.8 Electronic Finance 194
3.7.9 Payment Systems 194
Electronic Money Model 194
Electronic Checks Model 194
Electronic Transfer Model 194
3.7.10 Integrated Manufacturing Systems 194
3.7.11 Electronic Funds Transfer 195
Controls in an EFT Environment 195
3.7.12 Automated Teller Machine 195
Audit of ATMs 196
3.7.13 Interactive Voice Response 196
3.7.14 Purchase Accounting System 196
3.7.15 Image Processing 196
3.7.16 Industrial Control Systems 197
Risk Factors 197
Typical Controls 198
3.7.17 Artificial Intelligence and Expert Systems 198
3.7.18 Business Intelligence 199
Business Intelligence Governance 201
3.7.19 Decision Support System 202
Efficiency vs. Effectiveness 202
Decision Focus 202
DSS Frameworks 202
Design and Development 202
Implementation and Use 202
Risk Factors 203
Implementation Strategies 203
Assessment and Evaluation 203
DSS Common Characteristics 203
DSS Trends 203
3.7.20 Customer Relationship Management 203
3.7.21 Supply Chain Management 204
3.8 Development Methods 204
3.8.1 Use of Structured Analysis, Design and Development Techniques 204
3.8.2 Agile Development 204
3.8.3 Prototyping-evolutionary Development 205
3.8.4 Rapid Application Development 206
3.8.5 Object-oriented System Development 206
3.8.6 Component-based Development 207
3.8.7 Web-based Application Development 208
3.8.8 Software Reengineering 208
3.8.9 Reverse Engineering 209

3.9 Infrastructure Development/Acquisition Practices 209
3.9.1 Project Phases of Physical Architecture Analysis 209
Review of Existing Architecture 210
Analysis and Design 210
Draft Functional Requirements 210
Vendor and Product Selection 211
Writing Functional Requirements 211
Proof of Concept 211
3.9.2 Planning Implementation of Infrastructure 211
Procurement Phase 211
Delivery Time 211
Installation Plan 211
Installation Test Plan 213
3.9.3 Critical Success Factors 213
3.9.4 Hardware Acquisition 213
Acquisition Steps 214
3.9.5 System Software Acquisition 214
3.9.6 System Software Implementation 214
3.10 Information Systems Maintenance Practices 214
3.10.1 Change Management Process Overview 215
Deploying Changes 215
Documentation 215
Testing Changed Programs 218
Auditing Program Changes 218
Emergency Changes 218
Deploying Changes Back Into Production 218
Change Exposures (Unauthorized Changes) 218
3.10.2 Configuration Management 218
3.11 System Development Tools and Productivity Aids 219
3.11.1 Code Generators 219
3.11.2 Computer-aided Software Engineering 219
3.11.3 Fourth-generation Languages 220
3.12 Process Improvement Practices 221
3.12.1 Business Process Reengineering and Process Change Projects 221
BPR Methods and Techniques 222
BPR Audit and Evaluation 222
3.12.2 ISO/IEC 25010:2011 223
3.12.3 Capability Maturity Model Integration 223
3.12.4 ISO/IEC 330XX Series 223
3.13 Application Controls 224
3.13.1 Input/Origination Controls 224
Input Authorization 224
Batch Controls and Balancing 224
Error Reporting and Handling 225
3.13.2 Processing Procedures and Controls 225
Data Validation and Editing Procedures 225
Processing Controls 226
Data File Control Procedures 227
3.13.3 Output Controls 228
3.13.4 Business Process Control Assurance 229

3.14 Auditing Application Controls ... 229
3.14.1 Flow of Transactions Through the System ... 229
3.14.2 Risk Assessment Model to Analyze Application Controls ... 229
3.14.3 Observing and Testing User Performing Procedures ... 229
3.14.4 Data Integrity Testing ... 230
3.14.5 Data Integrity in Online Transaction Processing Systems ... 230
3.14.6 Test Application Systems ... 230
3.14.7 Continuous Online Auditing ... 232
3.14.8 Online Auditing Techniques ... 232
3.15 Auditing Systems Development, Acquisition and Maintenance ... 233
3.15.1 Project Management ... 233
3.15.2 Feasibility Study ... 234
3.15.3 Requirements Definition ... 234
3.15.4 Software Acquisition Process ... 234
3.15.5 Detailed Design and Development ... 234
3.15.6 Testing ... 234
3.15.7 Implementation Phase ... 234
3.15.8 Postimplementation Review ... 235
3.15.9 System Change Procedures and the Program Migration Process ... 235
3.16 Case Studies ... 235
3.16.1 Case Study A ... 235
3.16.2 Case Study B ... 236
3.17 Answers to Case Study Questions ... 237
Answers to Case Study A Questions ... 237
Answers to Case Study B Questions ... 237

Chapter 4:
Information Systems Operations, Maintenance and Service Management ... 239

Section One: Overview ... 240
Definition ... 240
Objectives ... 240
Task and Knowledge Statements ... 240
Tasks ... 240
Knowledge Statements ... 240
Suggested Resources for Further Study ... 249
Self-assessment Questions ... 250
Answers to Self-assessment Questions ... 251

Section Two: Content ... 254
4.1 Quick Reference ... 254
4.2 Information Systems Operations ... 255
4.2.1 Management of IS Operations ... 255
Control Functions ... 255
4.2.2 IT Service Management Frameworks ... 256
4.2.3 IT Service Management ... 256
Service Level ... 257
Monitoring of Service Levels ... 258
Service Levels and Enterprise Architecture ... 258
4.2.4 IS Operations ... 258
Job Scheduling ... 258
Job Scheduling Software ... 259

4.2.5 Incident and Problem Management ... 259
Process of Incident Handling ... 259
Problem Management ... 259
Detection, Documentation, Control, Resolution and Reporting of Abnormal Conditions ... 259
4.2.6 Support/Help Desk ... 260
4.2.7 Change Management Process ... 260
Patch Management ... 261
4.2.8 Release Management ... 261
4.2.9 Quality Assurance ... 262
4.3 IT Asset Management ... 262
4.4 Information Systems Hardware ... 262
4.4.1 Computer Hardware Components and Architectures ... 262
Processing Components ... 262
Input/Output Components ... 262
Types of Computers ... 263
Common Enterprise Back-end Devices ... 263
Universal Serial Bus ... 264
Memory Cards/Flash Drives ... 264
Radio Frequency Identification ... 265
4.4.2 Hardware Maintenance Program ... 266
4.4.3 Hardware Monitoring Procedures ... 266
4.4.4 Capacity Management ... 266
4.5 IS Architecture and Software ... 267
4.5.1 Operating Systems ... 268
Software Control Features or Parameters ... 268
Software Integrity Issues ... 268
Activity Logging and Reporting Options ... 269
4.5.2 Access Control Software ... 269
4.5.3 Data Communications Software ... 269
4.5.4 Data Management ... 270
Data Quality ... 270
Data Life Cycle ... 270
4.5.5 Database Management System ... 270
DBMS Architecture ... 272
Detailed DBMS Metadata Architecture ... 272
Data Dictionary/Directory System ... 272
Database Structure ... 272
Database Controls ... 274
4.5.6 Utility Programs ... 275
4.5.7 Software Licensing Issues ... 275
4.5.8 Source Code Management ... 276
4.5.9 End-user Computing ... 276
4.6 IS Network Infrastructure ... 276
4.6.1 Enterprise Network Architectures ... 277
4.6.2 Types of Networks ... 277
4.6.3 Network Services ... 278
4.6.4 Network Standards and Protocols ... 278
4.6.5 OSI Architecture ... 278
4.6.6 Application of the OSI Model In Network Architectures ... 280
Local Area Network ... 280
Wide Area Network ... 284
Wireless Networks ... 287
Public “Global” Internet Infrastructure ... 289

Network Administration and Control ... 292
Applications in a Networked Environment ... 293
On-demand Computing ... 295
4.7 Auditing Infrastructure and Operations ... 295
4.7.1 Enterprise Architecture and Auditing ... 295
4.7.2 Hardware Reviews ... 295
4.7.3 Operating System Reviews ... 295
4.7.4 Database Reviews ... 295
4.7.5 Network Infrastructure and Implementation Reviews ... 295
4.7.6 IS Operations Reviews ... 300
4.7.7 Scheduling Reviews ... 301
4.7.8 Problem Management Reporting Reviews ... 302
4.8 Disaster Recovery Planning ... 302
4.8.1 Recovery Point Objective and Recovery Time Objective ... 303
4.8.2 Recovery Strategies ... 304
4.8.3 Recovery Alternatives ... 304
Contractual Provisions ... 305
Procuring Alternative Hardware ... 305
Application Resiliency and Disaster Recovery Methods ... 306
Data Storage Resiliency and Disaster Recovery Methods ... 306
Telecommunication Networks Resiliency and Disaster Recovery Methods ... 306
4.8.4 Development of Disaster Recovery Plans ... 307
IT DRP Contents ... 307
IT DRP Scenarios ... 308
Recovery Procedures ... 308
4.8.5 Organization and Assignment of Responsibilities ... 308
4.8.6 Backup and Restoration ... 309
Offsite Library Controls ... 309
Security and Control of Offsite Facilities ... 310
Media and Documentation Backup ... 310
Types of Backup Devices and Media ... 310
Periodic Backup Procedures ... 311
Frequency of Rotation ... 311
Types of Media and Documentation Rotated ... 311
Backup Schemes ... 312
Method of Rotation ... 312
Record Keeping for Offsite Storage ... 313
4.8.7 Disaster Recovery Testing Methods ... 313
Types of Tests ... 313
Testing ... 314
Test Results ... 315
4.8.8 Invoking Disaster Recovery Plans ... 315
4.9 Case Studies ... 315
4.9.1 Case Study A ... 315
4.9.2 Case Study B ... 316
4.10 Answers to Case Study Questions ... 316
Answers to Case Study A Questions ... 316
Answers to Case Study B Questions ... 316

Chapter 5:
Protection of Information Assets ... 317

Section One: Overview ... 318
Definition ... 318
Objectives ... 318
Task and Knowledge Statements ... 318
Tasks ... 318
Knowledge Statements ... 318
Suggested Resources for Further Study ... 331
Self-assessment Questions ... 332
Answers to Self-assessment Questions ... 333

Section Two: Content ... 335
5.1 Quick Reference ... 335
5.2 Information Security Management ... 335
5.2.1 Key Elements of Information Security Management ... 336
Information Security Management System ... 336
5.2.2 Information Security Management Roles and Responsibilities ... 337
5.2.3 Classification of Information Assets ... 337
5.2.4 Fraud Risk Factors ... 338
5.2.5 Information Security Control Design ... 338
Managerial, Technical and Physical Controls ... 339
Control Standards and Frameworks ... 339
Control Monitoring and Effectiveness ... 339
5.2.6 System Access Permission ... 339
5.2.7 Mandatory and Discretionary Access Controls ... 340
5.2.8 Privacy Principles and the Role of IS Auditors ... 340
5.2.9 Critical Success Factors to Information Security Management ... 341
Security Awareness, Training and Education ... 341
5.2.10 Information Security and External Parties ... 342
Identification of Risk Related to External Parties ... 342
Addressing Security When Dealing With Customers ... 343
Addressing Security in Third-party Agreements ... 343
5.2.11 Human Resources Security and Third Parties ... 345
Screening ... 345
Terms and Conditions of Employment ... 345
During Employment ... 345
Termination or Change of Employment ... 345
Removal of Access Rights ... 346
5.2.12 Computer Crime Issues and Exposures ... 346
5.2.13 Security Incident Handling and Response ... 352
5.3 Logical Access ... 352
5.3.1 Logical Access Exposures ... 352
5.3.2 Familiarization With the Enterprise's IT Environment ... 353
5.3.3 Paths of Logical Access ... 353
General Points of Entry ... 353
5.3.4 Logical Access Control Software ... 353
5.3.5 Identification and Authentication ... 354
Logon IDS and Passwords ... 355
Token Devices, One-time Passwords ... 356
Biometrics ... 356
Single Sign-on ... 358

5.3.6 Authorization Issues 359
Access Control Lists........ 359
Logical Access Security Administration 359
Remote Access Security 359
Audit Logging in Monitoring System Access........ 360
Naming Conventions for Logical Access Controls 362
5.3.7 Storing, Retrieving, Transporting and Disposing of Confidential Information........ 362
Preserving Information During Shipment or Storage 363
Media-Specific Storage Precautions 363
5.4 Network Infrastructure Security........ 363
5.4.1 LAN Security........ 363
Virtualization 364
5.4.2 Client-server Security 365
5.4.3 Wireless Security Threats and Risk Mitigation 365
5.4.4 Internet Threats and Security........ 366
Network Security Threats........ 366
Passive Attacks 366
Active Attacks 366
Causal Factors for Internet Attacks 367
Internet Security Controls 367
Firewall Security Systems 367
Firewall General Features........ 368
Firewall Types........ 368
Examples of Firewall Implementations........ 369
Firewall Issues 370
Firewall Platforms 370
Intrusion Detection Systems 370
Intrusion Prevention Systems........ 371
Honeypots and Honeynets........ 371
5.4.5 Encryption 371
Key Elements of Encryption Systems........ 372
Symmetric Key Cryptographic Systems 372
Public (Asymmetric) Key Cryptographic Systems 374
Quantum Cryptography........ 374
Digital Signatures........ 374
Public Key Infrastructure 375
Applications of Cryptographic Systems 376
5.4.6 Malware 377
Virus and Worm Controls........ 377
Management Procedural Controls........ 377
Technical Controls........ 378
Anti-malware Software Implementation Strategies 378
5.4.7 Voice-over IP........ 379
VoIP Security Issues........ 379
5.4.8 Private Branch Exchange........ 380
PBX Risk........ 380
PBX Audit 381
PBX System Features........ 381
PBX System Attacks 381
Hardware Wiretapping........ 382
Hardware Conferencing........ 382
Remote Access 383
Maintenance 383
Special Manufacturer’s Features........ 383

Manufacturer's Development and Test Features ... 383
Software Loading and Update Tampering ... 384
Crash-restart Attacks ... 384
Passwords ... 384

5.5 Auditing Information Security Management Framework ... 384
5.5.1 Auditing Information Security Management Framework ... 384
Reviewing Written Policies, Procedures and Standards ... 384
Logical Access Security Policies ... 384
Formal Security Awareness and Training ... 384
Data Ownership ... 385
Data Owners ... 385
Data Custodians ... 385
Security Administrator ... 385
New IT Users ... 385
Data Users ... 385
Documented Authorizations ... 385
Terminated Employee Access ... 385
Security Baselines ... 386
Access Standards ... 386
5.5.2 Auditing Logical Access ... 386
Familiarization With the IT Environment ... 388
Assessing and Documenting the Access Paths ... 388
Interviewing Systems Personnel ... 389
Reviewing Reports From Access Control Software ... 389
Reviewing Application Systems Operations Manual ... 389
5.5.3 Techniques for Testing Security ... 389
Terminal Cards and Keys ... 389
Terminal Identification ... 389
Logon IDs and Passwords ... 389
Controls Over Production Resources ... 390
Logging and Reporting of Computer Access Violations ... 390
Follow-up Access Violations ... 390
Bypassing Security and Compensating Controls ... 390
Review Access Controls and Password Administration ... 390
5.5.4 Investigation Techniques ... 391
Investigation of Computer Crime ... 391
Computer Forensics ... 391
Protection of Evidence and Chain of Custody ... 392

5.6 Auditing Network Infrastructure Security ... 392
5.6.1 Auditing Remote Access ... 393
Auditing Internet Points of Presence ... 393
Network Penetration Tests ... 393
Full Network Assessment Reviews ... 396
Development and Authorization of Network Changes ... 396
Unauthorized Changes ... 396

5.7 Environmental Exposures and Controls ... 397
5.7.1 Environmental Issues and Exposures ... 397
5.7.2 Controls for Environmental Exposures ... 397
Alarm Control Panels ... 397
Water Detectors ... 397
Handheld Fire Extinguishers ... 397
Manual Fire Alarms ... 397
Smoke Detectors ... 397
Fire Suppression Systems ... 398
Strategically Locating the Computer Room ... 398

Regular Inspection by Fire Department 399
Fireproof Walls, Floors and Ceilings of the Computer Room 399
Electrical Surge Protectors 399
Uninterruptible Power Supply/Generator 399
Emergency Power-off Switch 399
Power Leads From Two Substations 399
Fully Documented and Tested Business Continuity Plan 399
Wiring Placed in Electrical Panels and Conduit 399
Inhibited Activities Within the Information Processing Facility 399
Fire-resistant Office Materials 399
Documented and Tested Emergency Evacuation Plans 399
5.7.3 Auditing Environmental Controls 399
Water and Smoke Detectors 399
Handheld Fire Extinguishers 399
Fire Suppression Systems 400
Regular Inspection by Fire Department 400
Fireproof Walls, Floors and Ceilings of the Computer Room 400
Electrical Surge Protectors 400
Power Leads From Two Substations 400
Fully Documented and Tested Business Continuity Plan 400
Wiring Placed in Electrical Panels and Conduit 400
UPS/Generator 400
Documented and Tested Emergency Evacuation Plans 400
Humidity/Temperature Control 400
5.8 Physical Access Exposures and Controls 400
5.8.1 Physical Access Issues and Exposures 400
Physical Access Exposures 400
Possible Perpetrators 400
5.8.2 Physical Access Controls 401
5.8.3 Auditing Physical Access 402
5.9 Mobile Computing 402
5.10 Peer-to-peer Computing 404
5.11 Instant Messaging 405
5.12 Social Media 405
5.13 Cloud Computing 407
5.14 Data Leakage 410
5.14.1 Data Leak Prevention 410
Data at Rest 410
Data in Motion (Network) 410
Data in Use (Endpoint) 410
Policy Creation and Management 410
Directory Services Integration 410
Workflow Management 410
Backup and Restore 410
Reporting 410
5.14.2 DLP Risk, Limitations and Considerations 411
5.15 End-user Computing Security Risk and Controls 411
5.16 Case Studies 412
5.16.1 Case Study A 412
5.16.2 Case Study B 412
5.16.3 Case Study C 413
5.16.4 Case Study D 413

5.17 Answers to Case Study Questions 414
Answers to Case Study A Questions 414
Answers to Case Study B Questions 414
Answers to Case Study C Questions 415
Answers to Case Study D Questions 415

APPENDIX A: IS AUDIT AND ASSURANCE STANDARDS, GUIDELINES AND TOOLS AND TECHNIQUES 417
Relationship of Standards to Guidelines and Tools and Techniques 417
Use 417

APPENDIX B: CISA EXAM GENERAL INFORMATION 419
Requirements for Certification 419
Successful Completion of the CISA Exam 419
Experience in IS Auditing, Control and Security 419
Description of the Exam 419
Registration for the CISA Exam 419
CISA Program Accreditation Renewed Under ISO/IEC 17024:2012 419
Preparing for the CISA Exam 420
Types of Exam Questions 420
Administration of the Exam 420
Sitting for the Exam 420
Budgeting Your Time 421
Rules and Procedures 421
Grading the Exam 421

Glossary 423

Acronyms 447

Index 453

About This Manual

OVERVIEW

The *CISA® Review Manual 26th Edition* is intended to assist candidates in preparing for the CISA exam. **The manual is one source of preparation for the exam and should not be thought of as the only source or be viewed as a comprehensive collection of all the information and experience that is required to pass the exam.** No single publication offers such coverage and detail.

As 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, additional references should be sought. The exam is a combination of questions testing **candidates'** technical and practical knowledge, and their ability to apply the knowledge (based on experience) in given situations.

The *CISA® Review Manual 26th Edition* provides coverage of the knowledge and activities related to the various functions associated with the content areas as detailed in the CISA job practice and described in the *ISACA Exam Candidate Information Guide (www.isaca.org/examguide)*:

Domain 1	The Process of Auditing Information Systems	21 percent
Domain 2	Governance and Management of IT	16 percent
Domain 3	Information Systems Acquisition, Development and Implementation	18 percent
Domain 4	Information Systems Operations, Maintenance and Service Management	20 percent
Domain 5	Protection of Information Assets	25 percent

Note: Each chapter defines the tasks that CISA candidates are expected to know how to do and includes a series of knowledge statements required to perform those tasks. These constitute the current practices for the IS auditor. The detailed CISA job practice can be viewed at *www.isaca.org/cisajobpractice.* This exam is based on these task and knowledge statements.

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.

FORMAT OF THIS MANUAL

Each of the five chapters of the *CISA® Review Manual 26th Edition* is divided into two sections for focused study.

Section one of each chapter includes:
- A definition of the domain
- Objectives for the domain as a practice area
- A listing of the task and knowledge statements for the domain
- A map of the relationship of each task to the knowledge statements for the domain
- A reference guide for the knowledge statements for the domain, including the relevant concepts and explanations
- References to specific content in section two for each knowledge statement
- Self-assessment questions and answers with explanations
- Suggested resources for further study

Section two of each chapter includes:
- Reference material and content that supports the knowledge statements
- Definitions of terms most commonly found on the exam

Material included is pertinent for CISA candidates' knowledge and/or understanding when preparing for the CISA certification exam.

The structure of the content includes numbering to identify the chapter where a topic is located and the headings of the subsequent levels of topics addressed in the chapter (i.e., 2.8.3 Risk Analysis Methods, is a subtopic of Risk Management in chapter 2). Relevant content in a subtopic is bolded for specific attention.

Understanding the material in this manual is one measurement of a candidate's knowledge, strengths and weaknesses, and an indication of areas where additional or focused study is needed. However, written material is not a substitute for experience. **CISA exam questions will test the candidate's practical application of this knowledge.** Case studies at the end of each chapter present situations within the profession and in specific areas of study. The scenarios involve topics addressed in the chapters and include practice questions which assist in understanding how a question could be presented on the CISA exam. The self-assessment questions in the first section of each chapter also serve this purpose and should not be used independently as a source of knowledge. Self-assessment questions should not be considered a measurement of one's ability to answer questions correctly on the CISA exam for that area. The questions are intended to familiarize candidates with question structure and general content, and may or may not be similar to questions that will appear on the actual exam. The reference material included in the first section of each chapter lists publications used in the creation of this manual.

At the end of the publication the candidate will find a glossary. The glossary includes both terms that are discussed in the text and terms that apply to the different areas but may not have been specifically discussed. The glossary can be another tool to identify areas in which candidates may need to seek additional references.

Although every effort is made to address the majority of information that candidates are expected to know, not all examination questions are necessarily covered in the manual, and candidates will need to rely on professional experience to provide the best answer.

Throughout the manual, the word "association" refers to ISACA. Also, please note that the manual has been written using standard American English.

Note: The *CISA® Review Manual 26th Edition* is a living document. As technology advances, the manual will be updated to reflect such advances. Further updates to this document before the date of the exam may be viewed at *www.isaca.org/studyaidupdates.*

EVALUATION OF THIS MANUAL

ISACA continuously monitors the swift and profound professional, technological and environmental advances affecting the IS audit, assurance, control and security professions. Recognizing these rapid advances, the *CISA® Review Manual* is updated periodically.

To assist ISACA in keeping abreast of these advances, please take a moment to evaluate the *CISA® Review Manual 26th Edition*. Such feedback is valuable to fully serve the profession and future CISA exam registrants.

To complete the evaluation on the web site, please go to *www.isaca.org/studyaidsevaluation.*

Thank you for your support and assistance.

ABOUT THE CISA REVIEW QUESTIONS, ANSWERS AND EXPLANATIONS MANUAL

Candidates may also wish to enhance their study and preparation for the exam by using the *CISA® Review Questions, Answers & Explanations Manual 11th Edition* or the CISA® Review Questions, Answers & Explanations Database – 12 month subscription.

The *CISA® Review Questions, Answers & Explanations Manual 11th Edition* consists of 1,000 multiple-choice study questions, answers and explanations arranged in the areas of the current CISA job practice. Many of these items appeared in previous editions of the *CISA® Review Questions, Answers & Explanations Manual*, but have been rewritten to correspond with current practice and/or be more representative of actual CISA exam items.

Another study aid that is available is the CISA® Review Questions, Answers & Explanations Database – 12 Month Subscription. It consists of the 1,000 questions, answers and explanations included in the *CISA® Review Questions, Answers & Explanations Manual 11th Edition*. With this product, CISA candidates can identify 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.

Questions in these products are representative of the types of questions that have appeared on the exam and include an explanation of the correct and incorrect answers. Questions are sorted by the CISA domains and as a sample test. These products are ideal for use in conjunction with the *CISA® Review Manual 26th Edition*. These manuals can be used as study sources throughout the study process or as part of a final review to determine where a candidate may need additional study. Again, it should be noted that these questions and suggested answers are provided as examples; they are not actual questions from the exam and may differ in content from those that actually appear on the exam.

Note: When using the CISA review materials to prepare for the exam, please note that they cover a broad spectrum of information systems audit, control and security issues. **Do not assume that reading these manuals and answering review questions will fully prepare you for the exam.** 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.

CISA ONLINE REVIEW COURSE

The CISA Online Review Course is a web-based, self-paced study tool. There are no hard copy materials (books, study manuals, etc.) provided with the course. While it is significantly different in terms of how the information is delivered, the course is based on content from the *CISA® Review Manual 26th Edition* and from additional content provided by subject matter experts. The course includes practice questions as well as interactive activities and exercises and an online glossary to reinforce content comprehension.

To better evaluate whether this is an appropriate study tool for you, please view the course demonstration at *http://demo.certification-partners.com/demo/v3/index.htm*. To register for the course, please go to *www.isaca.org/elearningcampus.*

Certified Information Systems Auditor®
An ISACA® Certification

Chapter 1:

The Process of Auditing Information Systems

Section One: Overview

Definition 20
Objectives 20
Task and Knowledge Statements 20
Suggested Resources for Further Study 28
Self-assessment Questions 29
Answers to Self-assessment Questions 30

Section Two: Content

1.1 Quick Reference 32
1.2 Management of the IS Audit Function 32
1.3 ISACA IS Audit and Assurance Standards and Guidelines 35
1.4 IS Controls 41
1.5 Performing an IS Audit 45
1.6 Communicating Audit Results 57
1.7 Control Self-assessment 60
1.8 The Evolving IS Audit Process 62
1.9 Case Studies 64
1.10 Answers to Case Study Questions 65

Section One: Overview

DEFINITION

This chapter is on the process of auditing information systems (IS) and encompasses the entire practice of IS auditing, including procedures and a thorough methodology that allows an IS auditor to perform an audit on any given IT area in a professional manner.

OBJECTIVES

The objective of this domain is to ensure that the CISA candidate has the knowledge necessary to provide audit services in accordance with IS audit standards to assist the organization with protecting and controlling information systems.

This area represents 21 percent of the CISA exam (approximately 32 questions).

TASK AND KNOWLEDGE STATEMENTS

TASKS

There are five tasks within the domain covering the process of auditing information systems:

T1.1 Execute a risk-based IS audit strategy in compliance with IS audit standards to ensure that key risk areas are audited.

T1.2 Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.

T1.3 Conduct audits in accordance with IS audit standards to achieve planned audit objectives.

T1.4 Communicate audit results and make recommendations to key stakeholders through meetings and audit reports to promote change when necessary.

T1.5 Conduct audit follow-ups to determine whether appropriate actions have been taken by management in a timely manner.

KNOWLEDGE STATEMENTS

The CISA candidate must have a good understanding of each of the topics or areas delineated by the knowledge statements. These statements are the basis for the exam.

There are 11 knowledge statements within the domain covering the process of auditing information systems:

K1.1 Knowledge of ISACA IS Audit and Assurance Standards, Guidelines, and Tools and Techniques, Code of Professional Ethics and other applicable standards

K1.2 Knowledge of risk assessment concepts and tools and techniques in planning, examination, reporting and follow-up

K1.3 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes

K1.4 Knowledge of control principles related to controls in information systems

K1.5 Knowledge of risk-based audit planning and audit project management techniques, including follow-up

K1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation and frequency of audits

K1.7 Knowledge of evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis, forensic investigation techniques, computer-assisted audit techniques [CAATs]) used to gather, protect and preserve audit evidence

K1.8 Knowledge of different sampling methodologies and other substantive/data analytical procedures

K1.9 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure, issue writing, management summary, result verification)

K1.10 Knowledge of audit quality assurance (QA) systems and frameworks

K1.11 Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities

Relationship of Task to Knowledge Statements

The task statements are what the CISA candidate is expected to know how to perform. The knowledge statements delineate each of the areas in which the CISA candidate must have a good understanding in order to perform the tasks. The task and knowledge statements are mapped in **figure 1.1** insofar as it is possible to do so. Note that although there is often overlap, each task statement will generally map to several knowledge statements.

Figure 1.1—Task and Knowledge Statements Mapping

T1.1 Execute a risk-based IS audit strategy in compliance with IS audit standards to ensure that key risk areas are audited.	K1.1 Knowledge of ISACA IS Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards K1.2 Knowledge of risk assessment concepts and tools and techniques in planning, examination, reporting and follow-up K1.3 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes K1.5 Knowledge of risk-based audit planning and audit project management techniques, including follow-up K1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation and frequency of audits K1.10 Knowledge of audit quality assurance systems and frameworks K1.11 Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities
T1.2 Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.	K1.1 Knowledge of ISACA IS Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards K1.2 Knowledge of risk assessment concepts and tools and techniques in planning, examination, reporting and follow-up K1.3 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes K1.4 Knowledge of control principles related to controls in information systems K1.5 Knowledge of risk-based audit planning and audit project management techniques, including follow-up K1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation and frequency of audits K1.10 Knowledge of audit quality assurance (QA) systems and frameworks K1.11 Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities
T1.3 Conduct audits in accordance with IS audit standards to achieve planned audit objectives.	K1.1 Knowledge of ISACA IS Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards K1.2 Knowledge of risk assessment concepts and tools and techniques in planning, examination, reporting and follow-up K1.3 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes K1.4 Knowledge of control principles related to controls in information systems K1.5 Knowledge of risk-based audit planning and audit project management techniques, including follow-up K1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation and frequency of audits K1.7 Knowledge of evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis, forensic investigation techniques, computer-assisted audit techniques [CAATs]) used to gather, protect and preserve audit evidence K1.8 Knowledge of different sampling methodologies and other substantive/data analytical procedures K1.9 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure, issue writing, management summary, result verification) K1.10 Knowledge of audit quality assurance (QA) systems and frameworks K1.11 Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities.
T1.4 Communicate audit results and make recommendations to key stakeholders through meetings and audit reports to promote change when necessary.	K1.1 Knowledge of ISACA IS Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards K1.2 Knowledge of risk assessment concepts and tools and techniques in planning, examination, reporting and follow-up K1.3 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes K1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation and frequency of audits K1.9 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure, issue writing, management summary, result verification) K1.10 Knowledge of audit quality assurance (QA) systems and frameworks K1.11 Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities

Figure 1.1—Task and Knowledge Statements Mapping *(cont.)*

T1.5 Conduct audit follow-ups to determine whether appropriate actions have been taken by management in a timely manner.	K1.1 Knowledge of ISACA IS Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards K1.2 Knowledge of risk assessment concepts and tools and techniques in planning, examination, reporting and follow-up K1.3 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes K1.4 Knowledge of control principles related to controls in information systems K1.5 Knowledge of risk-based audit planning and audit project management techniques, including follow-up K1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation and frequency of audits K1.7 Knowledge of evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis, forensic investigation techniques, computer-assisted audit techniques [CAATs]) used to gather, protect and preserve audit evidence K1.8 Knowledge of different sampling methodologies and other substantive/data analytical procedures K1.9 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure, issue writing, management summary, result verification) K1.10 Knowledge of audit quality assurance (QA) systems and frameworks K1.11 Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities

Knowledge Statement Reference Guide

Each knowledge statement is explained in terms of underlying concepts and relevance of the knowledge statement to the IS auditor. It is essential that the exam candidate understand the concepts. The knowledge statements are what the IS auditor must know in order to accomplish the tasks. Consequently, only the knowledge statements are detailed in this section.

The sections identified in K1.1 through K1.11 are described in greater detail in section two of this chapter.

K1.1 Knowledge of ISACA IS Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards

Explanation	Key Concepts	Reference in Manual
The credibility of any IS audit activity is largely determined by its adherence to commonly accepted standards. ISACA IS Audit and Assurance Standards, Guidelines and Tools and Techniques, and the Code of Professional Ethics, are developed, circulated for discussion among audit professionals and issued by ISACA in order to provide a framework of minimum and essential references regarding how an IS auditor should perform work and act in a professional manner. IS auditors should comply with ISACA IS Audit and Assurance Standards and follow guidelines, as relevant. Failure to follow standards or justify departure from guidelines may result in a violation of the Code of Professional Ethics. Although the CISA candidate is expected to have knowledge of these standards and guidelines, the exam will test the candidate's understanding of the application of the information rather than asking "definitional" questions that simply test information recall.	Code of Professional Ethics	1.3.1 ISACA Code of Professional Ethics
	IS Audit and Assurance Standards, Guidelines and Tools and Techniques	1.3.2 ISACA IS Audit and Assurance Standards 1.3.3 ISACA IS Audit and Assurance Guidelines 1.3.4 ISACA IS Audit and Assurance Tools and Techniques 1.3.5 Relationship Among Standards, Guidelines and Tools and Techniques
	Understanding ITAF™	1.3.6 ITAF™

K1.2 Knowledge of risk assessment concepts and tools and techniques in planning, examination, reporting and follow-up

Explanation	Key Concepts	Reference in Manual
The overall audit plan of the organization should be based on business risk related to the use of IT, and the IS auditor is expected to be aware of the need to focus on this risk. In addition, an audit must focus on the most critical elements of the function under review. For this reason, the IS auditor should be aware of, and be able to put into practice, the risk analysis techniques needed to identify and prioritize business risk within the audit scope. This approach allows the IS auditor to create an audit plan that applies finite audit resources to where they are most needed. Although business risk is the most important driver of the audit program, the IS auditor must also take steps to minimize associated elements such as sampling risk, detection risk, materiality of findings, etc., because these may impact the adequacy of the review.	Impact of risk assessment on IS auditing	1.4.1 Risk Analysis 1.5.3 Audit Methodology 1.5.4 Risk-based Auditing 1.5.5 Audit Risk and Materiality 1.5.7 IS Audit Risk Assessment Techniques
	Understanding risk analysis concepts within an auditing context	1.4.1 Risk Analysis
	Applying risk analysis techniques during audit planning	1.5.4 Risk-based Auditing 1.5.5 Audit Risk and Materiality 1.5.6 Risk Assessment and Treatment 1.5.7 IS Audit Risk Assessment Techniques
	Communicating results and following up on corrective actions and recommendations	1.6 Communicating Audit Results 1.6.1 Audit Report Structure and Contents 1.6.2 Audit Documentation

K1.3 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes

Explanation	Key Concepts	Reference in Manual
IS auditing involves the assessment of IS-related controls put in place to ensure the achievement of control objectives. Understanding control objectives and identifying the key controls that help achieve a properly controlled environment are essential for the effectiveness and efficiency of the IS audit process. Auditing is, therefore, a process of ensuring that control objectives are appropriately addressed by the associated controls. COBIT provides a comprehensive control framework that can help the IS auditor benchmark control objectives. The CISA candidate will find COBIT to be an excellent source of information when preparing for the CISA exam. The CISA candidate should remember that the CISA exam will not include questions that ask for COBIT definitions nor will the candidate be asked to quote any particular COBIT reference.	Proper audit planning techniques	1.2.3 Audit Planning
	Understanding control objectives	1.4.2 Internal Controls 1.4.3 IS Control Objectives 1.4.4 COBIT 5 1.4.5 General Controls 1.4.6 IS Specific Controls

K1.4 Knowledge of control principles related to controls in information systems

Explanation	Key Concepts	Reference in Manual
To achieve audit objectives within a precise scope and budget, the audit should be adequately planned. The performance of an IS audit does not differ substantially from a project. Accordingly, audit planning requires a similar level of preplanning to ensure an appropriate and efficient use of audit resources. Auditors need to understand project planning and management techniques to properly manage the audit and avoid an inefficient utilization of resources. The CISA exam will not include questions that are written for a project manager who is not an IS auditor.	Application of audit planning techniques	1.2.2 IS Audit Resource Management 1.2.3 Audit Planning 1.2.4 Effect of Laws and Regulations on IS Audit Planning
	Impact of IS environment on IS auditing practices and techniques	1.5.1 Audit Objectives 1.5.3 Audit Methodology 1.5.8 Audit Programs 2.11 Auditing IT Governance Structure and Implementation 2.13 Auditing Business Continuity 3.14 Auditing Application Controls 3.15 Auditing Systems Development, Acquisition and Maintenance 4.7 Auditing Infrastructure and Operations 5.5 Auditing Information Security Management Framework 5.6 Auditing Network Infrastructure Security

K1.5 Knowledge of risk-based audit planning and audit project management techniques, including follow-up

Explanation	Key Concepts	Reference in Manual
To effectively identify the enterprise's key risk, the IS auditor must obtain an understanding of the organization and its environment, specifically obtaining an understanding of the: • External and internal factors affecting the entity • Entity's selection and application of policies and procedures • Entity's objectives and strategies • Measurement and review of the entity's performance As part of obtaining this understanding, the IS auditor must also obtain an understanding of some key components, such as the entity's: • Strategic management • Business model • Corporate governance processes • Transaction types engaged in and with whom they are transacted One must understand how those transactions flow through and are captured into the information systems.	Understanding risk analysis concepts within an auditing context	1.4.1 Risk Analysis
	Understanding control objectives	1.4.2 Internal Controls 1.4.3 IS Control Objectives 1.4.4 COBIT 5 1.4.5 General Controls 1.4.6 IS Specific Controls

K1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation, and frequency of audits

Explanation	Key Concepts	Reference in Manual
Laws and regulations of any kind—including international treaties; central, federal or local government; or industry-related laws and regulations—affect the way that organizations conduct business, and very often determine scope, frequency and type of audits, and how reporting requirements are substantially affected. In fraud investigations or legal proceedings, maintaining the integrity of evidence throughout the evidence life cycle may be referred to as the chain of custody when the evidence is classified as forensic evidence. The CISA candidate is expected to be aware of, rather than a participant in, such specific evidence collection.	Factors to consider in collection, protection and chain of custody of audit evidence in an IS audit	1.5.11 Evidence 1.6.2 Audit Documentation
	Special considerations in audit documentation for evidence	1.8.2 Continuous Auditing

K1.7 Knowledge of evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis, forensic investigation techniques, computer-assisted audit techniques [CAATs]) used to gather, protect and preserve audit evidence

Explanation	Key Concepts	Reference in Manual
One essential audit concept is that audit findings must be supported by objective evidence. Therefore, it is essential to know the techniques used to gather and preserve evidence. Information is gathered from the auditees or from a variety of alternative sources, including reference manuals; accountants, banks, suppliers, vendors, etc.; and other related functional areas of the business. Information is gathered through inquiry, observation and interviews, and analysis of data using computer-assisted audit techniques (CAATs). Electronic media, including the use of automated audit software, may be used for preserving evidence that supports audit findings, but care should be taken to preserve any hard copy that may constitute part of the audit evidence. In all cases, it is important that retention policies for electronic evidence are sufficient to preserve evidence that supports audit findings. As an international organization, ISACA recognizes that the rules of evidence will differ according to local and national legislation, regulation and culture; however, concepts such as the importance of forensic evidence are universal. Audit conclusions should be supported by reliable and relevant evidence. Evidence collected during the course of an audit follows a life cycle. This life cycle includes collection, analysis, and preservation and destruction of evidence. The source of evidence should be reliable and qualified (i.e., from an appropriate, original source rather than obtained as a comment or hearsay) and originate directly from a trusted source to help ensure objectivity. As an example, system configuration settings copied by a system administrator to a spreadsheet and then presented to an auditor would not be considered as reliable because they would have been subject to alteration. Audit evidence should include information regarding date of creation and original source. Because electronic evidence is more dynamic than hard copy documents, security measures should be used to preserve the integrity of evidence collected and provide assurance that the evidence has not been altered in any way. Continuous auditing is a process by which the effectiveness and efficiency of controls is measured primarily by automated reporting processes that enable management to be aware of emerging risks or control weaknesses, without the need for a regular audit. The result is that information flow to management and implementation of corrective measures occur sooner. The IS auditor should be aware of the techniques involved in continuous auditing in order to facilitate the introduction of these techniques, as appropriate. The IS auditor must not rely solely on continuous auditing techniques when there is a high business risk and the continuous auditing technique deployed is not considered elaborate and exhaustive. This is the case when continuous auditing as a process has been put in place recently—for example, when the impact of control failure would be considerable. In such cases, regular formal audits must be scheduled to support and reinforce continuous auditing.	Application and relative value of computer-assisted audit techniques	1.5.15 Computer-assisted Audit Techniques
	Techniques for obtaining evidence	1.5.11 Evidence 1.5.12 Interviewing and Observing Personnel in Performance of Their Duties
	Computer-assisted audit techniques	1.5.15 Computer-assisted Audit Techniques
	Factors to consider in collection, protection and chain of custody of audit evidence in an IS audit	1.5.11 Evidence 1.6.2 Audit Documentation
	Special considerations in audit documentation for evidence	1.8.2 Continuous Auditing
	Continuous auditing techniques	1.8.2 Continuous Auditing

K1.8 Knowledge of different sampling methodologies and other substantive/data analytical procedures

Explanation	Key Concepts	Reference in Manual
Compliance testing is evidence gathering for the purpose of testing an enterprise'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. There is a direct correlation 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 the IS auditor is justified in minimizing the substantive procedures. 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. The efficiency and effectiveness of this testing can be enhanced through the use of 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 the sample. Sampling is used to infer characteristics about the entire population, based on the characteristics of the sample. For some time, there has been a focus on the IS auditor's ability to verify the adequacy of internal controls through the use of sampling techniques. This has become necessary because many controls are transactional in nature, which can make it difficult to test the entire population. However, sampling is not always warranted because software may allow the testing of certain attributes across the entire population. Although a CISA candidate is not expected to become a sampling expert, it is important for the candidate to have a foundational understanding of the general principles of sampling and how to design a relevant and reliable sample.	Relative use of compliance and substantive testing	1.5.10 Compliance Versus Substantive Testing
	Basic approaches to sampling and their relation to testing approaches	1.5.13 Sampling

K1.9 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure, issue writing, management summary, result verification)

Explanation	Key Concepts	Reference in Manual
Effective and clear communication can significantly improve the quality of audits and maximize 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. Auditors should also take into account the motivations and perspectives of recipients of the audit report so that 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 activity. Successful resolution of audit findings with auditees is essential so that auditees will adopt the recommendations in the report and initiate prompt corrective action. This goal may require the use of techniques such as facilitation, negotiation and conflict resolution. IS auditors should also understand the concept of materiality (i.e., the relative importance of findings based on business impact).	Understanding reporting standards	1.3.2 ISACA IS Audit and Assurance Standards (1400 Reporting)
	Applying various communications techniques to the reporting of audit results	1.6 Communicating Audit Results 1.6.1 Audit Report Structure and Contents 1.6.2 Audit Documentation
	Applying communication techniques to facilitation roles in control self-assessments	1.7 Control Self-assessment 1.7.4 Auditor Role in CSA

K1.10 Knowledge of audit quality assurance (QA) systems and frameworks

Explanation	Key Concepts	Reference in Manual
IS auditing is a branch of the broader field of auditing. Auditing standards refer to minimum parameters that should be taken into account when performing an audit. However, there may be guidelines and additional audit procedures that an auditor may wish to add in order to develop an opinion on the proper functioning of controls. Most of the basic auditing practices and techniques are equally relevant in an IS audit. The IS auditor should understand the impact of the IS environment on traditional auditing practices and techniques to ensure that the basic objective of the audit exercise is achieved. The practices and techniques to be used in a specific IS audit should be determined during the audit planning stage and incorporated into an audit program. ISACA does not define, or require knowledge of, any specific audit methodology, but expects the IS auditor to be aware of the general principles involved in planning and conducting an effective audit program. Control self-assessment (CSA) is a process in which an IS auditor can act in the role of facilitator to the business process owners to help them define and assess appropriate controls. 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 taking into account the risk appetite of the enterprise. Process owners are in an ideal position to define the appropriate controls because they have a greater knowledge of the process objectives. The IS auditor helps the process owners understand the need for controls, based on risk to the business processes. Results must be interpreted with a certain level of skepticism because process owners are not always objective when assessing their own activities.	Impact of IS environment on IS auditing practices and techniques	1.5.1 Audit Objectives 1.5.3 Audit Methodology 1.5.8 Audit Programs 2.11 Auditing IT Governance Structure and Implementation 2.13 Auditing Business Continuity 3.14 Auditing Application Controls 3.15 Auditing Systems Development, Acquisition and Maintenance 4.7 Auditing Infrastructure and Operations 5.5 Auditing Information Security Management Framework 5.6 Auditing Network Infrastructure Security
	Points of relevance while using services of other auditors and experts	1.5.14 Using the Services of Other Auditors and Experts
	Advantages and disadvantages of CSA	1.7 Control Self-assessment 1.7.1 Objectives of CSA 1.7.2 Benefits of CSA 1.7.3 Disadvantages of CSA
	The role of the auditor in CSA	1.7.4 Auditor Role in CSA
	Relevance of different technology drivers for CSA in the current business environment	1.7.5 Technology Drivers for CSA 1.7.6 Traditional Versus CSA Approach
	Relevance of different approaches of CSA in a given context	
	Applying communication techniques to facilitation roles in control self-assessments	1.7 Control Self-assessment 1.7.4 Auditor Role in CSA
	Audit quality evaluation	1.5.16 Evaluation of the Control Environment

K1.11 Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities

Explanation	Key Concepts	Reference in Manual
The IS auditor must be aware of the variety of audits that can be performed along with the goals and objectives of each of these engagements. Furthermore, there are a wide variety of entities (Payment Card Industry Data Security Standard [PCI DSS] third-party providers, government regulators, third-party assessing organizations/independent validation and verification, etc.) auditing the same organization, often concurrently. IS auditors must understand the purpose, scope and timing of these audits, so they can take these audits into consideration during their audit planning, testing and reporting processes. Recognizing that many recent, current and upcoming audits may provide adequate depth and coverage of area within the IS auditor's audit scope could enable the IS auditor to place reliance on other auditors' or control entities' work, if the work of others meets the standards of professional practice and testing needed to provide reasonable assurance that the IS controls are operating effectively, efficiently and are aligned with both current and planned organizational goals and objectives.	Understanding the proper techniques to plan assigned audits while maximizing IS Audit resource utilization and preventing duplication of audit activities	1.3.2 ISACA IS Audit and Assurance Standards (1201 Engagement Planning)
	Understanding the other type of audits that may be performed by other auditors and experts	1.5.2 Types of Audits
	Application of audit planning techniques	1.2.2 IS Audit Resource Management 1.2.3 Audit Planning 1.2.4 Effect of Laws and Regulations on IS Audit Planning
	Understanding risk analysis concepts within an auditing context	1.4.1 Risk Analysis
	Points of relevance while using services of other auditors and experts	1.3.2 ISACA IS Audit and Assurance Standards (1206 Using the Work of Other Experts) 1.5.14 Using the Services of Other Auditors and Experts

SUGGESTED RESOURCES FOR FURTHER STUDY

Cascarino, Richard E.; *Auditor's Guide to IT Auditing and Software Demo, 2nd Edition*, Wiley, USA, 2012

Davis, Chris; Mike Schiller; Kevin Wheeler; *IT Auditing: Using Controls to Protect Information Assets, 2nd Edition*, McGraw Hill, USA, 2011

ISACA, COBIT 5, USA, 2012, *www.isaca.org/cobit*

ISACA, *COBIT 5 for Assurance*, USA, 2013, *www.isaca.org/cobit*

ISACA, *IT Control Objectives for Sarbanes-Oxley: Using COBIT® 5 in the Design and Implementation of Internal Controls Over Financial Reporting*, USA, 2014, *www.isaca.org/sox*

ISACA, *ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition*, USA, 2014, *www.isaca.org/ITAF*

IT Governance Institute, *Control Objectives for BASEL II: The Importance of Governance and Risk Management for Compliance*, USA, 2007

Senft, Sandra; Frederick Gallegos; Aleksandra Davis; *Information Technology Control and Audit, 4th Edition*, CRC Press, USA, 2012

Note: Publications in bold are stocked in the ISACA Bookstore.

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 have typically appeared on the exam. Questions are written in a multiple-choice format and designed for one best answer. Each question has a stem (question) and four options (answer choices). The stem may be written in the form of a question or an incomplete statement. In some instances, a scenario or a description problem may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. Many times a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided.

In each case, the candidate must read the question carefully, eliminate known incorrect answers and then make the best choice possible. Knowing the format in which questions are asked, and how to study and gain knowledge of what will be tested, will help the candidate correctly answer the questions.

1-1 Which of the following outlines the overall authority to perform an 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

1-2 In performing a risk-based audit, which risk assessment is completed **INITIALLY** by the IS auditor?

A. Detection risk assessment
B. Control risk assessment
C. Inherent risk assessment
D. Fraud risk assessment

1-3 While developing a risk-based audit program, on which of the following would the IS auditor **MOST** likely focus?

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

1-4 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

1-5 An IS auditor performing a review of an application's controls finds a weakness in system software that could materially impact the application. The 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 in the report a statement that the audit was limited to a review of the application's controls.
D. review the system software controls as relevant and recommend a detailed system software review.

1-6 Which of the following is the **MOST** important reason why an audit planning process should be reviewed 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

1-7 Which of the following is **MOST** effective for implementing a control self-assessment (CSA) within business units?

A. Informal peer reviews
B. Facilitated workshops
C. Process flow narratives
D. Data flow diagrams

1-8 The **FIRST** step in planning an audit is to:

A. define audit deliverables.
B. finalize the audit scope and audit objectives.
C. gain an understanding of the business' objectives.
D. develop the audit approach or audit strategy.

1-9 The approach an IS auditor should use to plan IS audit coverage should be based on:

A. risk.
B. materiality.
C. professional skepticism.
D. sufficiency of audit evidence.

1-10 A company performs a daily backup of critical data and software files, and stores the backup tapes at an offsite location. The backup tapes are used to restore the files in case of a disruption. This is a:

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

ANSWERS TO SELF-ASSESSMENT QUESTIONS

1-1 A. The audit scope is specific to one 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.

1-2 A. Detection risk assessment is performed only after the inherent and control risk assessment have been performed to determine ability to detect either errors within a targeted processes.

B. Control risk assessment is performed after the inherent risk assessment has been completed and is to determine the level of risk that remains after controls for the targeted process are in place.

C. Inherent risk exists independently of an audit and can occur because of the nature of the business. To successfully conduct an audit, it is important to be aware of the related business processes. To perform the audit, the IS auditor needs to understand the business process, and by understanding the business process, the IS auditor better understands the inherent risk.

D. Fraud risk assessments are a subset of a control risk assessment in which the auditor determines if the control risk addresses the ability of internal and/or external parties to commit fraudulent transactions within the system.

1-3 **A. A risk-based audit approach focuses on the understanding of 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 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 scope of the audit.

C. Like administrative controls, operational controls are an important subset of controls; 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, the IS auditor is focusing on the business processes that were put in place to enable the organization to meet the strategy.

1-4 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 the auditor's substantive tests. It consists of two components, sampling risk and nonsampling risk.

C. The risk level or exposure without taking into account the actions that management has taken or might take is inherent risk.

D. Sampling risk is the risk that incorrect assumptions are made about the characteristics of a population from which a sample is taken. Nonsampling risk is the detection risk not related to sampling; it can be due to a variety of reasons, including, but not limited to, human error.

1-5 A. The 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 the IS auditor may not be technically competent to do such a review at this time.

C. If there are control weaknesses that have been discovered by the IS auditor, they should be disclosed. By issuing a disclaimer, this responsibility would be waived.

D. The appropriate option would be to review the systems software as relevant to the review and recommend a detailed systems software review for which additional resources may be recommended.

1-6 A. Planning for deployment of available audit resources is determined by the audit assignments planned, which is 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 IS audit standards, guidelines and procedures is universal to any audit engagement and is not influenced by short- and long-term issues.

1-7 A. Informal peer reviews would not be as effective because they would not necessarily identify and assess all control issues.

B. Facilitated workshops work well within business units.

C. Process flow narratives would not be as effective because they would not necessarily identify and assess all control issues.

D. Data flow diagrams would not be as effective because they would not necessarily identify and assess all control issues.

1-8 A. Defining audit deliverables is dependent upon having a thorough understanding of the business' objectives and purpose.

B. Finalizing the audit scope and objectives is dependent upon having a thorough understanding of the business' objectives and purpose.

C. The first step in audit planning is to gain an understanding of the business's mission, objectives and purpose, which in turn identifies the relevant policies, standards, guidelines, procedures and organization structure.

D. Developing the audit approach or strategy is dependent upon having a thorough understanding of the business' objectives and purpose.

1-9 **A. ISACA IS Audit and Assurance Standard 1202, Planning, establishes standards and provides guidance on planning an audit. It requires a risk-based approach.**

B. Materiality is addressed within ISACA IS Audit and Assurance Standard 1204: "IS audit and assurance professionals shall consider potential weaknesses or absences of controls while planning an engagement, and whether such weaknesses or absences of controls could result in a significant deficiency or a material weakness."

C. Professional skepticism is addressed within ISACA IS Audit and Assurance Standard 1207.2: "IS audit and assurance professionals shall maintain an attitude of professional skepticism during the engagement."

D. Sufficiency of audit evidence is addressed within ISACA IS Audit and Assurance Standard 1205.2: "IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives."

1-10 A. Preventive controls are those that avert problems before they arise. Backup tapes cannot be used to prevent damage to files and, therefore, cannot be classified as a preventive control.

B. Management controls modify processing systems to minimize a repeat occurrence of the problem. Backup tapes do not modify processing systems and, therefore, do not fit the definition of a management control.

C. A corrective control helps to correct or minimize the impact of a problem. Backup tapes can be used for restoring the files in case of damage of files, thereby reducing the impact of a disruption.

D. Detective controls help to detect and report problems as they occur. Backup tapes do not aid in detecting errors.

Section Two: Content

1.1 QUICK REFERENCE

Quick Reference Review

Chapter 1 outlines the framework for performing IS auditing, specifically including those mandatory requirements regarding the IS auditor's mission and activity as well as good practices to achieve an appropriate IS auditing outcome. CISA candidates should have a sound understanding of the following items, not only within the context of the present chapter, but also to correctly address questions in related subject areas. It is important to keep in mind that it is not enough to know these concepts from a definitional perspective. The CISA candidate must also be able to identify which elements may represent the greatest risk and which controls are most effective at mitigating this risk. Key topics in this chapter include:

- IS auditor roles and associated responsibilities, including expected audit outcomes and differences between IS auditing tasks within an assurance assignment and those within a consulting assignment
- The need for audit independence and level of authority within the internal audit environment as opposed to an external context
- Minimum audit planning requirements for an IS audit assignment, regardless of the specific or particular audit objective and scope
- Understanding the required level of compliance with ISACA IS Audit and Assurance Standards, as well as for ISACA IS Audit and Assurance Guidelines
- When planning audit work, the importance of clear identification of the audit approach related to controls defined as general versus auditing controls that are defined as application controls
- Scope, field work, application and execution of the concepts included in audit risk versus business risk
- The key role of requirements-compliant audit evidence when supporting the credibility of audit results and reporting
- The reliance on electronic audit work papers and evidence
- Purpose and planning opportunities of compliance testing versus substantive testing
- Audit responsibility and level of knowledge when considering legal requirements affecting IT within an audit scope
- The IS risk-oriented audit approach versus the complementary need for IS auditors to be acquainted with diverse IS standards and frameworks
- Understanding the difference between the objectives of implemented controls and control procedures
- Understanding evidence collection, sampling and evidence analysis techniques and its importance while conducting an IS audit
- Understanding reporting and communication methods

1.2 MANAGEMENT OF THE IS AUDIT FUNCTION

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

Note: Information systems (IS) are defined as the combination of strategic, managerial and operational activities 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 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. Therefore, the terms "IS" and "IT" will be used according to these definitions throughout the manual.

1.2.1 ORGANIZATION OF THE IS AUDIT FUNCTION

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

- Information systems are in compliance with applicable laws, regulations, contracts and/or industry guidelines
- IS data and information have appropriate levels of confidentiality, integrity and availability
- IS operations are being accomplished efficiently and effectiveness targets are being met

An organization can use both externally or internally provided IS audit services. The fundamental elements of IS audit are listed in section 1.3, ISACA IS Audit and Assurance Standards and Guidelines.

The role of the IS internal audit function should be established by an audit charter approved by board of directors and the audit committee (senior management if these entities do not exist). IS audit can be a part of internal audit, function as an independent group, or 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. The charter should clearly state management's responsibility and objectives for, and delegation of authority to, the IS audit function. This document should outline the overall authority, scope and responsibilities of the audit function. The highest level of management and the audit committee, if one exists, should approve this charter. Once established, this charter should be changed only if the change can be and is thoroughly justified. ISACA IS Audit and Assurance Standards require that the responsibility, authority and accountability of the IS audit function are appropriately documented in an audit charter or engagement letter (1001 Audit Charter). 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 that is sought 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 these 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.

1.2.2 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. ISACA IS Audit and Assurance Standards require that the IS auditor be technically competent (1006 Proficiency), having the skills and knowledge necessary to perform the auditor's work. Further, the IS auditor is to 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 for the year based on the organization's direction in terms of technology and related risk that needs to be addressed. This should be reviewed periodically to ensure that the training efforts and results are aligned to the direction that the audit organization is taking. Additionally, IS audit management should also provide the necessary IT resources to properly perform IS audits of a highly specialized nature (e.g., tools, methodology, work programs).

1.2.3 AUDIT PLANNING

Annual Planning

Audit planning includes both short- and long-term planning. Short-term planning takes into account audit issues that will be covered during the year, whereas long-term planning relates to audit plans that will take into account 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 entity's business should be included in the audit universe. The audit universe ideally lists all of the processes that may be considered for audit. Each of these processes may be subjected to a qualitative or quantitative risk assessment by evaluating the risk in respect to defined, relevant risk factors. The risk factors are those factors that influence the frequency and/or business impact of risk scenarios. For example, for an entity engaged in 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, in respect to 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 damage to the reputation of the entity that will take more than six months to recover
- **Medium**—A process issue may result in damage to the reputation of the entity that will take less than six months but more than three months to recover
- **Low**—A process issue may result in damage to the reputation of the entity that will take 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, an overall criterion may be defined to determine the overall risk of 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, when the resources required to execute the ideal plan are agreed on, often the available resources are not sufficient to execute the entire ideal plan. This analysis will help the audit function to demonstrate to top management the gap in resourcing and give top management a good idea of the amount of risk that management 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 is necessary to take into account new control issues; changes in the risk environment, technologies and business processes; and enhanced evaluation techniques. The results of this analysis for planning future audit activities 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).

Individual Audit Assignments

In addition to overall annual planning, each individual audit assignment must be adequately planned. The 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. The IS auditor should also take into consideration system implementation/upgrade deadlines, current and future technologies, requirements from business process owners, and IS resource limitations.

When planning an audit, the IS auditor must have an understanding of the overall environment under review. This should include 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, the IS auditor should be familiar with the regulatory environment in which the business operates.

To perform audit planning, the IS auditor should perform the steps indicated in **figure 1.2**.

Figure 1.2—Steps to Perform Audit Planning

- Gain an understanding of the business's mission, objectives, purpose and processes, which include information and processing requirements such as availability, integrity, security and business technology and information confidentiality.
- Understand changes in 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.

ISACA IS Audit and Assurance Standards require the IS auditor to plan the IS audit work to address the audit objectives and comply with applicable professional auditing standards (1201 Engagement Planning). The IS auditor should develop an audit plan that takes into consideration the objectives of the auditee relevant to the audit area and its technology infrastructure. Where appropriate, the IS auditor should also consider the area under review and its relationship to the organization (strategically, financially and/or operationally) and obtain information on the strategic plan, including the IS strategic plan. The IS auditor should have an understanding of the auditee's information technology architecture and technological direction to design a plan appropriate for the present and, where appropriate, future technology of the auditee.

Steps an IS auditor could take to gain an understanding of the business include:
- Reading background material including industry publications, annual reports and independent financial analysis reports
- Reviewing prior audit reports or IT-related reports (from external or internal audits, or specific reviews such as regulatory reviews)
- Reviewing business and IT long-term strategic plans
- Interviewing key managers to understand business issues
- Identifying specific regulations applicable to IT
- Identifying IT functions or related activities that have been outsourced
- Touring key organization facilities

Another basic component of planning is the matching of available audit resources to the tasks as defined in the audit plan. The IS auditor who prepares the plan should consider the requirements of the audit project, staffing resources and other constraints. This matching exercise should consider the needs of individual audit projects as well as the overall needs of the audit department.

1.2.4 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 computer system practices and controls and to the manner in which computers, programs and data are stored and used. Additionally, business regulations can impact the way data are processed, transmitted and stored (stock exchange, central banks, etc.). Special attention should be given to these issues in industries that are closely regulated. The banking industry worldwide has severe penalties for banks and their officers should a bank be unable to provide an adequate level of service due to security breaches. Inadequate security in a bank's online portal can result in loss of customer funds. In several countries, Internet service providers (ISPs) are subject to laws regarding confidentiality and service availability.

Because of a growing dependency on information systems and related technology, several countries are making efforts to add legal regulations concerning IS audit. The content of these legal regulations pertains to:
- Establishment of regulatory requirements
- Responsibilities assigned to corresponding entities
- Financial, operational and IT audit functions

Management personnel as well as audit 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: legal requirements (laws, regulatory and contractual agreements) placed on audit or IS audit, and legal requirements placed on the auditee and its systems, data management, reporting, etc. These areas impact the audit scope and audit objectives. The latter is important to internal and external auditors. Legal issues also impact the organizations' business operations in terms of compliance with ergonomic regulations, the US Health Insurance Portability and Accountability Act (HIPAA), Protection of Personal Data Directives and Electronic Commerce within the European Community, fraud prevention within banking organizations, etc.

An example of strong control practices is the US Sarbanes-Oxley Act of 2002, which requires evaluating an organization's internal controls. Sarbanes-Oxley provides for new corporate governance rules, regulations and standards for specified public companies including US Securities and Exchange Commission (SEC) registrants. The SEC has mandated the use of a recognized internal control framework. Sarbanes-Oxley requires organizations to select and implement a suitable internal control framework. Similarly, Japan enacted the Tokyo Stock Exchange Principles. In March 2004, the Listed Company Corporate Governance Committee, established by the Tokyo Stock Exchange in December 2002, published *Principles of Corporate Governance for Listed Companies*. The *Internal Control—Integrated Framework* from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has become the most commonly adopted framework by public companies seeking to comply. Because the US Sarbanes-Oxley Act has as its objective increasing the level of control of business processes and the information systems supporting them, IS auditors must consider the impact of Sarbanes-Oxley as part of audit planning.

A similar example of regulatory impact is the Basel Accords (Basel I, Basel II and Basel III). The Basel Accords regulate the minimum amount of capital for financial organizations based on the level of risk they face. The Basel Committee on Banking Supervision recommends conditions and capital requirements that

should be fulfilled to manage risk exposure. These conditions will ideally result in an improvement in:
- Credit risk
- Operational risk
- Market risk

The following are steps an IS auditor would perform to determine an organization's level of compliance with external requirements:
- Identify those government or other relevant external requirements dealing with:
  - Electronic data, personal data, copyrights, e-commerce, e-signatures, etc.
  - Computer system 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, as well as 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 these requirements.
- Determine if there are procedures in place to ensure contracts or agreements with external IT services providers reflect any legal requirements related to responsibilities.

It is expected that the organization would have a legal compliance function on which the IS control practitioner could rely.

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. The examination will only test knowledge of accepted global practices.

1.3 ISACA IS AUDIT AND ASSURANCE STANDARDS AND GUIDELINES

1.3.1 ISACA CODE OF PROFESSIONAL ETHICS

ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:
1. Support the implementation of, and encourage compliance with, appropriate standards, 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.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures.

Note: A CISA candidate is not expected to have memorized the ISACA IS Audit and Assurance Standards, Guidelines, and Tools and Techniques and the ISACA Code of Professional Ethics (*www.isaca.org/certification/code-of-professional-ethics*), word for word. Rather, the candidates will be tested on their understanding of the standard, guideline or code, its objectives and how it applies in a given situation.

1.3.2 ISACA IS AUDIT AND ASSURANCE STANDARDS

The specialized nature of IS auditing and the skills and knowledge necessary to perform such audits require globally applicable standards that pertain specifically to IS auditing. One of the most important functions of ISACA is providing information (common body of knowledge) to support knowledge requirements. (See standard 1006 Proficiency.)

One of ISACA's goals is to advance standards to meet this need. The development and dissemination of the ISACA IS Audit and Assurance Standards is a cornerstone of the association's professional contribution to the audit community. The IS auditor needs to be aware that there may be additional standards, or even legal requirements, placed on the auditor.

Standards contain statements of mandatory requirements for IS audit and assurance. They inform:
- IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession's expectations concerning the work of practitioners
- Holders of the Certified Information Systems Auditor (CISA) designation of their requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA group and, ultimately, in disciplinary action.

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.
- Guidelines provide guidance in applying IS Audit and Assurance Standards. The IS auditor should consider them in determining how to achieve implementation of the above standards, use

professional judgment in their application and be prepared to justify any departure from the standards.

- 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 the standards when completing IS auditing work, but do not set requirements.

Note: The complete text of the ISACA IS Audit and Assurance Standards, Guidelines, and Tools and Techniques is available at *www.isaca.org/standards.*

There are three categories of standards and guidelines—general, performance and reporting:

- **General**—The guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as 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

General

- **1001 Audit Charter**
  - 1001.1 The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability.
  - 1001.2 The IS audit and assurance function shall have the audit charter agreed upon and approved at an appropriate level within the enterprise.
- **1002 Organisational Independence**
  - 1002.1 The IS audit and assurance function shall be independent of the area or activity being reviewed to permit objective completion of the audit and assurance engagement.
- **1003 Professional Independence**
  - 1003.1 IS audit and assurance professionals shall be independent and objective in both attitude and appearance in all matters related to audit and assurance engagements.
- **1004 Reasonable Expectation**
  - 1004.1 IS audit and assurance professionals shall have reasonable expectation that the engagement can be completed in accordance with the IS audit and assurance standards and, where required, other appropriate professional or industry standards or applicable regulations and result in a professional opinion or conclusion.
  - 1004.2 IS audit and assurance professionals shall have reasonable expectation that the scope of the engagement enables conclusion on the subject matter and addresses any restrictions.
  - 1004.3 IS audit and assurance professionals shall have reasonable expectation that management understands its obligations and responsibilities with respect to the provision of appropriate, relevant and timely information required to perform the engagement.
- **1005 Due Professional Care**
  - 1005.1 IS audit and assurance professionals shall exercise due professional care, including observance of applicable professional audit standards, in planning, performing and reporting on the results of engagements.
- **1006 Proficiency**
  - 1006.1 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate skills and proficiency in conducting IS audit and assurance engagements and be professionally competent to perform the work required.
  - 1006.2 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate knowledge of the subject matter.
  - 1006.3 IS audit and assurance professionals shall maintain professional competence through appropriate continuing professional education and training.
- **1007 Assertions**
  - 1007.1 IS audit and assurance professionals shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.
- **1008 Criteria**
  - 1008.1 IS audit and assurance professionals shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, measureable, understandable, widely recognised, authoritative and understood by, or available to, all readers and users of the report.
  - 1008.2 IS audit and assurance professionals shall consider the source of the criteria and focus on those issued by relevant authoritative bodies before accepting lesser-known criteria.

Performance

- **1201 Engagement Planning**
  - 1201.1 IS audit and assurance professionals shall plan each IS audit and assurance engagement to address:
    - · Objective(s), scope, timeline and deliverables
    - · Compliance with applicable laws and professional auditing standards
    - · Use of a risk-based approach, where appropriate
    - · Engagement-specific issues
    - · Documentation and reporting requirements
  - 1201.2 IS audit and assurance professionals shall develop and document an IS audit or assurance engagement project plan, describing the:
    - · Engagement nature, objectives, timeline and resource requirements
    - · Timing and extent of audit procedures to complete the engagement
- **1202 Risk Assessment in Planning**
  - 1202.1 The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources.
  - 1202.2 IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements.
  - 1202.3 IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.
- **1203 Performance and Supervision**
  - 1203.1 IS audit and assurance professionals shall conduct the work in accordance with the approved IS audit plan to cover identified risk and within the agreed-on schedule.
  - 1203.2 IS audit and assurance professionals shall provide supervision to IS audit staff whom they have supervisory responsibility for so as to accomplish audit objectives and meet applicable professional audit standards.

- 1203.3 IS audit and assurance professionals shall accept only tasks that are within their knowledge and skills or for which they have a reasonable expectation of either acquiring the skills during the engagement or achieving the task under supervision.
- 1203.4 IS audit and assurance professionals shall obtain sufficient and appropriate evidence to achieve the audit objectives. The audit findings and conclusions shall be supported by appropriate analysis and interpretation of this evidence.
- 1203.5 IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions.
- 1203.6 IS audit and assurance professionals shall identify and conclude on findings.

- **1204 Materiality**
  - 1204.1 IS audit and assurance professionals shall consider potential weaknesses or absences of controls while planning an engagement, and whether such weaknesses or absences of controls could result in a significant deficiency or a material weakness.
  - 1204.2 IS audit and assurance professionals shall consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures.
  - 1204.3 IS audit and assurance professionals shall consider the cumulative effect of minor control deficiencies or weaknesses and whether the absence of controls translates into a significant deficiency or a material weakness.
  - 1204.4 IS audit and assurance professionals shall disclose the following in the report:
    - Absence of controls or ineffective controls
    - Significance of the control deficiency
    - Probability of these weaknesses resulting in a significant deficiency or material weakness
- **1205 Evidence**
  - 1205.1 IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results.
  - 1205.2 IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.
- **1206 Using the Work of Other Experts**
  - 1206.1 IS audit and assurance professionals shall consider using the work of other experts for the engagement, where appropriate.
  - 1206.2 IS audit and assurance professionals shall assess and approve the adequacy of the other experts' professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement.
  - 1206.3 IS audit and assurance professionals shall assess, review and evaluate the work of other experts as part of the engagement, and document the conclusion on the extent of use and reliance on their work.
  - 1206.4 IS audit and assurance professionals shall determine whether the work of other experts, who are not part of the engagement team, is adequate and complete to conclude on the current engagement objectives, and clearly document the conclusion.
  - 1206.5 IS audit and assurance professionals shall determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.
  - 1206.6 IS audit and assurance professionals shall apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.
  - 1206.7 IS audit and assurance professionals shall provide an appropriate audit opinion or conclusion and include any scope limitation where required evidence is not obtained through additional test procedures.
- **1207 Irregularity and Illegal Acts**
  - 1207.1 IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement.
  - 1207.2 IS audit and assurance professionals shall maintain an attitude of professional scepticism during the engagement.
  - 1207.3 IS audit and assurance professionals shall document and communicate any material irregularities or illegal act to the appropriate party in a timely manner.

Reporting

- **1401 Reporting**
  - 1401.1 IS audit and assurance professionals shall provide a report to communicate the results upon completion of the engagement including:
    - Identification of the enterprise, the intended recipients and any restrictions on content and circulation
    - The scope, engagement objectives, period of coverage and the nature, timing and extent of the work performed
    - The findings, conclusions, and recommendations
    - Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement
    - Signature, date and distribution according to the terms of the audit charter or engagement letter
  - 1401.2 IS audit and assurance professionals shall ensure that findings in the audit report are supported by sufficient and appropriate evidence.
- **1402 Follow-up Activities**
  - 1402.1 IS audit and assurance professionals shall monitor relevant information to conclude whether management has planned/taken appropriate, timely action to address reported audit findings and recommendations.

> **Note:** The CISA exam does not test whether a candidate knows the specific number of an IS auditing standard. The CISA exam tests how standards are applied within the audit process.

1.3.3 ISACA IS AUDIT AND ASSURANCE GUIDELINES

The objective of the ISACA IS Audit and Assurance Guidelines is to provide guidance and additional information on how to comply with the ISACA IS Audit and Assurance Standards. The IS auditor and assurance professional should:

- Consider them in determining how to implement the above standards.
- Use professional judgment in applying them to specific audits.
- Be able to justify any departure from the standards.

Note: The CISA candidate is not expected to know the specific number of an IS Audit and Assurance Guideline. The CISA exam tests how guidelines are applied within the audit process. The IS auditor should review the IS Audit and Assurance Guidelines thoroughly to identify the subject matter that is truly needed in the job. The IS Audit and Assurance Guidelines are living documents. The most current documents may be viewed at *www.isaca.org/guidelines*.

The following are the Purpose sections of the guidelines, section 1.1.

General

- **2001 Audit Charter**
  - 1.1.1 The purpose of this guideline is to assist IS audit and assurance professionals in preparing an audit charter. The audit charter defines the purpose, responsibility, authority and accountability of the IS audit and assurance function.
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2002 Organisational Independence**
  - 1.1.1 The purpose of this guideline is to address the independence of the IS audit and assurance function in the enterprise. Three important aspects are considered:
    - The position of the IS audit and assurance function within the enterprise
    - The level to which the IS audit and assurance function reports to within the enterprise
    - The performance of non-audit services within the enterprise by IS audit and assurance management and IS audit and assurance professionals
  - 1.1.2 This guideline provides guidance on assessing organisational independence and details the relationship between organisational independence and the audit charter and audit plan.
  - 1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2003 Professional Independence**
  - 1.1.1 The purpose of this guideline is to provide a framework that enables the IS audit and assurance professional to:
    - Establish when independence may be, or may appear to be, impaired
    - Consider potential alternative approaches to the audit process when independence is, or may appear to be, impaired
    - Reduce or eliminate the impact on independence of IS audit and assurance professionals performing non-audit roles, functions and services
    - Determine disclosure requirements when required independence may be, or may appear to be, impaired
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2004 Reasonable Expectation**
  - 1.1.1 The purpose of this guideline is to assist the IS audit and assurance professionals in implementing the principle of reasonable expectation in the execution of audit engagements. The main features over which the professionals should have reasonable expectation are that:
    - The audit engagement can be completed in accordance with these standards, other applicable standards or regulations, and result in a professional opinion or conclusion.
    - The scope of the audit engagement permits an opinion or conclusion to be expressed on the subject matter.
    - Management will provide them with appropriate, relevant and timely information required to perform the audit engagement.
  - 1.1.2 This guideline further assists the IS audit and assurance professionals in addressing scope limitations and provides guidance on accepting a change in terms.
  - 1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2005 Due Professional Care**
  - 1.1.1 The purpose of this guideline is to clarify the term 'due professional care' as it applies to performing an audit engagement with integrity and care in compliance with the ISACA Code of Professional Ethics.
  - 1.1.2 This guideline explains how IS audit and assurance professionals should apply due professional care in planning, performing and reporting on an audit engagement.
  - 1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2006 Proficiency**
  - 1.1.1 This guideline provides guidance to the IS audit and assurance professionals to acquire the necessary skills and knowledge and maintain the professional competences while carrying out audit engagements.
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2007 Assertions**
  - 1.1.1 The purpose of this guideline is to detail the different assertions, guide IS audit and assurance professionals in assuring that the criteria, against which the subject matter is to be assessed, supports the assertions, and provide guidance on formulating a conclusion and drafting a report on the assertions.
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2008 Criteria**
  - 1.1.1 The purpose of this guideline is to assist IS audit and assurance professionals in selecting criteria, against which the subject matter will be assessed, that are suitable, acceptable and come from a relevant source.

- 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

Performance

- **2201 Engagement Planning**
  - 1.1.1 This guideline provides guidance to the IS audit and assurance professionals. Adequate planning helps to ensure that appropriate attention is devoted to important areas of the audit, potential problems are identified and resolved on a timely basis, and the audit engagement is properly organised, managed and performed in an effective and efficient manner.
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2202 Risk Assessment in Planning**
  - 1.1.1 The level of audit work required to meet the audit objective is a subjective decision made by IS audit and assurance professionals. The purpose of this guideline is to reduce the risk of reaching an incorrect conclusion based on the audit findings and to reduce the existence of errors occurring in the area being audited.
  - 1.1.2 The guideline provides guidance in applying a risk assessment approach to develop an:
    - IS audit plan that covers all annual audit engagements
    - Audit engagement project plan that focuses on one specific audit engagement
  - 1.1.3 The guideline provides the details of the different types of risk the IS audit and assurance professionals encounter.
  - 1.1.4 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2203 Performance and Supervision**
  - 1.1.1 This guideline provides guidance to IS audit and assurance professionals in performing the audit engagement and supervising IS audit team members. It covers:
    - Performing an audit engagement
    - Roles and responsibilities, required knowledge and skills for performing audit engagements
    - Key aspects of supervision
    - Gathering evidence
    - Documenting work performed
    - Formulating findings and conclusions
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2204 Materiality**
  - 1.1.1 The purpose of this guideline is to clearly define the concept 'materiality' for the IS audit and assurance professionals and make a clear distinction with the materiality concept used by financial audit and assurance professionals.
  - 1.1.2 The guideline assists the IS audit and assurance professionals in assessing materiality of the subject matter and considering materiality in relationship to controls and reportable issues.
  - 1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2205 Evidence**
  - 1.1.1 The purpose of this guideline is to provide guidance to IS audit and assurance professionals in obtaining sufficient and appropriate evidence, evaluating the received evidence and preparing appropriate audit documentation.
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2206 Using the Work of Other Experts**
  - 1.1.1 This guideline provides guidance to IS audit and assurance professionals when considering the use of work of other experts. The guideline assists in assessing the adequacy of the experts, reviewing and evaluating the work of other experts, assessing the need for performing additional test procedures and expressing an opinion for the audit engagement, while taking into account the work performed by other experts.
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2207 Irregularity and Illegal Acts**
  - 1.1.1 The purpose of this guideline is to provide IS audit and assurance professionals with guidance on how to deal with irregularities and illegal acts.
  - 1.1.2 The guideline details the responsibilities of both management and IS audit and assurance professionals with regards to irregularities and illegal acts. It furthermore provides guidance on how to deal with irregularities and illegal acts during the planning and performance of the audit work. Finally, the guideline suggests good practices for internal and external reporting on irregularities and illegal acts.
  - 1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standards, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2208 Sampling**
  - 1.1.1 The purpose of this guideline is to provide guidance to IS audit and assurance professionals to design and select an audit sample and evaluate sample results. Appropriate sampling and evaluation will help in achieving the requirements of sufficient and appropriate evidence.
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement related standards, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

Reporting

- **2401 Reporting**
  - 1.1.1 This guideline provides guidance for IS audit and assurance professionals on the different types of IS audit engagements and related reports.
  - 1.1.2 The guideline details all aspects that should be included in an audit engagement report and provides IS audit and assurance professionals with considerations to make when drafting and finalising an audit engagement report.
  - 1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.
- **2402 Follow-up Activities**
  - 1.1.1 The purpose of this guideline is to provide guidance to IS audit and assurance professionals in monitoring if management has taken appropriate and timely action on reported recommendations and audit findings.
  - 1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

> **Note:** The CISA candidate should be familiar with IS Audit and Assurance Guideline 2001 Audit Charter. Also important is 2207 Irregularities and Illegal Acts in relation to the standard 1207 Irregularities and Illegal Acts for the purpose of reporting irregularities such as fraud. In addition, the IS auditor should be familiar with the IS Audit and Assurance Guideline 2003 Professional Independence and the related standard 1003 Professional Independence. Knowledge on 2402 Follow-up Activities, should be further identified by the IS auditor in the IS Audit and Assurance Guidelines.

1.3.4 ISACA IS AUDIT AND ASSURANCE TOOLS AND TECHNIQUES

Tools and techniques developed by ISACA provide examples of possible processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific tool and technique, IS auditors should apply their own professional judgment to the specific circumstances. The tools and techniques documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements.

Tools and techniques are currently categorized into:

- White papers, *www.isaca.org/whitepapers* (complimentary PDF files)
- Audit/Assurance programs, *www.isaca.org/auditprograms* (complimentary Microsoft® Word files for ISACA members)
- COBIT 5 family of products, *www.isaca.org/cobit*
- Technical and Risk Management Reference series, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/Pages/Reference-Series.aspx* (available in the ISACA Bookstore)
- *ISACA® Journal* IT Audit Basics column, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IT-Audit-Basics/Pages/IT-Audit-Basics-Articles.aspx* (complimentary access)

It is not mandatory for the IS auditor to follow these tools and techniques; however, following these procedures will provide assurance that the standards are being followed by the auditor.

> **Note:** The ISACA IS Audit and Assurance Tools and Techniques are living documents. The most current documents may be viewed at *www.isaca.org/standards.*

1.3.5 RELATIONSHIP AMONG STANDARDS, GUIDELINES, AND TOOLS AND TECHNIQUES

Standards defined by ISACA are to be followed by the IS auditor. Guidelines provide assistance on how the auditor can implement standards in various audit assignments. Tools and techniques are not intended to provide exhaustive guidance to the auditor when performing an audit. Tools and techniques provide examples of steps the auditor may follow in specific audit assignments to implement the standards; however, the IS auditor should use professional judgment when using guidelines and tools and techniques.

There may be situations in which the legal/regulatory requirements are more stringent than the requirements contained in ISACA IS Audit and Assurance Standards. In such cases, the IS auditor should ensure compliance with the more stringent legal/regulatory requirements.

For example, section 2.3.2 of Guideline 2002 supporting Standard 1002 Organisational Independence states: "Activities that are routine and administrative or involve matters that are insignificant generally are deemed not to be management responsibilities and, therefore, would not impair independence. Non-audit services that would also not impair independence or objectivity if adequate safeguards are implemented include providing routine advice on information technology risk and controls." However, in some countries, regulatory enactments strictly prohibit auditors from accepting audit assignments from banks from which they have availed credit facilities. In such cases, IS auditors should give precedence to the applicable regulatory requirement and not accept the assignment, even though accepting the assignment would be in compliance with the requirement of the Guideline 2002. As stated throughout the IS Audit and Assurance Guidelines, the IS audit and assurance professionals should consider all guidelines when determining how to implement related standards, use professional judgment in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.3.6 ITAF™

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

- Establishes standards that address IS audit and assurance professional 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

ITAF is focused on ISACA material and provides a single source through which IS audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programs, and develop effective reports. ITAF 3rd Edition (*www.isaca.org/ITAF*) incorporates guidelines effective 1 September 2014. As new guidance is developed and issued, it will be indexed within the framework.

1.4 IS CONTROLS

In order for information systems to fully realize the benefits and risk and resource optimization goals, risk that could prevent or inhibit obtaining these goals needs to be addressed. Organizations design, develop, implement and monitor information systems through policies, procedures, practices and organizational structures to address these types of risk. The internal control life cycle is dynamic in nature and designed to provide reasonable assurance that business goals and objectives will be achieved and undesired events will be prevented or detected and corrected.

1.4.1 RISK ANALYSIS

Risk analysis is part of audit planning and helps identify risk and vulnerabilities so the IS auditor can determine the controls needed to mitigate risk.

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

Risk is the combination of the probability of an event and its consequence (*International Organization for Standardization [ISO] 31000:2009: Risk management—Principles and guidelines/ISO Guide 73:2009: Risk management—Vocabulary*). Business risk may negatively impact the assets, processes or objectives of a specific business or organization. The 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, IS auditors will often assess the effectiveness of the risk management process an organization uses.

In analyzing the business risk arising from the use of IT, it is important for the IS auditor to have a clear understanding of:

- 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
- The dependence on technology to process and deliver business information
- 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

ISACA's *Risk IT Framework* is based on a set of guiding principles and features business processes and management guidelines that conform to these principles. It is dedicated to helping enterprises manage IT-related risk. The collective experience of a global team of practitioners and experts and existing and emerging practices and methodologies for effective IT risk management have been consulted in the development of the Risk IT framework.

There are many definitions of risk, reflecting that risk means different things to different people. Perhaps one of the most holistic definitions of risk applicable throughout the information security business world is derived from *NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments*:

> *Adverse impact(s) that could occur…to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations…due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.*

This definition is used commonly by the IT industry because it puts risk into an organizational context by using the concepts of assets and loss of value—terms that are easily understood by business managers.

The risk assessment process is characterized as 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 (hardware, software, databases, networks, facilities, people, etc.) critical to achieving these objectives. Because IT risk is dynamic, it is strategic for management to recognize the need for and establish a dynamic IT risk management process that supports the business risk management process. The greatest degree of risk management effort may then be directed toward those considered most sensitive or critical to the organization. After sensitive and/or critical information assets are identified, 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.

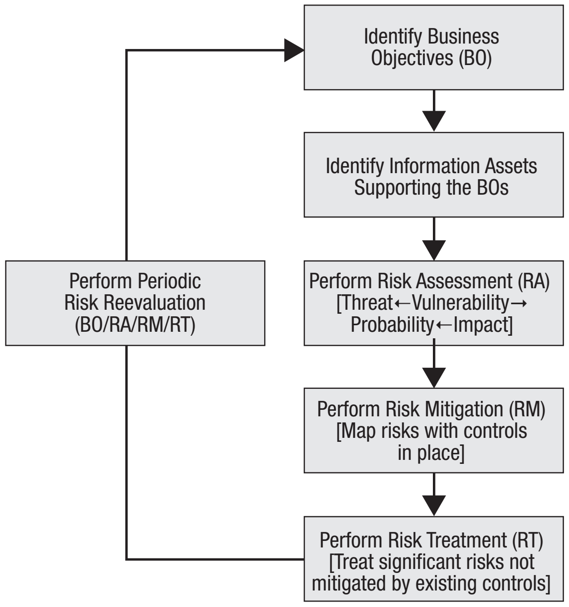
Next, during the risk mitigation phase, controls are identified for mitigating identified risk. These controls are risk-mitigating countermeasures that should prevent or reduce the likelihood of a risk event occurring, detect the occurrence of a risk event, minimize the impact, or transfer the risk to another organization.

The assessment of countermeasures should be performed through a cost-benefit analysis where controls to mitigate risk are selected

to reduce risk to a level acceptable to management. This analysis process may be based on any of the following:
- The cost of the control compared to the benefit of minimizing the risk
- Management's appetite for risk (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)

The final phase relates to monitoring performance levels of the risk being managed when identifying any significant changes in the environment that would trigger a risk reassessment, warranting changes to its control environment. It 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 organization that endeavors to continually identify and evaluate risk as it arises and evolves. See **figure 1.3** for the summary of the risk management process.

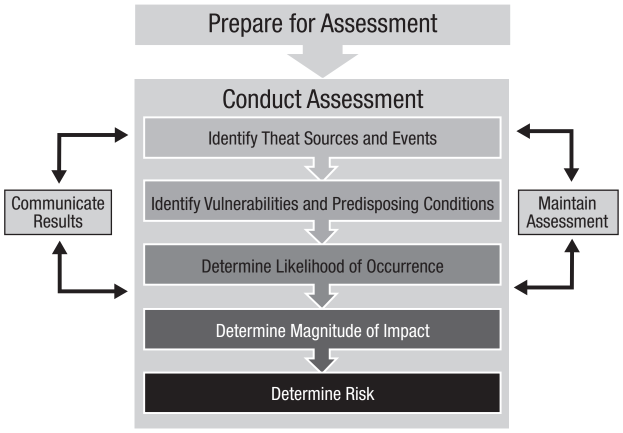
Figure 1.3—Risk Management Process


Identify Business Objectives (BO)
Identify Information Assets Supporting the BOs
Perform Periodic Risk Reevaluation (BO/RA/RM/RT)
Perform Risk Assessment (RA) [Threat←Vulnerability→ Probability←Impact]
Perform Risk Mitigation (RM) [Map risks with controls in place]
Perform Risk Treatment (RT) [Treat significant risks not mitigated by existing controls]

From the IS auditor's perspective, risk analysis serves more than one purpose:
- It assists the IS auditor in identifying risk and threats to an IT environment and IS system—risk and threats that would need to be addressed by management—and in identifying system-specific internal controls. Depending on the level of risk, this assists the IS auditor in selecting certain areas to examine.
- It helps the IS auditor in his/her evaluation of controls in audit planning.
- It assists the IS auditor in determining audit objectives.
- It supports risk-based audit decision making.

Figure 1.4 depicts the specific processes used by the IS auditor to realize the above listed objectives.

Figure 1.4—Risk Assessment Process


Prepare for Assessment
Conduct Assessment
Identify Theat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Communicate Results
Maintain Assessment

Source: National Institute of Standards and Technology (NIST), *NIST Special Publication 800-30, Revision 1: Information Security*, USA, 2012. Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

1.4.2 INTERNAL CONTROLS

Internal 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 risk events will be prevented, or detected and corrected. Internal control activities and supporting processes are either manual or driven by automated computer information resources. Internal controls operate at all levels within an organization to mitigate its exposures to risk 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 and (2) what should be avoided. Internal controls address business/operational objectives and should also address undesired events through prevention, detection and correction.

Elements of controls that should be considered when evaluating control strength are classified as preventive, detective or corrective in nature.

Figure 1.5 displays control classifications, functions and usages.

Figure 1.5—Control Classifications

Class	Function	Examples
Preventive	• Detect problems before they arise. • Monitor both operation and inputs. • Attempt to predict potential problems before they occur and make adjustments. • Prevent an error, omission or malicious act from occurring. • Segregate duties (deterrent factor). • Control access to physical facilities. • Use well-designed documents (prevent errors).	• Employ only qualified personnel. • Establish suitable procedures for authorization of transactions. • Complete programmed edit checks. • Use access control software that allows only authorized personnel to access sensitive files. • Use encryption software to prevent unauthorized disclosure of data.
Detective	• Use controls that detect and report the occurrence of an error, omission or malicious act.	• Hash totals • Check points in production jobs • Echo controls in telecommunications • Error messages over tape labels • Duplicate checking of calculations • Periodic performance reporting with variances • Past-due account reports • Internal audit functions • Review of activity logs to detect unauthorized access attempts • Secure code reviews • Software quality assurance
Corrective	• Minimize the impact of a threat. • Remedy problems discovered by detective controls. • Identify the cause of a problem. • Correct errors arising from a problem. • Modify the processing system(s) to minimize future occurrences of the problem.	• Contingency/continuity of operations planning • Disaster recovery planning • Incident response planning • Backup procedures • Rerun procedures • System break/fix service level agreements

Note: A CISA candidate should know the differences between preventive, detective and corrective controls.

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 the following concepts:
- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

Control objectives apply to all controls, whether they are manual, automated or a combination (e.g., review of system logs). Control objectives in an IS environment do not differ from those in a manual environment; however, the way these controls are implemented may be different. Thus, control objectives need to be addressed relevant to specific IS-related processes.

1.4.3 IS CONTROL OBJECTIVES

IS control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process. IS control objectives are:
- Statements of the desired result or purpose to be achieved by implementing controls around information systems processes
- Comprised of 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

Enterprise management needs to make choices relative to these control objectives by:
- Selecting those that are applicable
- Deciding on those that will be implemented
- Choosing how to implement them (frequency, span, automation, etc.)
- Accepting the risk of not implementing those that may apply

Specific IS control objectives may include:
- Safeguarding assets: information on automated systems is secure from improper access and current
- Ensuring system development life cycle (SDLC) processes are established, in place and operating effectively to provide reasonable assurance that business, financial and/or industrial software systems and applications are developed in a repeatable and reliable manner to assure business objectives are met. (See chapter 3 Information Systems Acquisition, Development and Implementation, for more information.)
- 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 cause negative impact to the processing of transactions.
  - Accuracy and completeness of processing of transactions
  - All transactions are recorded accurately and entered into the system for the proper period.
  - Reliability of overall information processing activities

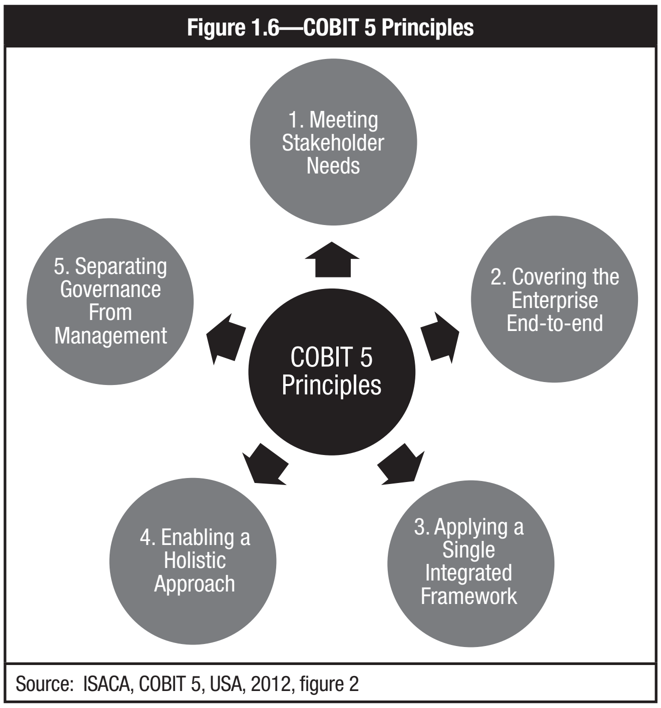
– Accuracy, completeness and security of the output
– Database confidentiality, integrity and availability

- Ensuring appropriate identification and authentication of users of IS resources (end users as well as infrastructure support)
- Ensuring the efficiency and effectiveness of operations (operational objectives)
- Complying with the 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)
- 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 to ensure the organization's assets are properly protected and meet business goals and objectives

1.4.4 COBIT 5

COBIT 5, developed by ISACA, provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT (GEIT). Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

Figure 1.6—COBIT 5 Principles


1. Meeting Stakeholder Needs
5. Separating Governance From Management
2. Covering the Enterprise End-to-end
COBIT 5 Principles
4. Enabling a Holistic Approach
3. Applying a Single Integrated Framework

Source: ISACA, COBIT 5, USA, 2012, figure 2

COBIT 5 is based on five key principles for governance and management of enterprise IT (shown in **figure 1.6**):

- **Principle 1: Meeting Stakeholder Needs**—Enterprises exist to create value for their stakeholders, by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT-related goals and mapping these to specific processes and practices.
- **Principle 2: Covering the Enterprise End-to-End**—COBIT 5 integrates governance of enterprise IT into enterprise governance:
  – It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the "IT function," but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.
  – It considers all IT-related governance and management enablers to be enterprisewide and end-to-end (i.e., inclusive of everything and everyone—internal and external—that is relevant to governance and management of enterprise information and related IT).
- **Principle 3: Applying a Single, Integrated Framework**—There are many IT-related standards and good practices, each providing guidance on a subset of IT activities. COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT.
- **Principle 4: Enabling a Holistic Approach**—Efficient and effective governance and management of enterprise IT requires a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise. The COBIT 5 framework defines seven categories of enablers:
  – Principles, Policies and Frameworks
  – Processes
  – Organizational Structures
  – Culture, Ethics and Behavior
  – Information
  – Services, Infrastructure and Applications
  – People, Skills and Competencies
- **Principle 5: Separating Governance from Management**—The COBIT 5 framework 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 5's view on this key distinction between governance and management is:
  – Governance

Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

– Management

Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).

Together, these five principles enable the enterprise to build an effective governance and management framework that optimizes information and technology investment and use for the benefit of stakeholders.

Note: A CISA candidate will not be asked to specifically identify the COBIT process, the COBIT domains or the set of IT processes defined in each. However, candidates should know what frameworks are, what they do and why they are used by enterprises. Knowledge of the existence, structure and key principles of major standards and frameworks related to IT governance, assurance and security will also be advantageous. COBIT can be used as a supplemental study material in understanding control objectives and principles as detailed in this review material.

1.4.5 GENERAL CONTROLS

Controls include policies, procedures and practices (tasks and activities) established by management to provide reasonable assurance that specific objectives will be achieved.

General controls apply to all areas of the organization including IT infrastructure and support services. General controls include:

- Internal accounting controls that are primarily directed at accounting operations—controls that concern the safeguarding of assets and reliability of financial records
- Operational controls that concern day-to-day operations, functions and activities, and ensure that the operation is meeting the business objectives
- Administrative controls that concern operational efficiency in a functional area and adherence to management policies (administrative controls support the operational controls specifically concerned with these areas)
- Organizational security policies and procedures to ensure proper usage of assets
- Overall policies for the design and use of adequate documents and records (manual/automated) to help ensure proper recording of transactions—transactional audit trail
- Procedures and practices to ensure adequate safeguards over access to and use of assets and facilities
- Physical and logical security policies for all facilities, data centers and IT resources (e.g., servers and telecom infrastructure)

1.4.6 IS SPECIFIC CONTROLS

Each general control 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, the 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 computer equipment. The IS auditor should understand the basic control objectives that exist for all functions. IS 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
- Business continuity (BCP)/disaster recovery planning (DRP)
- Networks and communications
- Database administration
- Protection and detective mechanisms against internal and external attacks

The IS auditor should understand concepts regarding IS controls and how to apply them in planning an audit.

Note: The IS controls listed in this section should be considered by the CISA candidate within the related job practice area (i.e., Protection of Information Assets).

1.5 PERFORMING AN IS AUDIT

Several steps are required to perform an audit. Adequate planning is a necessary first step in performing effective IS audits. 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 the 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 (areas of control weaknesses with recommendations for remediation) in an objective manner to management.

Audit management must ensure the availability of adequate audit resources and a schedule for performing the audits and, in the case of internal IS audit, for 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 managing and administering audit projects, whether automated or manual, include the following basic steps:

- **Plan the audit engagement**—Plan the audit considering project-specific risk.

- **Build the audit plan**—Chart out the necessary audit tasks across a time line, 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**—IS auditors report their 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 substantiating that internal controls exist to minimize business risk and that they function as expected. These audit objectives include assuring compliance with legal and regulatory requirements as well as the confidentiality, integrity, reliability and availability of information and IT resources. Audit management may give the 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 the 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 the account-posting activities.

The IS auditor must have an understanding of 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 basic purposes of any IS audit is to identify control objectives and the related controls that address the objective. For example, the IS auditor's initial review of an information system should identify key controls. The IS auditor should then decide whether to test these controls for compliance. The 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 these processes and general support systems. Based on that understanding, the 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 computer-assisted audit techniques (CAATs).

1.5.2 TYPES OF AUDITS

The IS auditor should understand the various types of audits that can be performed, internally or externally, and the audit procedures associated with each:

- **Compliance audits**—Compliance audits include specific tests of controls to demonstrate adherence to specific regulatory or industry standards. These audits often overlap traditional audits but may focus on particular systems or data. Examples include Payment Card Industry Data Security Standard (PCI DSS) audits for companies that process credit card data and Health Insurance Portability and Accountability Act (HIPAA) audits for companies that handle health care data.
- **Financial audits**—The purpose of a financial audit is to assess the accuracy of financial reporting. A financial audit will often involve detailed, substantive testing, although increasingly, auditors are placing more emphasis on a risk- and control-based audit approach. This kind of audit relates to financial information integrity and reliability.
- **Operational audits**—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 some examples of operational audits.
- **Integrated audits**—An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance. An integrated audit can be performed by external or internal auditors and would include compliance tests of internal controls and substantive audit steps.
- **Administrative audits**—These are oriented to assess issues related to the efficiency of operational productivity within an organization.
- **IS audits**—This process collects and evaluates evidence to determine whether the information systems and related resources adequately safeguard assets, 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 that business, operational and control objectives will be met and that undesired events will be prevented, or detected and corrected, in a timely manner.
- **Specialized audits**—Within the category of IS audits, a number of specialized reviews examine areas such as services performed by third parties. Because businesses are becoming increasingly reliant on third-party service providers, it is important that internal controls be evaluated in these environments. The Statement on Standards for Attestation Engagements 16 (SSAE 16), titled, "Reporting on Controls at a Service Organization," is a widely known auditing standard developed by the American Institute of Certified Public Accountants (AICPA). This standard replaced the previous standard, Statement on Auditing Standards 70 (SAS 70), titled "Reports on the Processing of Transactions by Service Organizations." This standard defines the professional standards used by a service auditor to assess the internal controls of a service organization. This type of audit has become increasingly relevant due to the current trend of outsourcing of financial and business processes to third-party service providers, which, in some cases, may operate in different jurisdictions or even different countries. It should be noted that a Type 2 SSAE 16 review is a more thorough variation of a regular SSAE 16 review, which is often required in connection with regulatory reviews. Many other countries have their own equivalent of this standard. An SSAE 16–type audit is important because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related

processes. SSAE 16–type reviews provide guidance to enable an independent auditor (service auditor) to issue an opinion on a service organization's description of controls through a service auditor's report, which then can be relied on by the IS auditor of the entity that utilizes the services of the service organization.

- **Forensic audits**—Forensic auditing has been defined as auditing specialized in discovering, disclosing and following up on fraud and crimes. The primary purpose of such a review is the development of evidence for review by law enforcement and judicial authorities. Forensic professionals have been called on to participate in investigations related to corporate fraud and cybercrime. In cases where computer resources may have been misused, further investigation is necessary to gather evidence for possible criminal activity that can then be reported to appropriate authorities. A computer forensic investigation includes the analysis of electronic devices such as computers, smartphones, disks, switches, routers, hubs and other electronic equipment. An IS auditor possessing the necessary skills can assist the information security manager in performing forensic investigations and conduct the audit of the systems to ensure compliance with the evidence collection procedures for forensic investigation. Electronic evidence is vulnerable to changes; therefore, it is necessary to handle electronic evidence with utmost care and controls should ensure that no manipulation can occur. Chain of custody for electronic evidence should be established to meet legal requirements.

  Improperly handled computer evidence is subject to being ruled inadmissible by judicial authorities. The most important consideration for a forensic auditor is to make a bit-stream image of the target drive and examine that image without altering date stamps or other information attributable to the examined files. Further, forensic audit tools and techniques such as data mapping for security and privacy risk assessment, and the search for intellectual property for data protection, are also being used for prevention, compliance and assurance.

1.5.3 AUDIT METHODOLOGY

An audit methodology is a set of documented audit procedures designed to achieve planned audit objectives. Its components are a statement of scope, audit objectives and audit programs.

The audit methodology should be set up and approved by audit management to achieve consistency in the audit approach. This methodology should be formalized and communicated to all audit staff.

Figure 1.7 lists the phases of a typical audit. An early and critical product of the audit process should be an audit program that is the guide for performing and documenting all of the audit steps and the extent and types of evidential matter reviewed.

Although an audit program does not necessarily follow a specific set of steps, the IS auditor typically would follow, as a minimum course of action, sequential program steps to gain an understanding of the entity under audit, evaluate the control structure and test the controls.

Figure 1.7—Audit Phases

Audit Phase	Description
Audit subject	• Identify the area to be audited.
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.
Audit scope	• Identify the specific systems, function or unit of the organization to be included in the review. For example, in the previous program changes example, the scope statement might limit the review to a single application system or to a limited period of time.
Preaudit planning	• Identify technical skills and resources needed. • Identify the sources of information for test or review such as functional flow charts, policies, standards, procedures and prior audit work papers. • Identify locations or facilities to be audited. • Develop a communication plan at the beginning of each engagement that describes who to communicate to, when, how often and for what purpose(s).
Audit procedures and steps for data gathering	• Identify and select the audit approach to verify and test the controls. • Identify a list of individuals to interview. • Identify and obtain departmental policies, standards and guidelines for review. • Develop audit tools and methodology to test and verify control.
Procedures for evaluating the test or review results	• Identify methods (including tools) to perform the evaluation. • Identify criteria for evaluating the test (similar to a test script for the auditor to use in conducting the evaluation). • Identify means and resources to confirm the evaluation was accurate (and repeatable, if applicable).
Procedures for communication with management	• Determine frequency of communication. • Prepare documentation for final report.
Audit report preparation	• Disclose follow-up review procedures. • Disclose procedures to evaluate/test operational efficiency and effectiveness. • Disclose procedures to test controls. • Review and evaluate the soundness of documents, policies and procedures.

Each audit department should design and approve an audit methodology as well as the minimum steps to be observed in any audit assignment.

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 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 their 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.

1.5.4 RISK-BASED AUDITING

Effective risk-based auditing is driven by two processes:

1. The risk assessment that drives the audit schedule (see section 1.5.6 Risk Assessment and Treatment)
2. The risk assessment that minimizes the audit risk during the execution of an audit (see section 1.5.5 Audit Risk and Materiality)

A risk-based audit approach is usually adapted to develop and improve the continuous audit process. This 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 the 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 weaknesses. In a risk-based audit approach, IS auditors are not just relying on risk; they also are relying on internal and operational controls as well as knowledge of the company or the business. This type of risk assessment decision can help relate the cost-benefit analysis of the control to the known risk, allowing practical choices.

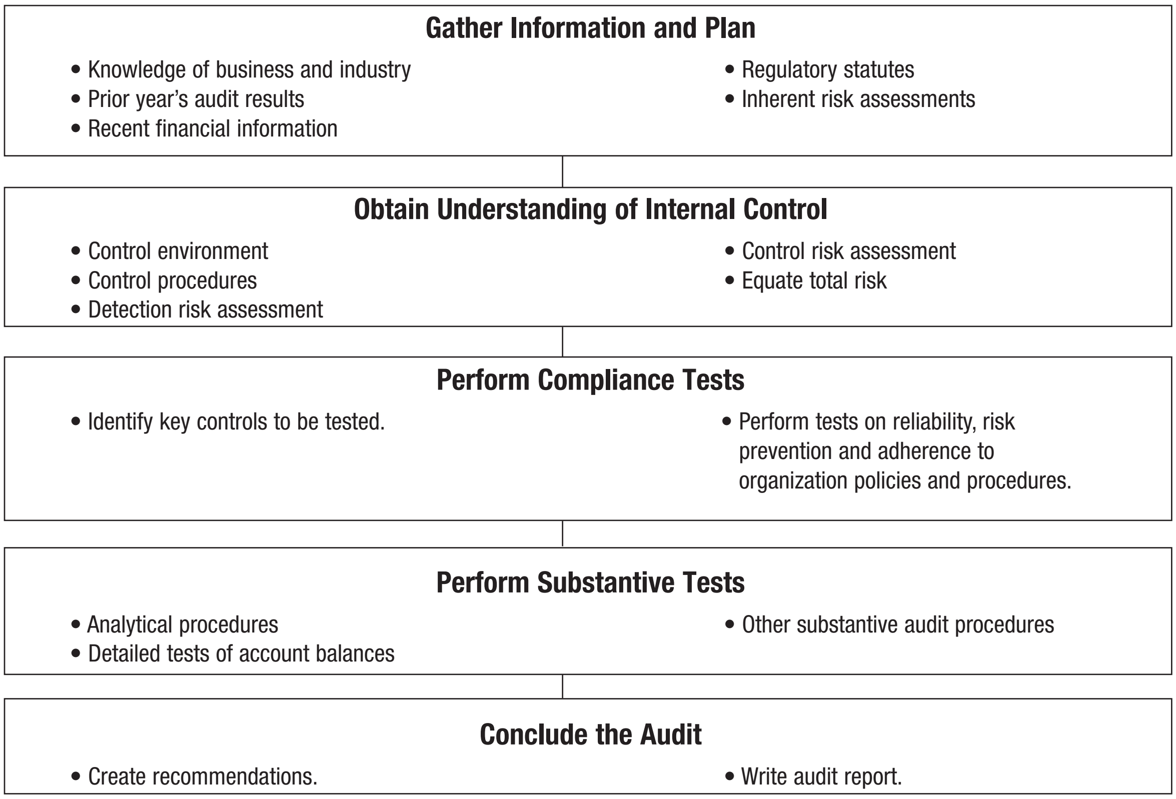
Business risk includes concerns about the probable effects of an uncertain event on achieving established business objectives. The nature of business risk may be financial, regulatory or operational and may also include risk derived from specific technology. For example, an airline company is subject to extensive safety regulations and economic changes, both of which impact the continuing operations of the company. In this context, the availability of IT service and its reliability are critical.

By understanding the nature of the business, IS auditors can identify and categorize the types of risk that will better determine the 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 where risk has been 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 can be seen in **figure 1.8**.

1.5.5 AUDIT RISK AND MATERIALITY

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

Figure 1.8—Risk-based Audit Approach


Gather Information and Plan
• Knowledge of business and industry
• Prior year's audit results
• Recent financial information
• Regulatory statutes
• Inherent risk assessments
Obtain Understanding of Internal Control
• Control environment
• Control procedures
• Detection risk assessment
• Control risk assessment
• Equate total risk
Perform Compliance Tests
• Identify key controls to be tested.
• Perform tests on reliability, risk prevention and adherence to organization policies and procedures.
Perform Substantive Tests
• Analytical procedures
• Detailed tests of account balances
• Other substantive audit procedures
Conclude the Audit
• Create recommendations.
• Write audit report.

Audit risk is influenced by:

- **Inherent risk**—As it relates to audit risk, it is the risk level or exposure of the process/entity to be audited without taking into account the controls that management has implemented. Inherent risk exists independent of an audit and can occur because of the nature of the business.
- **Control risk**—The risk that a material error exists 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 easily missed 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**—The risk that material errors or misstatements that have occurred will not be detected by the IS auditor.
- **Overall audit risk**—The probability that information or financial reports may contain material errors and that the auditor may not detect an error that has occurred. 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 a sufficiently low level at the completion of the examination.

Note: Audit risk should not be confused 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.

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

The IS auditor should have a good understanding of audit risk when planning an audit. An audit sample may not detect 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, the 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.

The concept of materiality requires sound judgment from the IS auditor. The IS auditor may detect a small error that could be considered significant at an operational level, but may not be viewed as significant to upper management. Materiality considerations combined with an understanding of audit risk are essential concepts for planning the areas to be audited and the specific test to be performed in a given audit.

1.5.6 RISK ASSESSMENT AND TREATMENT

Assessing Risk

To develop a more complete understanding of audit risk, the IS auditor should also understand how the organization being audited approaches risk assessment and treatment.

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 also be performed periodically to address changes in the environment, security requirements and in the risk situation (e.g., in the assets, threats, vulnerabilities, impacts) and when significant changes occur. These risk assessments should be undertaken in a methodical manner capable of producing comparable and reproducible results.

The scope of a risk assessment can be either the entire organization, parts of the organization, an individual information system, specific system components or services where this is practicable, realistic and helpful.

Treating Risk

Before considering the treatment of risk, the organization should decide the criteria for determining whether risk can be managed within the risk appetite. Risk may be accepted if, for example, it is assessed that the risk is low or that the cost of treatment is not cost-effective for the organization. Such decisions should be recorded.

Risk identified in the risk assessment needs to be treated. Possible risk response options include:

- **Risk mitigation**—Applying appropriate controls to reduce the risk
- **Risk acceptance**—Knowingly and objectively not taking action, providing the risk clearly satisfies the organization's policy and criteria for risk acceptance
- **Risk avoidance**—Avoiding risk by not allowing actions that would cause the risk to occur
- **Risk transfer/sharing**—Transferring the associated risk to other parties (e.g., insurers or suppliers)

For risk where the risk treatment decision has been to apply appropriate controls, controls should be selected to ensure that risk is reduced to an acceptable level, taking into account:

- Requirements and constraints of national and international legislation and regulations
- Organizational objectives
- Operational requirements and constraints
- Cost-effectiveness (the need to balance the investment in implementation and operation of controls against the harm likely to result from security failures)

Controls can be selected from professional or industry standards, or new controls can be designed to meet the specific needs of the organization. It is necessary to recognize that some controls may not be applicable to every information system or environment and might not be practical for all organizations.

Information security controls should be considered at the systems and project requirements specification and design stage. Failure to do so can result in additional costs and less effective solutions and, in a worst case scenario, the inability to achieve adequate security.

No set of controls can achieve complete security. Additional management action should be implemented to monitor, evaluate and improve the efficiency and effectiveness of security controls to support the organization's aims.

1.5.7 IS AUDIT RISK ASSESSMENT TECHNIQUES

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

There are many risk assessment methodologies, computerized and noncomputerized, from which the IS auditor may choose. These range from simple classifications based on the IS auditor's judgment of high, medium and low to complex scientific calculations that provide a numeric risk rating.

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 judgmental, where an independent decision is made based on business knowledge, executive management directives, historical perspectives, business goals and environmental factors. A combination of techniques may be used as well. Risk assessment methods may change and develop over time to best serve the needs of the organization. The IS auditor should consider the level of complexity and detail appropriate for the organization being audited.

Using risk assessment to determine areas to be audited:
- Enables 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 management. 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

1.5.8 AUDIT PROGRAMS

An audit program is a step-by-step set of audit procedures and instructions that should be performed to complete an audit. Audit programs for financial, operational, integrated, administrative and IS audits are based on the scope and objective of the particular assignment. IS auditors often evaluate IT functions and systems from different perspectives such as security (confidentiality, integrity and availability), quality (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
- A risk assessment and general audit plan and schedule
- Detailed audit planning that would include the necessary audit steps and a breakdown of the work planned across an anticipated time line
- Preliminary review of the audit area/subject
- Evaluating the audit area/subject
- Verifying and evaluating the appropriateness of controls designed to meet control objectives
- Compliance testing (tests of the implementation of controls and their consistent application)
- Substantive testing (confirming the accuracy of information)
- Reporting (communicating results)
- Follow-up in cases where there is an internal audit function

The IS auditor must understand the procedures for testing and evaluating IS controls. These procedures could include:
- The use of generalized audit software to survey the contents of data files (including system logs)
- The use of specialized software to assess the contents of OS database and application parameter files (or detect deficiencies in system parameter settings)
- Flow-charting techniques for documenting automated applications and business processes
- The use of audit logs/reports available in operation/application systems
- Documentation review
- Inquiry and observation
- Walk-throughs
- Reperformance of controls

The IS auditor should have a sufficient understanding of these procedures to allow for the planning of appropriate audit tests.

Note: For audit program examples, visit *www.isaca.org/auditprograms*

1.5.9 FRAUD DETECTION

The use of information technology for business has immensely benefited enterprises in terms of significantly increased quality of delivery of information. However, the widespread use of information technology and the Internet leads to risk that enables the perpetration of errors and fraud.

Management is primarily responsible for establishing, implementing and maintaining a framework and design of IT controls to meet the control objectives. A well-designed internal control system provides good opportunities for deterrence and/or timely detection of fraud. Internal controls may fail where such controls are circumvented by exploiting vulnerabilities or through management perpetrated weakness in controls or collusion among people.

Legislation and regulations relating to corporate governance cast significant responsibilities on management, auditors and the audit committee regarding detection and disclosure of any fraud, whether material or not.

IS auditors should observe and exercise due professional care (1005 Due Professional Care) in all aspects of their work. IS auditors entrusted with assurance functions should ensure reasonable care while performing their work and be alert to the possible opportunities that allow fraud to materialize.

The presence of internal controls does not altogether eliminate fraud. IS auditors should be aware of the possibility and means of perpetrating fraud, especially by exploiting the vulnerabilities and overriding controls in the IT-enabled environment. IS auditors 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, the IS auditor may come across instances or indicators of fraud. After careful evaluation, the IS auditor may communicate the need for a detailed investigation to appropriate authorities. In the case of the auditor identifying a major fraud or if the risk associated with the detection is high, audit management should also consider communicating in a timely manner to the audit committee.

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

1.5.10 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 the 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 IS auditors with reasonable assurance that the particular control on which the IS auditor plans to rely is operating as the IS auditor perceived in the preliminary evaluation.

It is important that the 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—for example, 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 these balances. IS auditors could use substantive tests to test 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 determine whether the tape library inventory records are stated correctly. To perform this test, the IS auditor might take a thorough inventory or might use a statistical sample, which will allow the IS auditor to develop a conclusion regarding the accuracy of the entire inventory.

There is a direct correlation 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 the IS auditor is justified in minimizing the substantive procedures. 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, software license audits, etc.

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, etc.

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

Figure 1.9 shows the relationship between compliance and substantive tests and describes the two categories of substantive tests.

Note: The IS auditor should be knowledgeable on when to perform compliance tests or substantive tests.

1.5.11 EVIDENCE

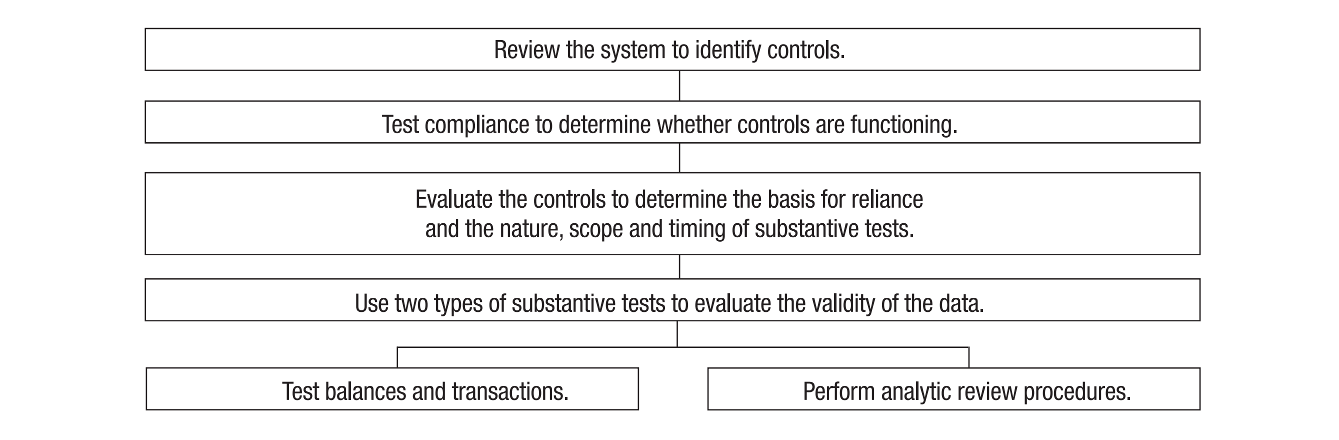
Evidence is any information used by the IS auditor to determine whether the entity or data being audited follows the established criteria or objectives and supports audit conclusions. It is a requirement that the auditor's conclusions be based on sufficient, relevant and competent evidence. When planning the IS audit, the IS auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability.

Audit evidence may include:

- The IS auditor's observations (presented to management)
- Notes taken from interviews
- Results of independent confirmations obtained by the IS auditor from different stakeholders
- Material extracted from correspondence and internal documentation or contracts with external partners
- The results of audit test procedures

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

Figure 1.9—Understand the Control Environment and Flow of Transactions


Review the system to identify controls.
Test compliance to determine whether controls are functioning.
Evaluate the controls to determine the basis for reliance and the nature, scope and timing of substantive tests.
Use two types of substantive tests to evaluate the validity of the data.
Test balances and transactions.
Perform analytic review procedures.

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 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 could 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, the IS auditor should always consider the qualifications and functional responsibilities of the persons providing the information. This can also be true of the 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**—The 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.

The IS auditor gathers a variety of evidence during the audit. Some evidence may be relevant to the objectives of the audit, while other evidence may be considered peripheral. The 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 by the IS auditor. These two characteristics are referred to by the International Federation of Accountants (IFAC) as competent (quality) and sufficient (quantity). Evidence is competent when it is both valid and relevant. Audit judgment is used to determine when sufficiency is achieved in the same manner that is used to determine the competency of evidence.

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

Gathering of evidence is a key step in the audit process. The IS auditor should be aware of the various forms of audit evidence and how evidence can be gathered and reviewed. The IS auditor should understand ISACA IS Audit and Assurance Standard 1205 Evidence and should obtain evidence of a nature and sufficiency to support audit findings.

Note: A CISA candidate, given an audit scenario, should be able to determine which type of evidence gathering technique would be best.

The following are techniques for gathering evidence:

- **Reviewing IS organization structures**—An organizational structure that provides an adequate separation or segregation of duties is a key general control in an IS environment. The IS auditor should understand general organizational controls and be able to evaluate these 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 than the classic IS organization, which consists of separate systems and operations functions. The IS auditor should be able to review these 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. The 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**—The 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 stored electronically. If the latter is the case, controls to preserve the document integrity should be evaluated by the IS auditor. The IS auditor should look for a minimum level of IS documentation. Documentation may include:
  - Systems development initiating documents (e.g., feasibility study)
  - 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**—Interviewing techniques are an important skill for the IS auditor. Interviews should be organized in advance with objectives clearly communicated, follow a fixed outline and be documented by interview notes. An interview form or checklist prepared by an IS auditor is a good approach. The IS auditor should always remember that the purpose of such an interview is to gather audit evidence. Procedures to gather audit evidence include inquiry, observation, inspection, confirmation, performance and monitoring. Personnel interviews are discovery in nature and should never be accusatory; the interviewer should help people feel comfortable, encouraging them to share information, ideas, concerns and knowledge. The IS auditor should verify the accuracy of the notes with the interviewee whether or not these notes would be necessary to support conclusions.
- **Observing processes and employee performance**—The observation of processes is a key audit technique for many types of review. The 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 at a later date. In some situations, the release of the audit report may not be timely enough to use this observation as evidence. This may necessitate the issuance of an interim report to management of the area being audited. The IS auditor may also 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.
- **Walk-throughs**—The walk-through is an audit technique to confirm the understanding of controls.

All of these techniques for gathering evidence are part of an audit, but an audit is not considered only review work. An audit includes examination, which incorporates by necessity the testing of controls and audit evidence, and therefore, includes the results of audit tests.

IS auditors 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 in an automated form rather than on paper. However, the IS auditor should look for documentation standards and practices within the IS organization.

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

1.5.12 INTERVIEWING AND OBSERVING PERSONNEL IN PERFORMANCE OF THEIR DUTIES

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

- **Actual functions**—Observation could 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 the 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 the IS auditor to gain evidence of compliance and observe deviations, if any. This type of observation could prove to be 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 company's assets and data. This type of information could be complemented with an examination of previous and planned security training.
- **Reporting relationships**—Reporting relationships should be observed to ensure that assigned responsibilities and adequate segregation of duties 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.

1.5.13 SAMPLING

Sampling is used 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.

Note: Increasing regulation of organizations has led to a major focus on the IS auditor's ability to verify the adequacy of internal controls through the use of sampling techniques. This has become necessary because many controls are transactional in nature, which can make it difficult to test the entire population. Although a candidate is not expected to become a sampling expert, it is important for the candidate to have a foundational understanding of the general principles of sampling and how to design a sample that is reliable.

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 the inference.
  - With statistical sampling, the 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 will be represented as a percentage. The results of a valid statistical sample are mathematically quantifiable.
- **Nonstatistical sampling (often referred to as judgmental sampling)**—Uses auditor 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.

When using either statistical or nonstatistical sampling methods, the IS auditor should design and select an audit sample; perform audit procedures; and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence. These methods of sampling require the IS auditor to use judgment when defining the population characteristics and, thus, are subject to the risk that the IS auditor will draw the wrong conclusion from the sample (sampling risk). However, statistical sampling permits the 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 by IS auditors—attribute sampling and variable sampling. Attribute sampling, generally applied in compliance testing situations, deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence. Variable sampling, generally applied in substantive testing situations, 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.

Attribute sampling refers to three different but related types of proportional sampling:
- **Attribute sampling (also referred to as fixed sample-size attribute sampling or frequency-estimating sampling)**—A sampling model that is used to estimate the rate (percent) of occurrence of a specific quality (attribute) in a population. Attribute sampling answers the question of "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 the IS auditor believes that relatively few errors will be found in a population.
- **Discovery sampling**—A sampling model that can be used when the expected occurrence rate is extremely low. Discovery sampling is most often used when the objective of the audit is to seek out (discover) fraud, circumvention of regulations or other irregularities.

Variable sampling—also known as 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 a number of different 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

To perform attribute or variable sampling, the following statistical sampling terms need to be understood:
- **Confidence coefficient (also referred to as 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 comfort. If the 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 the IS auditor, it represents 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 percent 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**—Computes the variance of the sample values from the mean of the sample. Sample standard deviation measures 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.

Key steps in the construction and selection of a sample for an audit test are seen in **figure 1.10**.

It is important to know that tools exist to analyze all of the data, not just those available through CAATs.

Note: The IS auditor should be familiar with the different types of sampling techniques and when it is appropriate to use each of them.

1.5.14 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. External experts could include experts in specific technologies such as networking, automated teller machines, wireless, systems integration and digital forensics or subject matter experts such as specialists in a particular industry or area of specialization such as banking, securities trading, insurance, legal experts, etc.

When a part or all of IS audit services are proposed to be outsourced to another audit or external service provider, the following should be considered with regard to using the services of other auditors and experts:

- 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 of work proposed to be outsourced and approach
- 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 following may also require special consideration:

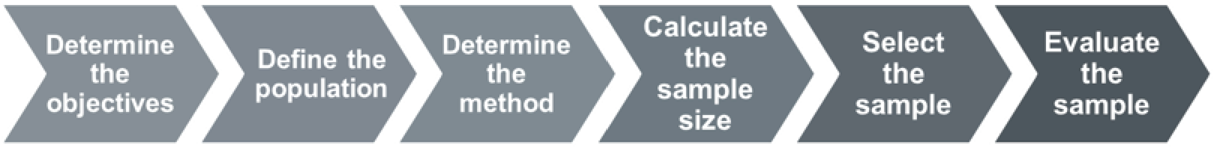
- Testimonials/references and background checks
- Access to systems, premises and records
- Confidentiality restrictions to protect customer-related information
- Use of CAATs and other tools to be used by the external audit service provider
- Standards and methodologies for performance of work and documentation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

The IS auditor or entity outsourcing the auditing services should monitor the relationship to ensure the objectivity and independence throughout the duration of the arrangement.

It is important to understand that although a part of 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.
- Put in place 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

Figure 1.10—Steps in the Selection of a Sample for an Audit Test



Source: ISACA, *Fundamentals of IS Audit and Assurance Training Course*, USA, 2014

to confirm the work was appropriately planned, supervised, documented and reviewed and to consider the appropriateness and sufficiency of the audit evidence provided. Another example is 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 met, that any significant assumptions used by other IS auditors or experts have been identified, and the findings and conclusions reported have been agreed on by management.
- Assess the usefulness and appropriateness of reports of such external providers, and assess the impact of significant findings on the overall audit objectives.

Note: The IS auditor should be familiar with ISACA Audit and Assurance Standard 1203 Performance and Supervision and the IS Audit and Assurance Guideline 2206 Using the Work of Other Experts focusing on the rights of access to the work of other experts.

1.5.15 COMPUTER-ASSISTED AUDIT TECHNIQUES

During the course of an audit, the IS auditor is to obtain sufficient, relevant and useful evidence to effectively achieve the audit objectives. The audit findings and conclusions should be supported by appropriate analysis and interpretation of the evidence. Current information processing environments pose a significant challenge to the IS auditor to collect sufficient, relevant and useful evidence because the evidence may only exist in electronic form.

CAATs are important tools for the IS auditor in gathering information from these environments. When systems have different hardware and software environments, data structures, record formats or processing functions, it is almost impossible for the auditors to collect certain evidence without a software tool to collect and analyze the records.

CAATs also enable IS auditors to gather information independently. CAATs 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 generalized audit software (GAS), utility software, debugging and scanning software, test data, application software tracing and mapping, and expert systems.

GAS refers to standard software that has the capability to directly read and access data from various database platforms, flat-file systems and ASCII formats. GAS provides IS auditors 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. The following functions are commonly supported by GAS:
- **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

The effective and efficient use of software requires an understanding of its capabilities and limitations.

Utility software is a subset of software—such as report generators of the database management system—that provides evidence to auditors about system control effectiveness. Test data involve the auditors 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 in the system. The audit-expert system will give 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 the senior auditors or managers.

These tools and techniques can be used in performing various audit procedures:
- 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

The IS auditor should have a thorough understanding of CAATs and know where and when to apply them. Please see ISACA Audit and Assurance Standard 2207 Irregularity and Illegal Acts, sections 2.2.4 and 2.5.3. Professionals 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 CAATs before going through the effort, time and expense of purchasing or developing them. Issues to consider include:
- Ease of use, both for existing and future audit staff
- Training requirements
- Complexity of coding and maintenance
- Flexibility of uses
- Installation requirements
- Processing efficiencies (especially with a PC CAAT)
- Effort required to bring the source data into the CAATs for analysis
- Ensuring the integrity of imported data by safeguarding their 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
- 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, the IS auditor should request read-only access. Any data manipulation by the IS auditor should be applied to copies of production files in a controlled environment to ensure that production data are not exposed to unauthorized updating. Most of the CAATs provide for downloading production data from production systems to a stand-alone platform and then conducting analysis from the standalone platform, thereby insulating the production systems from any adverse impact.

CAATs as a Continuous Online Audit Approach

An increasingly important advantage of CAATs is the ability to improve audit efficiency through continuous online auditing techniques. To this end, IS auditors must develop audit techniques that are appropriate for use with advanced computerized systems. In addition, they 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 their organization's automated environment. This takes the form of the continuous audit approach. (For more detailed information on continuous online auditing, see chapter 3 Information Systems Acquisition, Development and Implementation.)

1.5.16 EVALUATION OF THE CONTROL ENVIORNMENT

The IS auditor will review evidence gathered during the audit to determine if the operations reviewed are well controlled and effective. This is also an area that requires the IS auditor's judgment and experience. The IS auditor should assess the strengths and weaknesses of the controls evaluated and then determine if they are effective in meeting the control objectives established as part of the audit planning process.

A control matrix is often utilized in assessing the proper level of controls. Known types of errors that can occur in the area under review are placed on the top axis and known controls to detect or correct errors are placed on the side axis. Then, using a ranking method, the matrix is filled with the appropriate measurements. When completed, the matrix will illustrate areas where controls are weak or lacking.

In some instances, one strong control may compensate for a weak control in another area. For example, if the IS auditor finds weaknesses in a system's transaction error report, the IS auditor may find that a detailed manual balancing process over all transactions compensates for the weaknesses in the error report. The IS auditor should be aware of compensating controls in areas where controls have been identified as weak.

While a compensating control situation occurs when one stronger control supports a weaker one, overlapping controls are two strong controls. For example, if a data center employs a card key system to control physical access and a guard inside the door requires employees to show their card key or badge, an overlapping control exists. Either control might be adequate to restrict access, but the two complement each other.

Normally, a control objective will not be achieved by considering one control adequate. Rather, the IS auditor will perform a variety of testing procedures and evaluate how these relate to one another. Generally a group of controls, when aggregated together, may act as compensating controls, and thereby minimize the risk. An IS auditor should always review for compensating controls prior to reporting a control weakness.

The IS auditor may not find each control procedure to be in place but should evaluate the comprehensiveness of controls by considering the strengths and weaknesses of control procedures.

Judging the Materiality of Findings

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 the finding if corrective action is not taken. A weakness in computer security physical access controls at a remote distributed computer site may be significant to management at the site but will 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.

The IS auditor must use judgment when deciding which findings to present to various levels of management. For example, the IS auditor may find that the transmittal form for delivering tapes to the offsite storage location is not properly initialed or authorization evidenced by management as required by procedures. If the IS auditor finds that management otherwise pays attention to this process and that there have been no problems in this area, the IS auditor may decide that the failure to initial transmittal documents is not material enough to bring to the attention of upper management. The IS auditor might decide to discuss this only with local operations management. However, there may be other control problems that will cause the IS auditor to conclude that this is a material error because it may lead to a larger control problem in other areas. The IS auditor should always judge which findings are material to various levels of management and report them accordingly.

1.6 COMMUNICATING AUDIT RESULTS

The exit interview, conducted at the end of the audit, provides the IS auditor with the opportunity to discuss findings and recommendations with management. During the exit interview, the IS auditor should:
- Ensure that the facts presented in the report are correct
- 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

The IS auditor will frequently be asked to present the results of audit work to various levels of management. The IS auditor should have a thorough understanding of the presentation techniques necessary to communicate these results.

Presentation techniques could include the following:

- **Executive summary**—An easy-to-read, concise report that presents findings to management in an understandable manner. Findings and recommendations should be communicated from a business perspective. Detailed attachments can be more technical in nature because operations management will require the detail to correct the reported situations.
- **Visual presentation**—May include slides or computer graphics

IS auditors should be aware that ultimately they are responsible to senior management and the audit committee of the board of directors. IS auditors should feel free to communicate issues or concerns to such management. 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, the IS auditor should discuss the findings with the management staff of the audited entity. The goal of such a discussion would be to gain agreement on the findings and develop a course of corrective action. In cases where there is disagreement, the IS auditor should elaborate on the significance of the findings, risk and effects of not correcting the control weakness. Sometimes the auditee's management may request assistance from the IS auditor in implementing the recommended control enhancements. The IS auditor should communicate the difference between the IS auditor's role and that of a consultant and give careful consideration to how assisting the auditee may adversely affect the IS auditor's independence.

After agreement has been reached with the auditee, IS audit management should brief senior management of the audited organization. A summary of audit activities will 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 the auditors with an independent route to report sensitive findings.

1.6.1 AUDIT REPORT STRUCTURE AND CONTENTS

Audit reports are the end product of the IS audit work. They are used by the IS auditor to report findings and recommendations to management. The exact format of an audit report will vary by organization; however, the skilled 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.

There is no specific format for an IS audit report; the organization's audit policies and procedures will dictate the general format. Audit reports will usually have the following structure and content:

- An introduction to the report, including a statement of audit objectives, limitations to the audit and scope, the period of audit coverage, and a general statement on the nature and extent of audit procedures conducted and processes examined during the audit, followed by a statement on the IS audit methodology and guidelines
- Audit findings included in separate sections and often grouped in sections by materiality and/or intended recipient
- The IS auditor's overall conclusion and opinion on the adequacy of controls and procedures examined during the audit, and the actual potential risk identified as a consequence of detected deficiencies
- The IS auditor's reservations or qualifications with respect to the audit
  - This 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
  - The IS auditor decides whether to include specific findings in an audit report. This should be based on the materiality of the findings and the intended recipient of the audit report. An audit report directed to the audit committee of the board of directors, for example, may not include findings that are important only to local management but have little control significance to the overall organization. The decision of what to include in various levels of audit reports depends on the guidance provided by upper management.
- A variety of findings, some of which may be quite material while others are minor in nature
  - The auditor may choose to present minor findings to management in an alternate format such as by memorandum.

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

Auditee management evaluates the findings, stating corrective actions to be taken and timing for implementing these anticipated corrective actions.

Management may not be able to implement all audit recommendations immediately. For example, the IS auditor may recommend changes to an information system that is also undergoing other changes or enhancements. The IS auditor should not necessarily expect that the other changes will be suspended until the IS auditor's recommendations are implemented. Rather, all may be implemented at once.

The IS auditor should discuss the recommendations and any planned implementation dates while in the process of releasing the audit report. The IS auditor must realize that various constraints—such as staff limitations, budgets or other projects—may limit immediate implementation. Management should develop a firm program for corrective actions. It is important to obtain a commitment from the auditee/management on the date by which the action plan will be implemented (the solution can be something which takes a long time for implementation) and the manner in which it will be performed because the corrective action may bring risk that may be avoided if identified while discussing and finalizing the audit report. If appropriate, the IS auditor may want to report to upper management on the progress of implementing recommendations.

ISACA IS Audit and Assurance Standard 1401 Reporting and the ISACA IS Audit and Assurance Guideline 2401 Reporting state that the report should include all significant audit findings. When a finding requires explanation, the IS auditor should describe the finding, its cause and risk. When appropriate, the IS auditor should provide the explanation in a separate document and make reference to it in the report. For example, this approach may be appropriate for highly confidential matters. The IS auditor should also identify the organizational, professional and governmental criteria applied, such as COBIT. The report should be issued in a timely manner to encourage prompt corrective action. When appropriate, the IS auditor should promptly communicate significant findings to the appropriate persons prior to the issuance of the report. Prior communication of significant findings should not alter the intent or content of the report.

Note: The CISA candidate should review the detail from the ISACA IS Audit and Assurance Guideline 2401 Reporting.

1.6.2 AUDIT DOCUMENTATION

Audit documentation should include, at a minimum, a record of the following:
- 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 auditing entity and should be accessible only to authorized personnel under specific or general permission. Where access to audit documentation is requested by external parties, the auditor should obtain appropriate prior approval of senior management and legal counsel.

The IS auditor/IS audit department should also develop policies regarding custody, retention requirements and release of audit documentation.

Note: The CISA candidate should be familiar with the detailed content of the ISACA IS Audit and Assurance Guideline 2203 Performance and Supervision.

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

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.

Audit documentation should support the findings and conclusions/opinion. Time of evidence can be crucial to supporting audit findings and conclusions. The IS auditor should take enough care to ensure that the evidence gathered and documented will be able to support audit findings and conclusions. An IS auditor should be able to prepare adequate working papers, narratives, questionnaires and understandable system flowcharts.

IS auditors are a scarce and expensive resource. Any technology capable of increasing the audit productivity is welcome. Automating work papers affects productivity directly and indirectly (granting access to other auditors, reusing documents or parts of them in recurring audits, etc.).

The quest for integrating work papers in the auditor's e-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.

ISACA IS Audit and Assurance Standards and Guidelines set forth many specifications about work papers, including the need to document the audit plan, program and evidence (2205 Evidence); how to use those of other auditors (2206 Using the Work of Other Experts); or the use of sampling (2208 Sampling).

1.6.3 CLOSING FINDINGS

IS auditors should realize that auditing is an ongoing process. The 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 agreed to by the audited entity.

The timing of the follow-up will depend on the criticality of the findings and would be subject to the IS auditor's judgment. The results of the follow-up should be communicated to appropriate levels of management.

The level of the IS auditor's follow-up review will depend on several factors. In some instances, the IS auditor may merely need to inquire as to the current status. In other instances, the 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.

1.7 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 they conduct periodic, proactive reviews of controls. It is a methodology used to review key business objectives, risk involved in achieving the business objectives and internal controls designed to manage business risk in a formal, documented and collaborative process.

In practice, CSA is a series of tools on a continuum of sophistication ranging from simple questionnaires to facilitated workshops, designed to gather information about the organization by asking those with a day-to-day working knowledge of an area as well as their managers. The basic tools used during a CSA project are the same whether the project is technical, financial or operational. These tools include management meetings, client workshops, worksheets, rating sheets and the CSA project approach. Like the continuum of tools used to gather information, there are diverse approaches to the levels below management that are queried; some organizations even include outsiders (such as clients or trading partners) when making CSA assessments.

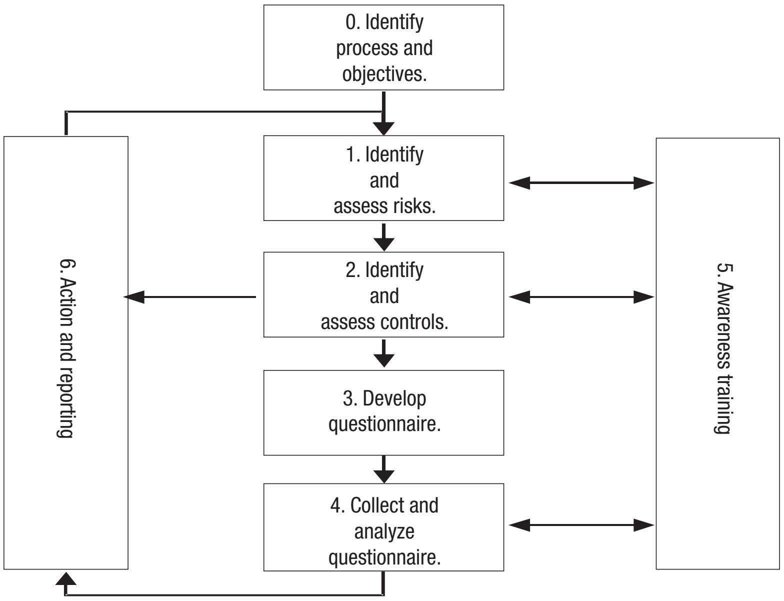
The CSA program can be implemented by various methods. For small business units within organizations, it can be implemented by facilitated workshops where functional management and control professionals such as auditors can come together and deliberate how best to evolve a control structure for the business 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, a facilitator may also offer his/her own expertise in addition to facilitating the exchange of ideas and experience. A facilitator does not have to be an expert in a certain process or subject matter; however, the facilitator should have basic skills such as:

- Active listening skills and the ability to ask good questions, including questions that probe the topics and move the discussions forward
- Good verbal communication skills, including the ability to pose questions in a nonthreatening manner and the ability to summarize material
- The ability to manage the dynamics of the group, including managing various personalities so that a few members do not dominate the discussions and managing processes so that goals are met
- The ability to resolve conflicts
- The ability to manage time and keep the proceedings on schedule

In organizations with offices located at geographically dispersed locations, it may not be practical to organize facilitated workshops. In this case, a hybrid approach is needed. A questionnaire based on the control structure can be used. Operational managers can periodically complete the questionnaire, which can be analyzed and evaluated for effectiveness of the controls. However, a hybrid approach will be effective only if the analysis and readjustment of the questionnaire is performed using a life cycle approach, as shown in **figure 1.11**.

Figure 1.11—Hybrid Approach for a CSA


0. Identify process and objectives.
1. Identify and assess risks.
2. Identify and assess controls.
3. Develop questionnaire.
4. Collect and analyze questionnaire.
5. Awareness training
6. Action and reporting

1.7.1 OBJECTIVES OF CSA

There are several objectives associated with adopting a CSA program. The primary objective 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 also should be responsible for monitoring the controls. CSA programs also must educate management about control design and monitoring, particularly concentration on areas of high risk. These programs are not just policies requiring clients to comply with control standards. Instead, they offer a variety of support ranging from written suggestions outlining acceptable control environments to in-depth workshops. When workshops are included in the program, an additional objective—the empowerment of workers to assess or even design the control environment—may be included in the program.

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 to conduct a meeting with the business unit representatives (including appropriate and relevant staff and management) to identify the business unit's primary objective—to determine the reliability of the internal control system. In addition, actions that increase the likelihood of achieving the primary objective should be identified.

A generic set of goals and metrics for each process, which can be used in designing and monitoring the CSA program, has been provided in COBIT.

COBIT is a governance and control framework that provides guidance in the development of the control assessment method. One could develop a CSA method by identifying the tasks and processes that are relevant to the business environment and then defining the controls for relevant activities. A CSA questionnaire can be developed using the statements in the relevant control objectives of the identified IT processes. Various components of the COBIT framework—such as input-output matrix, RACI chart, goals, metrics and maturity model—can be converted into the form of a CSA questionnaire to assess each of the areas as required.

1.7.2 BENEFITS OF CSA

Some of the benefits of a CSA include the following:
- Early detection of risk
- More effective and improved internal controls
- Creation of cohesive teams through employee involvement
- Developing a sense of ownership of the controls in the employees and process owners and reducing their resistance to control improvement initiatives
- Increased employee awareness of organizational objectives, and knowledge of risk and internal controls
- Increased communication between operational and top management
- Highly motivated 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 as required by the various regulatory agencies and laws such as the US Sarbanes-Oxley Act

1.7.3 DISADVANTAGES OF CSA

CSA contains several 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 motivation may limit effectiveness in the detection of weak controls

1.7.4 AUDITOR ROLE IN CSA

The auditor's role in CSAs should be considered enhanced when audit departments establish a CSA program. When these programs are established, auditors become internal control professionals and assessment facilitators. Their value in this role is evident when management takes responsibility and ownership for internal control systems under their authority through process improvements in their control structures, including an active monitoring component.

For an auditor to be effective in this facilitative and innovative role, the auditor must understand the business process being assessed. This can be attained via traditional audit tools such as a preliminary survey or walk-through. Also, the auditors must remember that they are the facilitators and the management client is the participant in the CSA process. For example, during a CSA workshop, instead of the auditor performing detailed audit procedures, the auditor will lead and guide the auditees in assessing their environment by providing insight about 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 auditor is better positioned to explain the risk associated with such changes.

1.7.5 TECHNOLOGY DRIVERS FOR CSA

The development of techniques for empowerment, information gathering and decision making is a necessary part of a CSA program implementation. Some of the technology drivers include the combination of hardware and software to support CSA selection, and the use of an electronic meeting system and computer-supported decision aids to facilitate group decision making. Group decision making is an essential component of a workshop-based CSA where employee empowerment is a goal. In case of a questionnaire approach, the same principle applies for the analysis and readjustment of the questionnaire.

1.7.6 TRADITIONAL VERSUS CSA APPROACH

The traditional approach can be summarized as any approach in which the primary responsibility for analyzing and reporting on internal control and risk is assigned to auditors, and to a lesser extent, controller departments and outside consultants. This approach has created and reinforced the notion that auditors and consultants, not management and work teams, are responsible for assessing and reporting on internal control. The CSA approach, on the other hand, emphasizes management and accountability over developing and monitoring internal controls of an organization's sensitive and critical business processes.

A summary of attributes or focus that distinguishes each from the other is described in **figure 1.12**.

Figure 1.12—Traditional and CSA Attributes

Traditional	CSA
Assigns duties/supervises staff	Empowered/accountable employees
Policy/rule-driven	Continuous improvement/learning curve
Limited employee participation	Extensive employee participation and training
Narrow stakeholder focus	Broad stakeholder focus
Auditors and other specialists	Staff at all levels, in all functions, are the primary control analysts.

1.8 THE EVOLVING IS AUDIT PROCESS

The IS audit process must continually change to keep pace with innovations in technology. Topics to address these evolving changes include areas such as integrated auditing and continuous auditing.

1.8.1 INTEGRATED AUDITING

Dependence of business processes on information technology has necessitated that traditional financial and operational auditors develop an understanding of IT control structures and IS auditors develop an understanding of the business control structures. 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.

The integrated approach focuses 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 IT audit is typically to understand and identify risk under topical areas such as information management, IT infrastructure, IT governance and IT operations. Other audit specialists will seek to understand the organizational environment, business risk and business controls. A key element of the integrated approach is discussion of the risk arising among the whole audit team, with consideration of impact and likelihood.

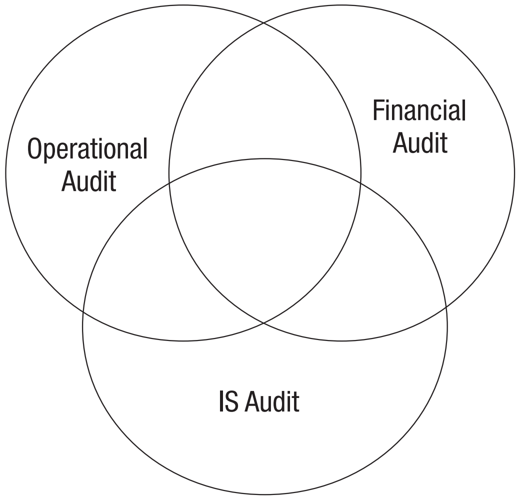
Detailed audit work then focuses on the relevant controls in place to manage this risk. IT systems frequently provide a first line of preventive and detective controls, and the integrated audit approach depends on a sound assessment of their efficiency and effectiveness.

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 that key controls are supported by the IT system
- Testing that management controls operate effectively
- A combined report or opinion on control risk, design and weaknesses

The integrated audit demands a focus on business risk and a drive for creative control solutions. It is a team effort of auditors 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 greater variety and the ability to see how all of the elements (functional and IT) mesh together to form the complete picture. See **figure 1.13** for an integrated auditing approach.

Figure 1.13—An Integrated Audit



The integrated audit concept has also radically changed the manner in which audits are looked on by the different stakeholders. Employees or process owners better understand the objectives of an audit because they are able to 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. Shareholders are able to 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 led to greater impetus for the growing popularity of integrated audits.

Note: This topic on integrated auditing, though important, is not specifically tested in the CISA exam.

1.8.2 CONTINUOUS AUDITING

The focus on increased effectiveness and efficiency of assurance, internal auditing and control has spurred the development of new studies and examination of new ideas concerning continuous auditing as opposed to more traditional periodic auditing reviews. Several research studies and documents addressing the subject carry different definitions of continuous auditing. All studies, however, recognize that a distinctive character of continuous auditing is the short time lapse between the facts to be audited, the collection of evidence and audit reporting.

Traditional financial reports and the traditional audit style sometimes prove to be insufficient because they lack the essential element in the current business environment—updated information. Therefore, continuous auditing appears to be gaining more and more followers.

Some of the drivers of continuous auditing are a better monitoring of financial issues within a company, ensuring that real-time transactions also benefit from real-time monitoring; prevention of financial fraud and audit scandals such as Enron and Tesco Plc; and the use of software to determine that financial controls are proper. Continuous auditing involves a large amount of work because the company practicing continuous auditing will not provide one report at the end of a quarter, but will provide financial reports on a more frequent basis. Audit functions in organizations that use ERP platforms are increasingly using automated governance, risk and compliance (GRC) tools, which flag transactions that meet predefined criteria on a real-time basis. These tools are set up at the database level and pull data that meet the predefined criteria. Such data may include purchase invoices that have the same or similar address as that of an employee. The advantage of using these tools is that voluminous data are analyzed at a high speed to highlight relevant patterns of data that may be of interest to the auditors.

Continuous auditing is not a recent development. Traditional application systems may contain embedded audit modules. These would allow an auditor to trap predefined types of events or to directly inspect abnormal or suspect conditions and transactions.

Most current commercial applications could be customized with such features. However, cost and other considerations and the technical skills that would be required to establish and operate these tools tend to limit the usage of embedded audit modules to specific fields and applications.

To properly understand the implications and requirements of continuous auditing, a clear distinction has to be made between continuous auditing and continuous monitoring:

- **Continuous monitoring**—This is provided by IS management tools and typically based on automated procedures to meet fiduciary responsibilities. For instance, real-time antivirus or intrusion detection systems (IDSs) may operate in a continuous monitoring fashion.
- **Continuous auditing**— According to the *Global Technology Audit Guide 3: Continuous Auditing: Implications for Assurance Monitoring and Risk Assessment*, continuous auditing is "a method to automatically perform control and risk assessments on a more frequent basis. Continuous auditing changes the audit paradigm from periodic reviews of a sample of transactions to ongoing audit testing of 100 percent of transactions. It becomes an integral part of modern auditing at many levels." Continuous IS (and non-IS) auditing is typically completed using automated audit procedures.

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 auditors. 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 artificial intelligence (AI) tools. Continuous auditing attempts to facilitate the collection and analysis of 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 of 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.

Prerequisites/preconditions for continuous auditing to succeed include:

- A high degree of automation
- An automated and highly reliable process in producing information about subject matter soon after or during the occurrence of events underlying the subject matter
- Alarm triggers to report timely control failures
- Implementation of highly automated audit tools that require the IS auditor to be involved in setting up the parameters
- Quickly informing IS auditors of the results of automated procedures, particularly when the process has identified anomalies or errors
- The quick and timely issuance of automated audit reports
- Technically proficient IS auditors
- Availability of reliable sources of evidence
- Adherence to materiality guidelines
- A change of mind-set required for IS auditors to embrace continuous reporting
- Evaluation of cost factors

Simpler continuous auditing and monitoring tools are already built into many ERP 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 difficult but significant added value to using these features is that they postulate a definition of what would be a "dangerous" or exception condition. For instance, whether a set of granted IS access permissions is to be deemed risk-free will depend on having well-defined rules of segregation of duties. 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 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 (CAAT)
- Database management system (DBMS)
- Data warehouses, data marts, data mining
- Intelligent agents
- Embedded audit modules (EAM)
- Neural network technology
- 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 (sometimes referred to as bots), allows for continuous monitoring of systems settings and the delivery of alert messages when certain thresholds are exceeded or when 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 to 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 resistant 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 the accuracy of the report.

The implementation of continuous auditing involves many factors; however, the task is not impossible. There is an increasing desire to provide auditing over information in a real-time environment (or as close to real time as possible).

1.9 CASE STUDIES

The following case studies are included as a learning tool to reinforce the concepts introduced in this chapter.

1.9.1 CASE STUDY A

The IS auditor has been asked to perform preliminary work that will assess the readiness of the organization for a review to measure compliance with new regulatory requirements. These requirements are designed to ensure that management is taking an active role in setting up and maintaining a well-controlled environment, and accordingly, will assess management's review and testing of the general IT control environment. Areas to be assessed include logical and physical security, change management, production control and network management, IT governance, and end-user computing. The IS auditor has been given six months to perform this preliminary work, so sufficient time should be available. It should be noted that in previous years, repeated problems have been identified in the areas of logical security and change management, so these areas will most likely require some degree of remediation. Logical security deficiencies noted 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. In anticipation of the work to be performed by the IS auditor, the chief information officer (CIO) requested direct reports to develop narratives and process flows describing the major activities for which IT is responsible. These were completed, approved by the various process owners and the CIO, and then forwarded to the IS auditor for examination.

CASE STUDY A QUESTIONS	
A1.	What should the IS auditor do **FIRST**? A. Perform an IT risk assessment. B. Perform a survey audit of logical access controls. C. Revise the audit plan to focus on risk-based auditing. D. Begin testing controls that the IS auditor feels are most critical.
A2.	When testing program change management, 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.
See answers and explanations to the case study questions at the end of the chapter (page 65).	

1.9.2 CASE STUDY B

An IS auditor is planning to review the security of a financial application for a large company with several locations worldwide. The application system is made up of a web interface, a business logic layer and a database layer. The application is accessed locally through a LAN and remotely through the Internet via a virtual private network (VPN) connection.

CASE STUDY B QUESTIONS	
B1.	The **MOST** appropriate type of CAATs tool the auditor should use to test security configuration settings for the entire application system is: A. generalized audit software (GAS). B. test data. C. utility software. D. expert system.
B2.	Given that the application is accessed through the Internet, how should the auditor determine whether to perform a detailed review of the firewall rules and VPN configuration settings? A. Documented risk analysis B. Availability of technical expertise C. Approach used in previous audit D. IS auditing guidelines and best practices
B3.	During the review, if the auditor detects that the transaction authorization control objective cannot be met due to a lack of clearly defined roles and privileges in the application, the auditor should **FIRST**: A. review the authorization on a sample of transactions. B. immediately report this finding to upper management. C. request that auditee management review the appropriateness of access rights for all users. D. use GAS to check the integrity of the database.
See answers and explanations to the case study questions at the end of the chapter (page 66).	

1.9.3 CASE STUDY C

An IS auditor has been appointed to carry out IS audits in an entity for a period of two years. After accepting the appointment the IS auditor noted that:

- The entity has an audit charter that detailed, among other things, the scope and responsibilities of the IS audit function and specifies the audit committee as the overseeing body for audit activity.
- The entity is planning a major increase in IT investment, mainly on account of implementation of a new ERP application, integrating business processes across units dispersed geographically. The ERP implementation is expected to become operational within the next 90 days. The servers supporting the business applications are hosted offsite by a third-party service provider.
- The entity has a new incumbent as chief information security officer (CISO) who reports to the chief financial officer (CFO).
- 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. However, the entity has seen increased employee turnover as well.

CASE STUDY C QUESTIONS	
C1.	The **FIRST** priority of the IS auditor in year one should be to study the: A. previous IS audit reports and plan the audit schedule. B. audit charter and plan the audit schedule. C. impact of the new incumbent as CISO. D. impact of the implementation of a new ERP on the IT environment and plan the audit schedule.
C2.	How should the IS auditor evaluate backup and batch processing within computer operations? A. Plan and carry out an independent review of computer operations. B. Rely on the service auditor's report of the service provider. C. Study the contract between the entity and the service provider. D. Compare the service delivery report to the service level agreement.
See answers and explanations to the case study questions at the end of the chapter (page 66).	

1.10 ANSWERS TO CASE STUDY QUESTIONS

ANSWERS TO CASE STUDY A QUESTIONS

A1. **A** An IT risk assessment should be performed first to ascertain which areas present the greatest risk and what controls mitigate that risk. Although narratives and process flows have been created, the organization has not yet assessed which controls are critical. All other choices would be undertaken after performing the IT risk assessment.

A2. **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 was accompanied by appropriate control documentation. Accordingly, changes to production code provide the most appropriate basis for selecting a sample. These sampled changes should then be traced to appropriate authorizing documentation. In contrast, selecting from the population of change management documents will not reveal any changes that bypassed the normal approval and documentation process. Similarly, comparing production code changes to system-produced logs will not provide evidence of proper approval of changes prior to their being migrated to production.

ANSWERS TO CASE STUDY B QUESTIONS

B1. **C** When testing the security of the entire application system—including OSs, database and application security—the auditor will most likely use a utility software that assists in reviewing the configuration settings. In contrast, the auditor might use GAS to perform a substantive testing of data and configuration files of the application. Test data are normally used to check the integrity of the data and expert systems are used to inquire on specific topics.

B2. **A** In order to decide if the audit scope should include specific infrastructure components (in this case, the firewall rules and VPN configuration settings), the auditor should perform and document a risk analysis in order to determine which sections present the greatest risk and include these sections in the audit scope. The risk analysis may consider factors such as previous revisions to the system, related security incidents within the company or other companies of the same sectors, resources available to do the review and others. Availability of technical expertise and the approach used in previous audits may be taken into consideration; however, these should be of secondary importance. IS auditing guidelines and best practices provide a guide to the auditor on how to comply with IS audit standards, but by themselves they would not be sufficient to make this decision.

B3. **A** The auditor should first review the authorization on a sample of transactions in order to determine and be able to report the impact and materiality of this issue. Whether the auditor would immediately report the issue or wait until the end of the audit to report this finding will depend on the impact and materiality of the issue, which would require reviewing a sample of transactions. The use of GAS to check the integrity of the database would not help the auditor assess the impact of this issue.

ANSWERS TO CASE STUDY C QUESTIONS

C1. **D** In terms of priority, because the implementation of the new ERP will have far reaching consequences on the way IS controls are configured in the system, the IS auditor should study the impact of implementation of the ERP and plan the audit schedule accordingly. Preferably, the IS auditor should discuss the audit plan with the external auditor and the internal audit division of the entity to make the audit more effective and useful for the entity.

C2. **D** The service delivery report that captures the actual performance of the service provider against the contractually agreed-on levels provides the best and most objective basis for evaluation of the computer operations. The service auditor's report is likely to be more useful from a controls evaluation perspective for the external auditor of the entity.