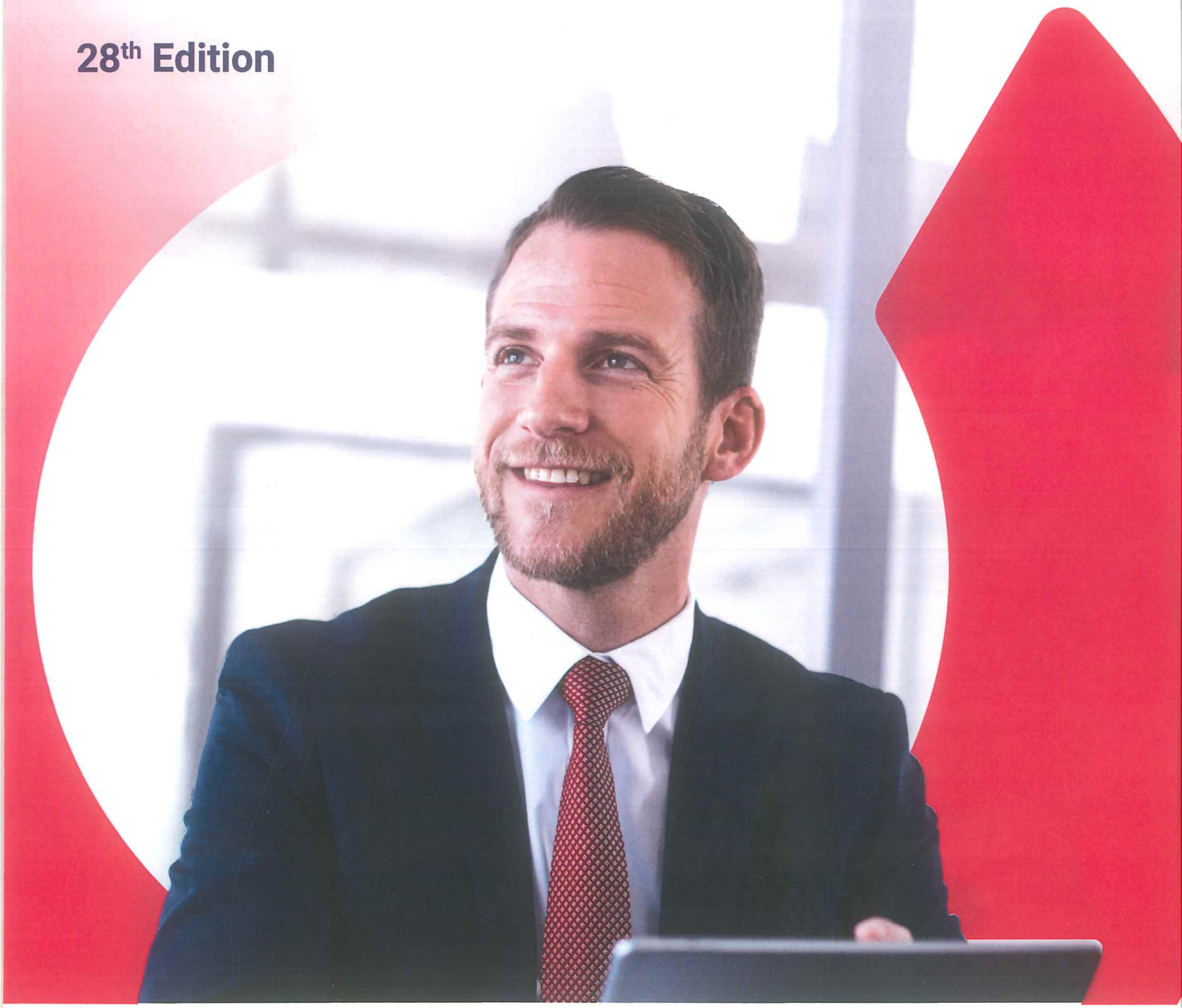
CISA® Official Review Manual

28th Edition



CISA Certified Information Systems Auditor.
An ISACA® Certification

ISACA®

Purpose of the CISA Official Review Manual 28th Edition

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

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

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

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

Page intentionally left blank

Acknowledgments

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

Authors

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

Expert Reviewers

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

New—CISA Job Practice

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

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

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

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

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

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

TABLE OF CONTENTS

Chapter 1

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

Chapter 2

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

Chapter 3

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

Chapter 4

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

Chapter 5

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

TABLE OF CONTENTS *(cont.)*

Appendix A

Appendix B

Glossary

Acronyms

About This Manual

Overview

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

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

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

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

Note

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

Format of This Manual

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

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

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

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

Preparing for the CISA Exam

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

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

Getting Started

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

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

Using the CISA Official Review Manual

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

Features in the Review Manual

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

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

Types of Questions on the CISA Exam

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

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

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

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

A helpful approach to these questions includes the following:

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

Preparing for the Exam

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

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

Using ISACA Exam Preparation Resources

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

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

About the CISA Official Questions, Answers & Explanations Database

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

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

Note

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

Page intentionally left blank

Chapter 1

Information System Auditing Process

Overview

Part A: Planning

Part B: Execution

Case Study

Overview

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

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

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

Domain 1 Exam Content Outline

Part A: Planning

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

Part B: Execution

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

Learning Objectives/Task Statements

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

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

Suggested Resources for Further Study

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

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

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

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

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

Self-Assessment Questions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Answers on page 28

Page intentionally left blank

Chapter 1 Answer Key

Self-Assessment Questions

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

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

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

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

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

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

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

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

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

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

Page intentionally left blank

Part A: Planning

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

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

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

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

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

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

Figure 1.1—Typical Audit Process Phases

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

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

Note

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

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

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

1.1.1 ISACA IS Audit and Assurance Standards

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

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

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

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

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

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

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

1.1.2 ISACA IS Audit and Assurance Guidelines

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

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

Note

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

1.1.3 ISACA Code of Professional Ethics

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

ISACA members and certification holders shall:

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

Note

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

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

1.1.4 ITAF TM

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

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

Note

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

1.1.5 IS Internal Audit Function

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

Audit Charter

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

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

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

Note

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

Management of the IS Audit Function

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

Note

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

IS Audit Resource Management

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

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

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

Note

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

Using the Services of Other Auditors and Experts

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

Note

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

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

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

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

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

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

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

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

1.2 Types of Audits, Assessments and Reviews

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

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

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

Some examples of audits, assessment and reviews include:

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

