ExamLabs

Certified Information Systems Auditor

Study Guide

Exam CISA

CONTENTS AT A GLANCE

CONTENTS

    - Asset Inventory and Classification
    - Access Controls
    - Privacy
    - Third-Party Management
    - Human Resources Security
    - Computer Crime
    - Security Incident Management
    - Forensic Investigations
- Logical Access Controls
    - Access Control Concepts
    - Access Control Models
    - Access Control Threats
    - Access Control Vulnerabilities
    - Access Points and Methods of Entry
    - Identification, Authentication, and Authorization
    - Protecting Stored Information
    - Managing User Access
    - Protecting Mobile Computing
- Network Security Controls
    - Network Security
    - Securing Client-Server Applications
    - Securing Wireless Networks
    - Protecting Internet Communications
    - Encryption
    - Voice over IP
    - Private Branch Exchange (PBX)
    - Malware
    - Information Leakage
- Environmental Controls
    - Environmental Threats and Vulnerabilities
    - Environmental Controls and Countermeasures
- Physical Security Controls
    - Physical Access Threats and Vulnerabilities
    - Physical Access Controls and Countermeasures

Appendix B Popular Methodologies, Frameworks, and Guidance

Figure Credits

Figure 4-6 courtesy of Digital Aardvark, Inc.

Figure 4-7 courtesy of AXELOS Limited. Copyright © AXELOS Limited 2016. PRINCE2® is a registered trade mark of AXELOS Limited. Used under permission of AXELOS Limited. All rights reserved.

Figure 4-9 courtesy of Oxford University Press, Inc. From Alexander et al., *The Oregon Experiment*, 1975, p. 44. Used by Permission of Oxford University Press, Inc.

Figure 5-2 courtesy of Fir0002/Flagstaffotos with permission granted under the terms of the GNU Free Documentation License, Version 1.2, http://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_L

Figure 5-3 courtesy of Sassospicco with permission granted under the terms of the Creative Commons Attribution Share-Alike 2.5 License, http://creativecommons.org/licenses/by-sa/2.5/.

Figure 5-4, courtesy of Robert Jacek Tomczak, has been released into the public domain by its author at the Polish Wikipedia project.

Figure 5-5 courtesy of Robert Kloosterhuis with permission granted under the terms of the Creative Commons Attribution Share-Alike 2.5 License, http://creativecommons.org/licenses/by-sa/2.5/.

Figure 5-15 courtesy of Rebecca Steele.

Figure 5-16 courtesy of Harout S. Hhedeshian with permission granted under the terms of the Creative Commons Attribution 3.0 Unported License, http://creativecommons.org/licenses/by/3.0/.

Figure 5-17 courtesy of Stephanie Tsacas with permission granted under the terms of the Creative Commons Attribution Share-Alike 2.5 License, http://creativecommons.org/licenses/by-sa/2.5/.

Figure 5-18 courtesy of Fdominec with permission granted under the terms of the GNU Free Documentation License, Version 1.2, http://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_L

Figure 6-3 courtesy Ingersoll Rand Security Technologies.

INTRODUCTION

The dizzying pace of information systems innovation has made vast expanses of information available to organizations and the public. Often, design flaws and technical vulnerabilities bring unintended consequences, often in the form of information theft and disclosure. The result: a patchwork of laws, regulations, and standards such as Sarbanes-Oxley, the European Data Protection Directive, Gramm-Leach-Bliley, HIPAA, PCI-DSS, PIPEDA, and scores of U.S. state laws requiring public disclosure of security breaches involving private information. Through these, organizations are either required or incentivized to perform their own internal audits or undergo external audits that measure compliance in order to avoid penalties, sanctions, and embarrassing news headlines.

These developments continue to drive demand for IT security professionals and IS auditors. These highly sought professionals play a crucial role in the development of better compliance programs and reduced risk.

The Certified Information Systems Auditor (CISA) certification, established in 1978, is indisputably the leading certification for IS auditing. Demand for the CISA certification has grown so much that the once-per-year certification exam was changed to twice per year in 2005, and is now offered three times each year. In 2005, the CISA certification was awarded accreditation by the American National Standards Institute (ANSI) under international standard ISO/IEC 17024. CISA is also one of the few certifications formally approved by the U.S. Department of Defense in its Information Assurance Technical category (DoD 8570.01-M). In 2009, *SC Magazine* named CISA the best professional certification program. In 2016, there were over 100,000 professionals holding the certification.

IS auditing is not a “bubble” or a flash in the pan. Rather, IS auditing is a permanent fixture in IS/IT organizations that have to contend with new technologies; new systems; new threats; and new data security and privacy laws, regulations, and standards. The CISA certification is the gold standard certification for professionals who work in this domain.

Purpose of This Book

Let’s get the obvious out of the way: this is a comprehensive study guide for the IT or audit professional who needs a serious reference for individual or group-led study for the Certified Information Systems Auditor (CISA) certification. The majority of the content in this book contains the technical information that CISA candidates are required to know.

This book is also a reference for aspiring and practicing IS auditors. The content that is required to pass the CISA exam is the same content that practicing auditors need to be familiar with in their day-to-day work. This book is an ideal CISA exam study guide as well as a desk reference for those who have already earned their CISA certification.

This book is also invaluable for security and business professionals who are required to undergo external audits from audit firms and examinations from regulators. Readers will gain considerable insight into the practices and methods used by auditors; this helps not only in internal audit operations but also to better understand external auditors and how they work.

This book is an excellent guide for someone exploring the IS audit profession. The study chapters explain all of the relevant technologies and audit procedures, and the appendices explain process frameworks and the practical side of professional audits. This is useful for those readers who may wonder what the IS audit profession is all about.

How This Book Is Organized

This book is logically divided into four major sections:

- **Introduction** This Introduction to the book plus Chapter 1 provide an overview of the CISA certification and the IS audit profession.
- **CISA study material** Chapters 2 through 6 contain everything an aspiring CISA candidate is required to know for the CISA exam. This same material is a handy desk reference for aspiring and practicing IS

auditors.

- **IS auditor reference** Appendix A walks the reader through the entire process of a professional IS audit, from audit planning to delivery of the final report. Appendix B discusses control frameworks; this will help an IS auditor who needs to understand how control frameworks function, or who is providing guidance to an organization that needs to implement a control framework.

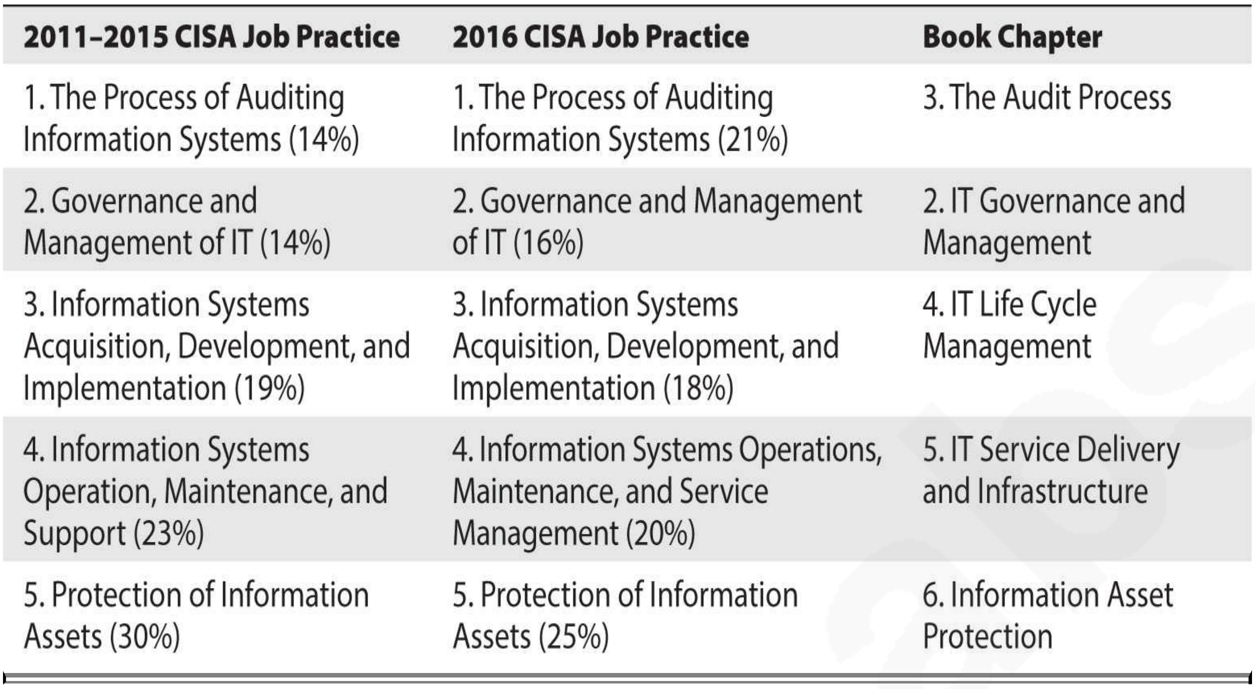
Notes on the Third Edition

ISACA has historically recalibrated the contents of its certifications every five years. In late 2015, ISACA announced that it would update the CISA job practice (the basis for the exam and the requirements to earn the certification), effective in the June 2016 examination. In order to keep this book up to date, I contacted Tim Green at McGraw-Hill so that we might develop a plan for the third edition of this book as quickly as possible. This book is the result of that effort.

The new CISA job practice information was made available in late December 2015. We began work at that time to update the second edition manuscript. The result is this book, which has been updated to reflect all of the changes in the CISA job practice, as well as changes in audit practices, information security, and information technology since the second edition was published.

Changes to the CISA Job Practice

Table 1 illustrates the old and new CISA job practices and their relation to chapters in this book.



2011–2015 CISA Job Practice	2016 CISA Job Practice	Book Chapter
1. The Process of Auditing Information Systems (14%)	1. The Process of Auditing Information Systems (21%)	3. The Audit Process
2. Governance and Management of IT (14%)	2. Governance and Management of IT (16%)	2. IT Governance and Management
3. Information Systems Acquisition, Development, and Implementation (19%)	3. Information Systems Acquisition, Development, and Implementation (18%)	4. IT Life Cycle Management
4. Information Systems Operation, Maintenance, and Support (23%)	4. Information Systems Operations, Maintenance, and Service Management (20%)	5. IT Service Delivery and Infrastructure
5. Protection of Information Assets (30%)	5. Protection of Information Assets (25%)	6. Information Asset Protection

Table 1 Old and New CISA Job Practices

A noteworthy change to the 2016 CISA job practice is the increase in weight of the first domain, The Process of Auditing Information Systems. In 2010 this was only 10 percent of the exam, during 2011–15 it was 14 percent, and now it is 21 percent of the exam. The “A” in CISA receives more emphasis.

Within each domain, the CISA job practice contains many Knowledge Statements and Task Statements. These Knowledge Statements and Task Statements have undergone significant changes in their wording, but often the underlying meanings are similar to the old CISA job practice.

There are, however, several CISA job practice Knowledge Statements that are entirely new, listed here:

- **KS1.11** 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
- **KS2.12** Knowledge of the practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA])
- **KS2.17** Knowledge of the procedures used to invoke and execute the

business continuity plan (BCP) and return to normal operations

- **KS3.2** Knowledge of IT acquisition and vendor management practices (e.g., evaluation and selection process, contract management, vendor risk and relationship management, escrow, software licensing), including third-party outsourcing relationships, IT suppliers, and service providers.
- **KS4.1** Knowledge of service management frameworks
- **KS4.4** Knowledge of enterprise architecture (EA)
- **KS4.8** Knowledge of job scheduling practices, including exception handling
- **KS4.14** Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention)
- **KS4.17** Knowledge of the operational risk and controls related to end-user computing
- **KS5.1** Knowledge of the generally accepted practices and applicable external requirements (e.g., laws, regulations) related to the protection of information assets
- **KS5.2** Knowledge of privacy principles
- **KS5.19** Knowledge of the security risk and controls related to end-user computing
- **KS5.20** Knowledge of methods for implementing a security awareness program
- **KS5.26** Knowledge of the fraud risk factors related to the protection of information assets

Some of these new Knowledge Statements represent additional emphasis on subjects that have been a part of the CISA job practice (e.g., types of audits, security awareness, and control performance), while others are evidence of the need for IS auditors to be familiar with emerging threats, trends, and practices (e.g., enterprise architecture, service management frameworks, and privacy).

A few Task Statements are also new:

- **TS4.6** Evaluate data quality and life cycle management to determine whether they continue to meet strategic objectives.

- **TS4.9** Evaluate end-user computing to determine whether the processes are effectively controlled and support the organization’s objectives.
- **TS5.6** Evaluate the information security program to determine its effectiveness and alignment with the organization’s strategies and objectives.