"All-in-One Is All You Need."

ALL-IN-ONE

CISA®

Certified Information Systems Auditor

EXAM GUIDE

FOURTH EDITION

Complete coverage of all current domains for the 2019 ISACA® Certified Information Systems Auditor exam

Ideal as both a study tool and an on-the-job reference

Filled with practice exam questions and in-depth explanations

Online content includes:

- 300 practice exam questions
- Test engine that provides full-length practice exams and customizable quizzes by exam topic

PETER H. GREGORY

CISA, CISM®, CRISC®, CISSP®, CIPM®, CCISO™, CCSK™, PCI®-QSA

ALL ■ IN ■ ONE

CISA®

Certified Information Systems Auditor

EXAM GUIDE

ABOUT THE AUTHOR

Peter H. Gregory, CISM, CISA, CRISC, CISSP, CIPM, CCISO, CCSK, PCI-QSA, is a 30-year career technologist and an executive director at Optiv Security, the largest security systems integrator (SSI) in the Americas. He has been developing and managing information security management programs since 2002 and has been leading the development and testing of secure IT environments since 1990. Also, Gregory spent many years as a software engineer and architect, systems engineer, network engineer, and security engineer. Throughout his career, he has written many articles, white papers, user manuals, processes, and procedures, and has conducted numerous lectures, training classes, seminars, and university courses.

Peter is the author of more than 40 books about information security and technology, including *Solaris Security* (Prentice Hall, 1999), *CISSP Guide to Security Essentials* (Cengage Learning, 2014), *CISM Certified Information Security Manager All-In-One Exam Guide* (McGraw-Hill Education, 2018), and *CISA Certified Information Systems Auditor All-In-One Exam Guide* (McGraw-Hill Education, 2016). He has spoken at numerous industry conferences, including RSA, Interop, ISACA CACS, (ISC)² Congress, SecureWorld Expo, West Coast Security Forum, OptivCon, Victoria (BC) Privacy and Security Conference, IP3, Society for Information Management, Interface, Tech Junction, SOURCE, the Washington Technology Industry Association, and InfraGard.

Peter is an advisory board member at the University of Washington's certificate program in information security and risk management and the lead instructor (emeritus) and advisory board member for the University of Washington certificate program in cybersecurity. He is an advisory board member and instructor at the University of South Florida's Cybersecurity for Executives program, a former board member of the Washington State chapter of InfraGard, and a founding member of the Pacific CISO Forum. He is a 2008 graduate of the FBI Citizens' Academy and a member of the FBI Citizens' Academy Alumni Association.

Peter resides with his family in Washington State and can be contacted at www.peterhgregory.com.

About the Technical Editor

Bobby E. Rogers is an information security engineer working as a contractor for Department of Defense agencies, helping to secure, certify, and accredit their information systems. His duties include information system security engineering, risk management, and certification and accreditation efforts. He retired after 21 years in the U.S. Air Force, serving as a network security engineer and instructor, and has secured networks all over the world. Bobby has a master's degree in information assurance (IA) and is pursuing a doctoral degree in cybersecurity from Capitol Technology University in Maryland. His many certifications include CISSP-ISSEP, CRISC, CEH, and MCSE: Security, as well as the CompTIA A+, CompTIA Network+, and CompTIA Security+ certifications. He is the author of *CRISC Certified in Risk and Information Systems Control All-In-One Exam Guide* (McGraw-Hill Education, 2016) and *CompTIA Mobility+ All-In-One Exam Guide* (McGraw-Hill Education, 2014). Bobby is also the technical editor for numerous books, including the eighth edition of *CISSP All-in-One Exam Guide* (McGraw-Hill Education, 2018).

This page intentionally left blank

ALL ■ IN ■ ONE

CISA®
Certified Information Systems Auditor

EXAM GUIDE

Fourth Edition

Peter H. Gregory

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

ISBN: 978-1-26-045881-7
MHID: 1-26-045881-4

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-045880-0, MHID: 1-26-045880-6.

eBook conversion by codeMantra
Version 1.0

To Rebekah

This page intentionally left blank

CONTENTS AT A GLANCE

This page intentionally left blank

CONTENTS

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 4-10 courtesy of Don Wells.

Figure 4-11 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_License,_version_1.2.

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/.

(*Continued*)

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_License,_version_1.2.

Figure 6-3 courtesy Ingersoll Rand Security Technologies.

Figure 6-10 courtesy of Rstubbs2 - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=44105524.

ACKNOWLEDGMENTS

I am especially grateful to Wendy Rinaldi for managing the revision process and helping to have this book published on a tight timeline.

Heartfelt thanks to Amy Stonebraker Gray for her project oversight and Claire Yee (and later, Emily Walters) for proficiently managing the submissions phase of this project, facilitating rapid turnaround, and equipping me with the information I needed to produce the manuscript.

I want to thank Bobby Rogers, who took on the task of tech reviewing the manuscript. Bobby carefully and thoughtfully read the entire draft manuscript and made many useful suggestions that have improved the book's quality.

Many thanks to contributors Tanya Scott, who wrote Chapter 1 and Appendix B of the first edition of this book and revised it for the second edition of this book; Chris Tarnstrom, who wrote the original Appendix A; and Justin Hendrickson, a CISA and consultant who practices in Seattle, for updates of Appendix A and B for the third edition. Also, thanks to security and privacy expert John Clark (CISA, CISSP, Security+, CIPP/E, CIPT, CIPM, FIP, PMP), for his revisions of Appendix B. These important texts help readers better understand the CISA certification process and help IS auditors to be more effective in their work. Tanya, Chris, Justin, and John's professional auditing experience and insight add considerable value to this book, long after readers become CISA-certified. My vision for this book includes value for aspiring as well as practicing IS auditors; these contributions allow the book to fulfill this vision.

Many thanks to Lisa Theobald for her excellent copyediting and further improving readability; Lisa caught several errors and made numerous suggestions for this edition. Much appreciation to Cenveo Publisher Services for the page layout. Like Olympic athletes, they make hard work look easy.

Special thanks to Radhika Jolly and Janet Walden for overseeing the production of the book and wringing out errors.

Many thanks to my literary agent, Carole Jelen, for diligent assistance during this and many other projects. Sincere thanks to Rebecca Steele, my business manager, publicist, and research assistant for her long-term vision, for keeping me on track, and for photos that she obtained for earlier editions of the book that are still in use.

Despite having written more than 40 books, I have difficulty putting into words my gratitude for my wife, Rebekah, for tolerating my frequent absences (in the home office) while I revised and added content for this fourth edition. This project could not have been completed without her unfailing support. She deserves the credit.

This page intentionally left blank

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, GLBA, HIPAA, PCI-DSS, NYDFS, PIPEDA, GDPR, CCPA, 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, then three times each year, and is now offered on a continuous basis. 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 and 2017, *SC Magazine* named CISA the best professional certification program. In 2016, there were more than 129,000 professionals holding the certification.

IS auditing is not a "bubble" or a flash in the pan. Instead, IS auditing is a permanent fixture in 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 security 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 in understanding external auditors and how they work. This knowledge and insight will lead to better audit outcomes.

This book is an excellent guide for someone exploring the IS audit profession. The study chapters explain all the relevant technologies and audit procedures, and the appendices explain process frameworks and the practical side of professional audits. The glossary contains a rich collection of terms used by IT security and IS auditors. These are 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.
- **Practice exams** Appendix C explains the CISA practice exams and TotalTester Online test engine that accompany this book.

Notes on the Fourth Edition

ISACA has historically recalibrated the contents of its certifications every five years. In late 2018, 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 2019 examination. In order to keep this book up to date, I contacted Wendy Rinaldi at McGraw-Hill so that we might develop a plan for the fourth 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 2018. We began work at that time to update the third 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 previous and current CISA job practices and their relation to chapters in this book.

2016 CISA Job Practice		2019 CISA Job Practice		All-in-One Coverage
1. The Process of Auditing Information Systems	21%	1. Information Systems Auditing Process	21%	Chapter 3: The Audit Process
2. Governance and Management of IT	16%	2. Governance and Management of IT	17%	Chapter 2: IT Governance and Management
3. Information Systems Acquisition, Development, and Implementation	18%	3. Information Systems Acquisition, Development, and Implementation	12%	Chapter 4: IT Life Cycle Management
4. Information Systems Operation, Maintenance, and Service Management	20%	4. Information Systems Operations and Business Resilience	23%	Chapter 5: IT Service Management and Continuity
5. Protection of Information Assets	25%	5. Protection of Information Assets	27%	Chapter 6: Information Asset Protection

Table 1 Previous and Current CISA Job Practices

For the 2019 CISA job practice, ISACA reformatted the way that the practice areas are described. Previously, each job practice had a set of Knowledge Statements and Task Statements. In the 2019 edition, each job practice consists of two major categories, and each category has four to eleven subtopic areas. This is followed by 39 Supporting Tasks for CISA overall that are not specifically associated with the five domains.

As is typical for each new job practice and revision of this *CISA All-In-One Exam Guide*, I perform a gap analysis to understand what subject matter has been added to the new job practice and what has been eliminated. While the change in structure made this a bit more tedious, in general here are the noteworthy changes in content:

- Audit Project Management is a new topic.
- Audit Data Analytics is a new topic.
- Privacy Principles is a new topic.
- Business continuity planning and disaster recovery planning moved from domain 2 (Governance and Management of IT) to domain 4 (Information Systems Operations and Business Resilience) but are otherwise unchanged.
- Enterprise Architecture moved from domain 3 to domain 2.
- IoT is a new topic.

In addition to the changes to the CISA practice, there are several topics that are altogether new or expanded from the third edition. These changes include

- Segmentation and microsegmentation
- Virtualization, containerization, and virtual keyboards

- 5G
- A greater emphasis on systems acquisition with the systems development life cycle, which reflects the migration away from custom software development toward the acquisition of shrink-wrap software and Software-as-a-Service for core business applications
- The impact of digital transformation
- Zero Trust principles of enterprise architecture
- The NIST Cybersecurity Framework (CSF)
- New laws and regulations such as GDPR and CCPA
- Agile methodology for managing changes to infrastructure and business processes
- Several new development methodologies
- Cloud responsibility models
- Passwords, and whether they should periodically expire
- The threat of ransomware and destructware
- Changes in the meaning of remote access and VPNs
- Addition of numerous new technologies such as BLE and WPA3
- Removal of long-deprecated technology such as X.25
- Addition of 64 new items and cross-references to the glossary (and a few deprecated items removed)

By the time we completed this book, there were even more new developments, technologies, techniques, and breaches that provided additional insight and the promise of still more improvements. Like the surface of Saturn's moon, Io, our profession is ever changing. The technology boneyard is filled with vendors, products, protocols, techniques, and methodologies that once held great promise, later replaced with better things. This underscores the need for IS auditors (and IT, security, and risk professionals) to stay current by reading up on current events, new technologies, and techniques.

CHAPTER 1

Becoming a CISA

This chapter discusses the following topics:

- What it means to be a CISA-certified professional
- Getting to know ISACA, its code of ethics, and its standards
- Undergoing the certification process
- Applying for the exam
- Maintaining your certification
- Getting the most from your CISA journey

Congratulations on choosing to become a Certified Information Systems Auditor (CISA). Whether you have worked for several years in the field of information systems auditing or have just recently been introduced to the world of controls, assurance, and security, don't underestimate the hard work and dedication required to obtain and maintain CISA certification. Although ambition and motivation are essential, the rewards of being CISA certified can far exceed the effort.

You probably never imagined you would find yourself working in the world of auditing or looking to obtain a professional auditing certification. Perhaps the increase in legislative or regulatory requirements for information system security led to your introduction to this field. Or possibly you noticed that CISA-related career options are increasing exponentially and you have decided to get ahead of the curve. You aren't alone: since the inception of CISA certification in 1978, more than 129,000 professionals worldwide reached the same conclusion and have earned this well-respected certification. In 2009 and again in 2017, *SC Magazine* named CISA certification the winner of the *Best Professional Certification Program*, and in 2014 it was a finalist for the same award. The 2016 Global Knowledge *IT Skills and Salary Report*, as well as a recent *IT Skills and Certifications Pay Index* (ITSCPI) from Foote Partners, show the CISA certification among the highest-paying IT certifications. Welcome to the journey and the amazing opportunities that await you.

I have put together this information to help you understand the commitment needed, prepare for the exam, and maintain your certification. Not only is it my wish that you prepare for and pass the exam with flying colors, but I also provide you with the information and resources to maintain your certification and to represent yourself and the professional world of information system (IS) auditing proudly with your new credentials.

ISACA (formerly known as the Information Systems Audit and Control Association) is a recognized leader in the areas of control, assurance, and IT governance. Formed in 1967, this nonprofit organization represents more than 140,000 professionals in more than 180 countries. ISACA administers several exam certifications, including the CISA, the Certified Information Security Manager (CISM), the Certified in Risk and Information Systems Control (CRISC), and the Certified in the Governance of Enterprise IT (CGEIT) certifications. The certification program itself has been accredited by the American National Standards Institute (ANSI) under International Organization for Standardization and International Electrotechnical Commission standard ISO/IEC 17024:2012, which means that ISACA's procedures for accreditation meet international requirements for quality, continuous improvement, and accountability.

If you're new to ISACA, I recommend that you tour the organization's web site (www.isaca.org) and become familiar with the guides and resources available. In addition, if you're near one of the 200-plus local ISACA chapters in more than 80 countries worldwide, consider taking part in the activities and even reaching out to the chapter board for information on local meetings, training days, conferences, or study sessions. You may be able to meet other IS auditors who can give you additional insight into the CISA certification and the audit profession.

Established in 1978, the CISA certification primarily focuses on audit, controls, assurance, and security. It certifies the individual's knowledge of testing and documenting IS controls and his or her ability to conduct formal IS audits. Organizations seek out qualified personnel for assistance with developing and maintaining strong control environments. A CISA-certified individual is a great candidate for this.

Through the phenomenon of digital transformation, organizations in every industry sector around the world are becoming increasingly reliant on information systems for daily business operations. Further, the upward trend in IT outsourcing in the form of Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) offerings means organizations are put in a position of having to trust those service providers that the SaaS, PaaS, and IaaS platforms are secure. This reliance compels organizations to rely heavily on IS auditors to provide assurances that IT environments have the necessary security, integrity, and resilience that today's organizations require.

Benefits of CISA Certification

Obtaining the CISA certification offers several significant benefits:

- **Expands knowledge and skills, builds confidence** Developing knowledge and skills in the areas of audit, controls, assurance, and security can prepare you for advancement or expand your scope of responsibilities. The personal and professional achievement can boost confidence that encourages you to move forward and seek new career opportunities.
- **Increases marketability and career options** Because of various legal and regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes-Oxley (SOX), the Gramm-Leach-Bliley Act (GLBA),

the Food and Drug Administration (FDA), the Federal Energy Regulatory Commission/North American Electric Reliability Corporation (FERC/NERC), the European General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA), along with the growing need for information systems and automation, controls, assurance, and audit experience, demand is growing for individuals with experience in developing, documenting, and testing controls. In addition, obtaining your CISA certification demonstrates to current and potential employers your willingness and commitment to improve your knowledge and skills in information systems auditing. Having a CISA can provide a competitive advantage and open up many doors of opportunity in various industries and countries.

- **Helps you meet other certification requirements** The Payment Card Industry Qualified Security Assessor (PCI-QSA) certification requires that all certificate holders have a current security audit certification, either CISA or ISO 27001 Lead Auditor.
- **Helps you meet employment requirements** Many government agencies and organizations, such as the United States Department of Defense (DoD), require CISA certifications for positions involving IS audit activities. DoD Directive 8140.01 (formerly DoD Directive 8570.01-M) mandates that those personnel performing information assurance activities within the agency are certified with a commercial accreditation approved by the DoD. The DoD has approved the ANSI-accredited CISA certificate program because it meets ISO/IEC 17024:2012 requirements. All Information Assurance Technical (IAT) Level III personnel are mandated to obtain CISA certification, as are those who are contracted to perform similar activities.
- **Builds customer confidence and international credibility** Prospective customers needing control or audit work will have faith that the quality of the audits and controls documented or tested are in line with internationally recognized standards.

Regardless of your current position, demonstrating knowledge and experience in the areas of IT controls, audit, assurance, and security can expand your career options. The certification does not limit you to auditing; it can provide additional value and insight to those in or seeking the following positions:

- Executives such as chief executive officers (CEOs), chief financial officers (CFOs), and chief information officers (CIOs)
- Chief audit executives, audit partners, and audit directors
- Security and IT operations executives (chief technology officers [CTOs], chief information security officers [CISOs], chief information risk officers [CIROs], chief security officers [CSOs]), directors, managers, and staff
- Compliance executives and management
- Security and audit consultants
- Audit committee members

The CISA Certification Process

To become a CISA, you are required to pay the exam fee, pass the exam, prove that you have the required experience and education, and agree to uphold ethics and standards. To keep your CISA certification, you are required to take at least 20 continuing education hours each year (120 hours in three years) and pay annual maintenance fees. This is depicted in Figure 1-1.

The following list outlines the major requirements for becoming certified:

- **Experience** A CISA candidate must be able to submit verifiable evidence of at least five years' experience, with a minimum of two years' professional work experience in IS auditing, control, assurance, or security. Experience can be in any of the job content areas, but it must be verified. For those with less than five years' experience, substitution and waiver options for up to three years' experience are available.
- **Ethics** Candidates must commit to adhere to ISACA's Code of Professional Ethics, which guides the personal and professional conduct of those certified.
- **Standards** Those certified agree to abide by IS auditing standards and minimum guidelines for performing IS audits.
- **Exam** Candidates must receive a passing score on the CISA exam. A passing score is valid for up to five years, after which the score is void. This means that a CISA candidate who passes the exam has a *maximum* of five years to apply for CISA certification; candidates who pass the exam but fail to act after five years will have to take the exam again if they want to become CISA certified.
- **Application** After successfully passing the exam, meeting the experience requirements, and having read through ISACA's Code of Professional Ethics and Information Systems Auditing Standards, a candidate is ready to apply for certification. An application must be received within five years of passing the exam.

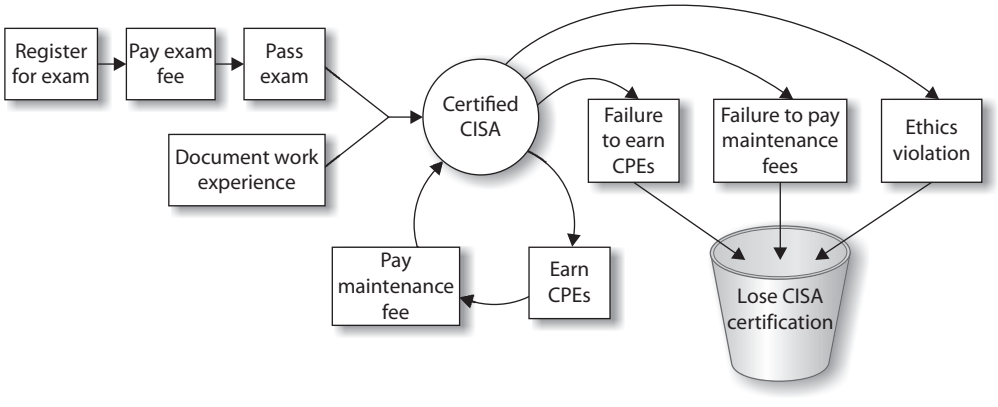

Figure 1-1 The CISA certification life cycle

- **Education** Those certified must adhere to the CISA Continuing Education Policy, which requires a minimum of 20 continuing professional education (CPE) hours each year, with a total requirement of 120 CPEs over the course of the certification period (three years).

Experience Requirements

To qualify for CISA certification, you must have completed the equivalent of five years' total work experience. These five years can take many forms, with several substitutions available. Additional details on the minimum certification requirements, substitution options, and various examples are discussed next.

NOTE Although it is not recommended, a CISA candidate can take the exam before completing any work experience directly related to IS auditing. As long as the candidate passes the exam and the work experience requirements are fulfilled within five years of the exam date, and within ten years from application for certification, the candidate is eligible for certification.

Direct Work Experience

You are required to have a minimum of two years' work experience in the field of IS audit, controls, or security. This is equivalent to 4,000 actual work hours, which must be related to one or more of the five following CISA job practice areas:

- **Information Systems Auditing Process** Planning and conducting information systems audits in accordance with IS standards and best practices, communicating results, and advising on risk management and control practices.
- **Governance and Management of IT** Ensuring that adequate organizational structures and processes are in place to align and support the organization's strategies and objectives.
- **Information Systems Acquisition, Development, and Implementation** Ensuring that appropriate processes and controls are in place for the acquisition, development, testing, and implementation of information systems in order to provide reasonable assurance that the organization's strategies and objectives will be met.
- **Information Systems Operations and Business Resilience** Ensuring that systems and infrastructure have appropriate operations, maintenance, and service management processes and controls in place to support meeting the organization's strategies and objectives.
- **Protection of Information Assets** Ensuring that the organization's security policies, standards, procedures, and controls protect the confidentiality, integrity, and availability of information assets.

All work experience must be completed within the ten-year period before completing the certification application or within five years from the date of initially passing the

CISA exam. You will need to complete a separate Verification of Work Experience form for each segment of experience.

There is only one exception to this minimum two-year direct work experience requirement: if you are a full-time instructor. This option is discussed in the next section.

Substitution of Experience

Up to a maximum of three years' direct work experience can be substituted with the following to meet the five-year experience requirement:

- One year of information systems or one year of non-IS auditing experience can be substituted for up to one year of direct work experience.
- Completion of a two- or four-year degree (60 to 120 completed university semester credit hours), regardless of when completed, can be substituted for one or two years of direct work experience, respectively. Transcripts or a letter confirming degree status must be sent from the university attended to obtain the experience waiver.
- If you have completed a bachelor's or master's degree from a university that enforces an ISACA-sponsored curriculum, it can be substituted for one or two years of direct work experience, respectively (for information on ISACA-sponsored Model Curricula and participating universities, see www.isaca.org/modeluniversities). Transcripts or a letter confirming degree status must be sent from the university to obtain an experience waiver. This option cannot be used if you have already substituted or waived three years of direct work experience.
- Association of Chartered Certified Accountants (ACCA) members and Chartered Institute of Management Accountants (CIMA) members with full certification can apply for a two-year educational waiver.
- Those applying with a master's degree in information systems or information technology (IT) from an accredited university can apply for a one-year experience waiver.

As noted, there is only one exception to the experience requirements. Should you have experience as a full-time university instructor in a related field (that is, information security, computer science, or accounting), each two years of your experience can be substituted for one year of required direct work experience, without limitation.

Here is an example CISA candidate whose experience and education are considered for CISA certification:

> Jane Doe graduated in 2004 with a bachelor's degree in accounting. She spent five years working for an accounting firm conducting non-IS audits, and in January 2009, she began conducting IS audits full time. In January 2011, she took some time off work for personal reasons and rejoined the workforce in December 2017, working for a public company in its internal audit department documenting and testing financial controls. Jane passed the CISA exam in June 2018 and applied for CISA certification in January 2019. Does Jane have all of the experience required? What evidence will she need to submit?

- **Two-year substitution** Jane obtained a bachelor's degree in accounting, which equates to two years' experience substitution.
- **Two years' direct experience** She can count her two full years of IS audit experience (in 2009 and 2010).
- **One-year substitution** She cannot take into account one year of non-IS audit experience completed between January 2008 to January 2009, as it was not completed within ten years of application.
- **One-year substitution** Jane would want to utilize her new internal audit financial controls experience for experience substitution rather than her earlier non-IS audit experience.

Jane would need to send the following with her application to prove experience requirements are met:

- Verification of Work Experience forms filled out and signed by her supervisors (or any superior) at the accounting firm, verifying both the IS and non-IS audit work conducted.
- Transcripts or letter confirming degree status sent from the university.

NOTE I recommend you also read the CISA certification qualifications on the ISACA web site. From time to time, ISACA changes the qualification rules, and I want you to have the most up-to-date information available.

IS vs. IT

You're probably noticing the use of the terms "IS" and "IT" in this chapter. Indeed, you'll find these terms throughout the entire book. IS means *information systems*, an inclusive term that can mean a single computer, its operating system, an application running on the system, a network device, a virtual machine, or a collection of systems that work together to fulfill some purpose. In the world of auditing information systems, a person who examines information systems is an IS auditor.

Notice also that the letters "IS" in CISA stand for *information systems*, not *information security*, as is sometimes believed. A CISA is expected to know how to audit all aspects of an information system, not just security controls used to protect systems and information.

IT means *information technology* and refers to the technology found in computers, software, storage systems, and applications. In most organizations, the group of people who manage information technology is known as the IT department. Some organizations, however, ascribe the term IS department.

Often, IS and IT are used interchangeably, and generally, such usage is not considered inappropriate or incorrect.

ISACA Code of Professional Ethics

Becoming a CISA means that you agree to adhere to the ISACA Code of Professional Ethics, a formal document outlining those things you will do to ensure the utmost integrity and that best support and represent the organization and certification.

The ISACA Code of Professional Ethics requires ISACA members and certification holders to do the following (from www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx):

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.

Failure to follow the code of ethics can result in an investigation of the person's actions; potential disciplinary measures range from a written warning to the loss of certification and/or membership.

You'll find the full text and terms of enforcement of the ISACA Code of Ethics at www.isaca.org/ethics.

ISACA IS Standards

An auditor can gather information from several credible resources to conduct an audit with integrity and confidence. ISACA has developed its own set of standards of mandatory requirements for IS auditing and reporting, known as the ITAF: Information Technology Assurance Framework.

ITAF offers multiple levels of IS audit and assurance guidance: standards, guidelines, and tools and techniques. Standards are higher level *mandatory* requirements that inform IS audit and assurance professionals of minimal performance expectations. Guidelines provide additional guidance in applying the standards, while tools and techniques provide examples of procedures that audit and assurance professionals may follow.

As a CISA, you are required to abide by and promote the IS standards where applicable, encouraging compliance and supporting their implementation. As you prepare for certification and beyond, you will need to read through and become familiar with these standards. These standards were created to define the minimum level of acceptable performance needed to meet the professional requirements as defined by ISACA and to help set expectations. They have been established, vetted, and approved by ISACA.

For more about ITAF, visit www.isaca.org/itaf.

General standards represent guiding principles by which the profession conducts IT audit and assurance activities. General standards include

- Audit charter
- Organizational independence
- Professional independence
- Reasonable expectation
- Due professional care
- Proficiency
- Assertions
- Criteria

Performance standards focus on the IT audit or assurance professional's conduct of assurance activities—such as the design, evidence, findings, and conclusions. These standards include

- Engagement planning
- Risk assessment in planning
- Performance and supervision
- Materiality
- Evidence
- Using the work of other experts
- Irregularity and illegal acts

Reporting standards cover the report produced by the IT audit or assurance professional, such as

- Reporting
- Follow-up activities

NOTE I recommend that you check the ISACA web site periodically for updates to these standards. As an ISACA member, you will automatically be notified when changes have been submitted and the documents are open for review (www.isaca.org/standards).

The Certification Exam

The certification exam is offered almost continuously throughout the year in periods known as *testing windows* that are generally several months in length. The ISACA web site will have information about current testing windows and sometimes about future testing windows. When you begin planning for your CISA examination, you'll want to consult the ISACA web site to see what scheduling options are available in your testing window. Other terms and conditions change from time to time, from one testing window to the next.

In 2019, the schedule of exam fees in U.S. dollars was

- CISA application fee: $50
- Regular registration: $575 member/$760 nonmember

The exam is administered by an ISACA-approved testing vendor, PSI Services, at numerous locations. For additional details on the locations nearest you, go to www.isaca.org/examlocations.

Once registration is complete, you will immediately receive an e-mail acknowledging your registration, and within four weeks of processing you will receive a hard copy of the letter and a registration receipt in the mail. Two to three weeks prior to the test date you will receive an exam admission ticket via e-mail and regular mail. You will need the admission ticket to enter the test site—be sure to keep it unmarked and in a safe place until test time.

Each registrant has four hours to take the multiple-choice-question exam. There are 150 questions on the computerized exam representing the five job practice areas. Each question has four answer choices; test-takers can select only one best answer by clicking it. You will be scored for each job practice area and then provided one final score. Before you close out the computerized exam, you will be notified of your tentative pass/fail status. All exam scores are scaled. Scores range from 200 to 800; however, a final score of 450 is required to pass.

Exam questions are derived from a job practice analysis study conducted by ISACA. The areas selected represent those tasks performed in a CISA's day-to-day activities and represent the background knowledge required to perform IS audit, control, assurance, and security tasks. More detailed descriptions of the task and knowledge statements can be found at www.isaca.org/cisajobpractice.

The CISA exam is quite broad in its scope. The exam covers five job practice areas, as shown in Table 1-1.

Independent committees have been developed to determine the best questions, review exam results, and statistically analyze the results for continuous improvement. Should you come across a horrifically difficult or strange question, do not panic. This question

Domain	CISA Job Practice Area	Percentage of Exam
1	Information Systems Auditing Process	21
2	Governance and Management of IT	17
3	Information Systems Acquisition, Development, and Implementation	12
4	Information Systems Operations and Business Resilience	23
5	Protection of Information Assets	27

Table 1-1 CISA Exam Practice Areas

may have been written for another purpose. A few questions on the exam are included for research and analysis purposes and will not be counted against your score.

Exam Preparation

The CISA certification requires a great deal of knowledge and experience from the CISA candidate. You need to map out a long-term study strategy to pass the exam. The following sections offer some tips and are intended to help guide you to, through, and beyond exam day.

Before the Exam

Consider the following list of tips on tasks and resources for exam preparation. They are listed in sequential order.

- **Read the ISACA Exam Candidate Information Guide** For information on the certification exam and requirements for the current year, see www.isaca.org/Certification/Pages/Candidates-Guide-for-Exams.aspx. Be sure to download the correct (usually the most recent) version of the guide.
- **Register** Register to solidify your commitment to moving forward with this professional achievement.
- **Become familiar with the CISA job practice areas** The job practice areas serve as the basis for the exam and requirements. Beginning with the June 2019 exam, the job practice areas have changed. Ensure that your study materials align with the current list at www.isaca.org/cisajobpractice.
- **Self-assess** Run through the questions in the two practice exams, provided as additional resources with this book; see Appendix C for more information. You may also go to the ISACA web site for a free 50-question CISA self-assessment.
- **Iterative study** Depending on how much work experience in IS auditing you have already, I suggest you plan your study program to take at least two months but as long as six months. During this time, periodically take practice exams and note your areas of strength and weakness. Once you have identified your weak areas, focus on those areas weekly by rereading the related sections in this book and retaking practice exams, and note your progress.

- **Avoid cramming** We've all seen the books on the shelves with titles that involve last-minute cramming. Just one look on the Internet reveals a variety of web sites that cater to teaching individuals how to cram for exams most effectively. There are also research sites claiming that exam cramming can lead to susceptibility to colds and flu, sleep disruptions, overeating, and digestive problems. One thing is certain: many people find that good, steady study habits result in less stress and greater clarity and focus during the exam. Because of the complexity of this exam, I highly recommend the long-term, steady-study option. Study the job practice areas thoroughly. There are many study options. If time permits, investigate the many resources available to you.
- **Find a study group** Many ISACA chapters have formed specific study groups or offer less expensive exam review courses. Contact your local chapter to see if these options are available to you. In addition, be sure to keep your eye on the ISACA web site.
- **Admission ticket** Approximately two to three weeks before the exam, you will receive your admission ticket. Do not write on or lose this ticket. Put it in a safe place, and take note of what time you will need to arrive at the site. Note this on your calendar.
- **Logistics check** Check the Candidate Information Guide and your admission ticket for the exact time you are required to report to the test site. Check the site a few days before the exam—become familiar with the location and tricks to getting there. If you are taking public transportation, be sure that you are looking at the schedule for the day of the exam. If you are driving, know the route and know where to park your vehicle.
- **Pack** Place your admissions ticket and a photo ID in a safe place, ready to go. Your ID must be a current, government-issued photo ID that matches the name on the admission ticket and must not be handwritten. Examples of acceptable forms of ID are passports, driver's licenses, state IDs, green cards, and national IDs. Make sure you leave food, drinks, laptops, cell phones, and other electronic devices behind, as they are not permitted at the test site. For information on what can and cannot be brought to the exam site, see www.isaca.org/cisabelongings.
- **Notification decision** Decide whether you want your exam results e-mailed to you. You will have the opportunity to consent to e-mail notification of the exam results. If you are fully paid (zero balance on exam fee) and have consented to the e-mail notification, you should receive a single e-mail a few weeks from the date of the exam with your exam results.
- **Sleep** Get a sound night's sleep before the exam. Research suggests that you should avoid caffeine at least four hours before bedtime, keep a notepad and pen next to the bed to capture late-night thoughts that might keep you awake, eliminate as much noise and light as possible, and keep your room a good temperature for sleeping. In the morning, arise early so as not to rush and subject yourself to additional stress.

Day of the Exam

Consider the following list of tips that can help you on exam day:

- **Arrive early** Check the Candidate Information Guide and your admission ticket for the exact time you are required to report to the test site. The ticket and the Candidate Information Guide explain that you must be at the test site *no later* than approximately 30 minutes *before* testing time. If you are late, you may miss your opportunity to take the exam on that day, and you'll have to reschedule your exam.
- **Observe test center rules** There may be rules about taking breaks. This will be discussed by the examiner along with exam instructions. If at any time during the exam you need something and are unsure as to the rules, be sure to ask first. For information on conduct during the exam, see www.isaca.org/cisabelongings.
- **Answering exam questions** Read questions carefully, but do not try to overanalyze. Remember to select the *best* solution. There may be several reasonable answers, but one is *better* than the others.

After the Exam

Although you'll be shown your preliminary pass/fail results when you have completed and closed your exam, you will receive your official exam results by e-mail or regular mail within a few weeks from the date of the exam. Each job practice area score will be noted in addition to the overall final score. Should you receive a passing score, you will also receive the application for certification.

Those unsuccessful in passing will also be notified. These individuals will want to take a close look at the job practice area scores to determine areas for further study. They may retake the exam as many times as needed on future exam dates, as long as they have registered and paid the applicable fees. Regardless of pass or fail, exam results will not be disclosed via telephone, fax, or e-mail (with the exception of the consented one-time e-mail notification).

CAUTION You are not yet permitted to use the CISA moniker after passing the exam. You must first apply for CISA certification, which is described in the next section.

Applying for CISA Certification

To apply for certification, you must be able to submit evidence of a passing score and related work experience. Keep in mind that once you receive a passing score, you have five years to use this score on a CISA application. After this time, you will need to take the exam again. In addition, all work experience submitted must have been within ten years of your new certification application.

To complete the application process, you need to submit the following information:

- **CISA application** Note the exam ID number located in your exam results letter; list the information systems audit, control, security experience, and/or any experience substitutions; and identify which ISACA job practice area(s) the experience pertains to.
- **Verification of Work Experience form(s)** These must be filled out and signed by your immediate supervisor or a person of higher rank in the organization to verify work experience noted on the application. You must fill out a complete set of Work Experience forms for each separate employer.
- **Transcript or letter** If you are using an educational experience waiver, you must submit an original transcript or a letter from the college or university confirming degree status.

As with the exam, after you've successfully mailed the application, you must wait approximately eight weeks for processing. If your application is approved, you will receive a package in the mail containing your letter of certification, a certificate, and a copy of the Continuing Education Policy. You can then proudly display your certificate and use the designation ("CISA") on your CV, résumé, e-mail profile, or business cards.

Retaining Your CISA Certification

There is more to becoming a CISA than merely passing an exam, submitting an application, and receiving a paper certificate. Being a CISA is an ongoing lifestyle. Those with the CISA certification not only agree to abide by the Code of Professional Ethics and adhere to the IS standards, but they must also meet ongoing education requirements and pay certification maintenance fees. Let's take a closer look at the education requirements and explain the fees involved in retaining certification.

Continuing Education

The goal of continuing professional education (CPE) requirements is to ensure that individuals maintain CISA-related knowledge so that they can better manage, assess, and design controls around IS. To maintain CISA certification, individuals must obtain 120 CPE hours within three years, with a minimum requirement of 20 hours per year. Each CPE hour is to account for 50 minutes of active participation in educational activities.

What Counts as a Valid CPE Credit?

In order for training and activities to be utilized for CPEs, they must involve technical or managerial training that is directly applicable to IS assessments, audit, controls, or security. The following list of activities has been approved by the CISA certification committee and can count toward your CPE requirements:

- ISACA professional education activities and meetings.
- If you are an ISACA member, you can take *ISACA Journal* CPE Quizzes online or participate in monthly webcasts. For each webcast, CPEs are rewarded after you pass a quiz.

- Non-ISACA professional education activities and meetings.
- Self-study courses.
- Vendor sales or marketing presentations (ten-hour annual limit).
- Teaching, lecturing, or presenting on subjects related to job practice areas.
- Publication of articles and books related to the profession.
- CISA exam question development and review.
- Passing related professional examinations.
- Participation in ISACA boards or committees (20-hour annual limit per ISACA certification).
- Contributions to the IS audit and control profession (ten-hour annual limit).
- Mentoring (ten-hour annual limit).

For more information on what is accepted as a valid CPE credit, see the continuing professional education policy (www.isaca.org/cisacpepolicy).

Tracking and Submitting CPEs

Not only are you required to submit a CPE tracking form for the annual renewal process, but you also should keep detailed records for each activity. Records associated with each activity should include the following:

- Name of attendee
- Name of sponsoring organization
- Activity title
- Activity description
- Activity date
- Number of CPE hours awarded

It is in your best interest to track all CPE information in a single document or worksheet. ISACA has developed a Verification of Attendance form for your use at www.isaca.org/cisacpepolicy. To make it easy on yourself, consider keeping all related records such as receipts, brochures, and certificates in the same place. Retain documentation throughout the three-year certification period and for one additional year afterward. This is especially important, because you may someday be audited. If this happens, you would be required to submit all paperwork. So why not be prepared?

For new CISAs, the annual and three-year certification period begins January 1 of the year following certification. You are not required to report CPE hours for the first partial year after your certification; however, the hours earned from the time of certification to December 31 can be utilized in the first certification reporting period the following year. Therefore, should you get certified in January, you will have until the following January to accumulate CPEs and will not have to report them until you report the totals for the

following year, which will be in October or November. This is known as the *renewal period*. During this time, you will receive an e-mail directing you to the web site to enter CPEs earned over the course of the year. Alternatively, the renewal will be mailed to you, and you can record CPEs on the hard-copy invoice and send them with your maintenance fee payment. CPEs and maintenance fees must be received by January 15 to retain certification.

Notification of compliance from the certification department is sent after all of the information has been received and processed. Should ISACA have any questions about the information you have submitted, they will contact you directly.

Sample CPE Submission

Table 1-2 contains an example of a CPE submission.

CPE Maintenance Fees

To remain CISA certified, you must pay CPE maintenance fees each year. These fees are (as of 2019) $45 for members and $85 for nonmembers each year. These fees are in

Name: John Jacob
Certification Number: 67895787
Certification Period: 1/1/2019 to 12/31/2019

Activity Title/Sponsor	Activity Description	Date	CPE Hours	Support Docs Included?
ISACA presentation/lunch	PCI compliance	2/12/2019	1 CPE	Yes (receipt)
ISACA presentation/lunch	Security in SDLC	3/12/2019	1 CPE	Yes (receipt)
Regional Conference, RIMS	Compliance, risk	1/15–17/2019	6 CPEs	Yes (CPE receipt)
Brightfly webinar	Governance, risk, and compliance	2/16/2019	3 CPEs	Yes (confirmation e-mail)
ISACA board meeting	Chapter board meeting	4/9/2019	2 CPEs	Yes (meeting minutes)
Presented at IIA meeting	IT audit presentation	6/21/2019	1 CPE	Yes (meeting notice)
Published an article in XYZ	Journal article on SOX ITGC	4/12/2019	4 CPEs	Yes (article)
Vendor presentation	Learned about GRC tool capability	5/12/2019	2 CPEs	Yes
Employer-offered training	Change management course	3/26/2019	7 CPEs	Yes (certificate of course completion)

Table 1-2 Sample CPE Submission

addition to ISACA membership and local chapter dues (which are not required to maintain your CISA certification).

Revocation of Certification

A CISA-certified individual may have his or her certification revoked for the following reasons:

- Failure to complete the minimum number of CPEs during the required period.
- Failure to document and provide evidence of CPEs in an audit.
- Failure to submit payment for maintenance fees.
- Failure to comply with the Code of Professional Ethics; this can result in investigation and ultimately lead to revocation of certification.

If you have received a revocation notice, you will need to contact the ISACA Certification Department at certification@isaca.org for more information.

CISA Exam Preparation Pointers

Following are a few general pointers for exam prep:

- Register for the exam early to ensure that you can take the exam at a location and date of your choosing.
- When studying for the exam, take as many practice exams as possible.
- Memorization will not work—for this exam, it is critical that you understand the concepts.
- If you have time while studying for the exam, begin gathering relevant Work Experience Verification forms from past employers and original transcripts from your college or university (if using the education experience waiver).
- Do not arrive late to the exam site. Latecomers are immediately disqualified and they forfeit exam fees.
- Begin keeping track of CPEs as soon as you obtain certification.
- Mark your calendar for CPE renewal time, which begins in October/November each year and ends January 15. Don't wait for the e-mail; set your own reminder.
- Become familiar with the Code of Professional Ethics and IS standards.
- Become involved in your local ISACA chapter for networking and educational opportunities.

Summary

Becoming and being a CISA is a lifestyle, not just a one-time event. It takes motivation, skill, good judgment, and proficiency to be a strong leader in the world of information systems auditing. The CISA was designed to help you navigate the IS auditing world with greater ease and confidence.

In the following chapters, each CISA job practice area is discussed in detail, and additional reference material is presented. Not only is this information useful for studying prior to the exam, but it is also meant to serve as a resource throughout your career as an audit professional.

CHAPTER 2

IT Governance and Management

This chapter covers CISA Domain 2, "Governance and Management of IT," and discusses the following topics:

- IT governance structure
- Human resources management
- IT policies, standards, processes, and procedures
- Management practices
- IT resource investment, use, and allocation practices
- IT contracting and contract management strategies and practices
- Risk management practices
- Monitoring and assurance

The topics in this chapter represent 17 percent of the CISA examination.

IT governance should be the wellspring from which all other IT activities flow.

Properly implemented, *governance* is a process whereby senior management exerts strategic control over business functions through policies, objectives, delegation of authority, and monitoring. Governance is management's control over all other IT processes to ensure that IT processes continue to meet the organization's business objectives effectively.

Business alignment is a critical characteristic of IT governance. IT's primary mission should be the support of the overall business mission, goals, and objectives. The alignment of IT to the business must be intentional and deliberate for IT and the organization to succeed.

Organizations usually establish governance through an IT steering committee that is responsible for setting long-term IT strategy and by making changes to ensure that IT processes continue to support IT strategy and the organization's needs. This is accomplished through the development and enforcement of IT policies, requirements, and standards.

IT governance typically focuses on several key processes, such as personnel management, sourcing, change management, financial management, quality management, security management, and performance optimization. Another key component is the

establishment of an effective organization structure and clear statements of roles and responsibilities. An effective governance program will use a balanced scorecard (BSC) or other means to monitor these and other key processes, and through a process of continuous improvement, IT processes will be changed to remain effective and to support ongoing business needs.

IT Governance Practices for Executives and Boards of Directors

Governance starts at the top.

Whether the organization has a board of directors, council members, commissioners, or some other top-level governing body, governance begins with the establishment of top-level objectives and policies that are translated into more actions, policies, processes, procedures, and other activities downward through each level in the organization.

This section describes governance practices recommended for IT organizations, including a strategy-developing committee, measurement via the BSC, and security management.

NOTE Governance is not merely an IT practice. Rather, governance is practiced in the business apart from IT to facilitate management's control over all aspects of business operations, including IT.

IT Governance

The purpose of IT governance is to align the IT organization with the needs of the business. The term *IT governance* refers to a collection of top-down activities intended to control the IT organization from a strategic perspective to ensure that the IT organization supports the business. The artifacts and activities that flow out of healthy IT governance include the following:

- **Policy** At its minimum, IT policy should directly reflect the mission, objectives, and goals of the overall organization.
- **Priorities** Priorities in the IT organization should flow directly from the organization's mission, objectives, and goals. Whatever is most important to the organization as a whole should be important to IT as well.
- **Standards** The technologies, protocols, and practices used by IT should reflect the organization's needs. On their own, standards help to drive a consistent approach to solving business challenges; the choice of standards should facilitate solutions that meet the organization's needs in a cost-effective and secure manner.
- **Resource management** The budget, personnel, equipment, and other resources are planned, selected, managed, and measured to ensure that the IT organization has the ability to meet its objectives.

- **Vendor management** The suppliers and service providers that IT selects should reflect IT and business priorities, standards, and practices.
- **Program and project management** IT programs and projects should be organized and performed in a consistent manner that reflects IT and business priorities and supports the business.

While IT governance contains the elements just described, strategic planning is also a key component of governance. Strategy development is discussed in the next section.

IT Governance Frameworks

Every organization may have a unique mission, objectives, goals, business models, tolerance for risk, and so on, but organizations need not invent governance frameworks from scratch to manage their IT and business objectives. Several good frameworks can be adapted to meet organizations' needs, including the following:

- **COBIT** This IT management framework was developed by the IT Governance Institute and ISACA. COBIT's five domains are Evaluate, Direct, and Monitor; Align, Plan, and Organize; Build, Acquire, and Implement; Deliver, Service, and Support; and Monitor, Evaluate, and Assess.
- **ISO/IEC 27001** This is the well-known international standard for top-down information security management. In the context of IT security governance, most important here are the requirements (sometimes referred to as the *clauses*) in ISO/IEC 27001, not the security controls that appear in its appendix. This is a good opportunity to point out that governance frameworks and control frameworks are not the same thing.
- **ITIL** Formerly an acronym for *IT Infrastructure Library*, ITIL is a framework of processes for IT service delivery. ITIL was originally sponsored by the UK Office of Government Commerce to improve its IT management processes, but it is now owned by AXELOS. The international standard, ISO/IEC 20000, is adapted from ITIL.
- **ISO/IEC 38500** This international standard on corporate governance of information technology is suitable for small and large organizations in the public or private sector.
- **COSO** This framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission to combat internal fraud. COSO is a framework of internal controls, mainly targeting financial accounting systems and implicitly underlying relevant IT controls.

These and other frameworks are discussed in greater detail in Appendix B.

Digital Transformation

The phenomenon known as *digital transformation* represents the trend of increasing reliance of businesses on information technology. DX, as it is sometimes known, surpasses the mere *support* of business processes with information technology, but also includes business processes entirely based on information technology. The United States is leading this revolution, with the UK and Europe not far behind. This trend underscores the need for IS auditors, and even the digital transformation of IS audit itself.

IT Strategy Committee

In organizations where IT provides significant business value, the board of directors should have an IT strategy committee. This group will advise the board of directors on strategies to enable better IT support of the organization's overall strategy and objectives.

The IT strategy committee can meet with the organization's top IT executives to impart the board's wishes directly to them. This works best as a two-way conversation, where IT executives can inform the strategy committee of their status on major initiatives, as well as on challenges and risks. This ongoing dialogue can take place as often as needed, usually once or twice per year.

Readers should note that this suggestion of the IT strategy committee communicating with IT management is not an attempt to circumvent communications through intermediate layers of management. Those individuals should be included in this conversation as well.

The Balanced Scorecard

The *balanced scorecard* (BSC) is a management tool that is used to measure the performance and effectiveness of an organization. The BSC is used to determine how well an organization can fulfill its mission and strategic objectives, and how well it is aligned with overall organizational objectives.

In the BSC, management defines key performance indicators in each of four perspectives:

- **Financial** Key financial items measured include the cost of strategic initiatives, support costs of key applications, and capital investment.
- **Customer** Key measurements include the satisfaction rate with various customer-facing aspects of the organization.
- **Internal processes** Measurements of key activities include the number of projects and the effectiveness of key internal workings of the organization.
- **Innovation and learning** Human-oriented measurements include turnover, illness, internal promotions, and training.

Each organization's BSC will represent a unique set of measurements that reflects the organization's type of business, business model, and style of management.

The BSC methodology of greatest interest to readers of this book is the standard IT balanced scorecard, discussed in the next section.

The Standard IT Balanced Scorecard

The BSC should be used to measure overall organizational effectiveness and progress. A similar scorecard, the standard IT balanced scorecard (IT-BSC), can be used specifically to measure IT organization performance and results.

Like the BSC, the standard IT-BSC has four perspectives:

- **Business contribution** Key indicators here are the perception of IT department effectiveness and value as seen from other (non-IT) corporate executives.
- **User** Key measurements include end-user satisfaction rate with IT systems and the IT support organization. Satisfaction rates of external users should be included if the IT department builds or supports externally facing applications or systems.
- **Operational excellence** Key measurements include the number of support cases, amount of unscheduled downtime, and defects reported.
- **Innovation** This includes the rate at which the IT organization utilizes newer technologies to increase IT value and the amount of training made available to IT staff.

The IT-BSC should flow directly out of the organization's overall BSC. This will ensure that IT will align itself with corporate objectives. Although the perspectives between the overall BSC and the IT-BSC vary, the approach for each is similar, and the results for the IT-BSC can "roll up" to the organization's overall BSC.

Information Security Governance

Security governance is the collection of management activities that establishes key roles and responsibilities, identifies and treats risks to key assets, and measures key security processes. Depending upon the structure of the organization and its business purpose, information security governance may be included in IT governance, or security governance may stand on its own (but if so, it should still be linked to IT governance so that these two activities are kept in sync). Security governance helps to align information security with business goals and objectives.

The main roles and responsibilities for security should be as follows:

- **Board of directors** The board is responsible for establishing the tone for risk appetite and risk management in the organization. To the extent that the board of directors establishes business and IT security, so, too, should the board consider risk and security in that strategy.