CISA®

Certified Information Systems Auditor

STUDY GUIDE

COVERS 2024-2029 EXAM OBJECTIVES

Includes interactive online learning environment and study tools:

2 custom practice exams

100 electronic flashcards

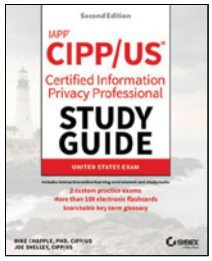
Searchable key term glossary

PETER H. GREGORY, CISA, CISSP

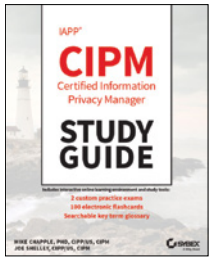
MIKE CHAPPLE, PH.D., CISA, CISSP

SYBEX®
A Wiley Brand

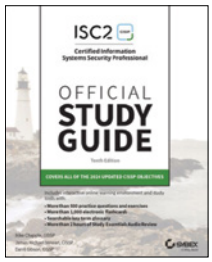
Other Information Security Study Guides from Sybex



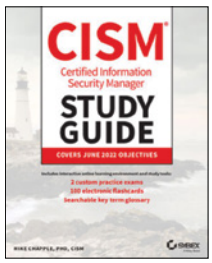
IAPP CIPP / US Certified Information Privacy Professional Study Guide, 2nd Edition — ISBN 978-1-394-28490-0, January 2025



IAPP CIPM Certified Information Privacy Manager Study Guide — ISBN 978-1-394-15380-0, January 2023



ISC2 CISSP Certified Information Systems Security Professional Official Study Guide, 10th Edition — ISBN 978-1-394-25469-9, June 2024



CISM Certified Information Security Manager Study Guide — ISBN 978-1-119-80193-1, May 2022

ISC2 CCSP Certified Cloud Security Professional Official Study Guide, 3rd Edition — ISBN 978-1-119-90937-8, October 2022

CISA®

Certified Information Systems Auditor

Study Guide

Covers 2024–2029 Exam Objectives

Peter H. Gregory, CISA, CISSP

Mike Chapple, Ph.D., CISA, CISSP

SYBEX®
A Wiley Brand

Some content was previously published in CISA Certified Information Systems Auditor All-in-One Exam Guide, Fourth Edition by Peter H. Gregory (© 2020 McGraw-Hill).

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394288380 (paperback), 9781394288403 (ePDF), 9781394288397 (ePub)

Library of Congress Control Number: 2024942279

Cover image: © Jeremy Woodhouse/Getty Images
Cover design: Wiley

To my grandchildren – may they grow up in a safer world.
—Peter
To my wife, Renee. We are a quarter century into this adventure together and yet we still find ourselves standing on the precipice of change. Here's to what's next!
—Mike

Acknowledgments

Books like this involve work from many people, and as authors, we truly appreciate the hard work and dedication that the team at Wiley shows. We would especially like to thank our acquisitions editor, Jim Minatel, who jumped through some incredible hoops to make this project possible.

We also greatly appreciated the editing and production team for the book, including Christine O'Connor, the managing editor, who brought years of experience and great talent to the project; Archana Pragash, the production editor who kept the train on the tracks, guided us through layouts, formatting, and final cleanup to produce a great book; Bobby Rogers and Jessica Chang, the technical editors, who provided insightful advice and gave wonderful feedback throughout the book. We would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who make the book and companion materials into a finished product.

Shahla Pirnia, Mike's technical editor at `CertMike.com`, was instrumental in helping us get all of the details straightened out as we prepared the manuscript.

Our agent, Carole Jelen of Waterside Productions, continues to provide us with wonderful opportunities, advice, and assistance throughout us writing career.

Finally, we would like to thank our families, who supported us through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

About the Authors

Peter H. Gregory, CISSP, CISM, CISA, CRISC, CIPM, CDPSE, CCSK, DRCE, A/CCRF, A/CCRP, is the author of more than 60 books on security and technology, including *Solaris Security* (Prentice Hall, 2000), *The Art of Writing Technical Books* (Waterside Productions, 2022), *CISM Certified Information Security Manager All-In-One Exam Guide* (McGraw-Hill, 2022), *Chromebook For Dummies* (Wiley, 2023), and *Elementary Information Security* (Jones & Bartlett Learning, 2024).

Peter is a career technologist and a security executive at a regional telecommunications provider. Before this, he held security leadership positions at Optiv Security (`www.optiv.com`) and Concur Technologies (`www.concur.com`). Peter is an advisory board member for the University of Washington and Seattle University for education programs in cybersecurity. He is a graduate of the FBI Citizens Academy.

Peter resides in Central Washington State and can be found at `www.peterhgregory.com`.

Mike Chapple, PhD, CISA, is the author of over 50 books, including the best-selling *ISC2 CISSP Certified Information Systems Security Professional Official Study Guide* (Sybex, 2024) and the *ISC2 CISSP Official Practice Tests* (Sybex, 2024). He is a cybersecurity professional with 25 years of experience in higher education, the private sector, and government.

Mike currently serves as Teaching Professor in the IT, Analytics, and Operations department at the University of Notre Dame's Mendoza College of Business, where he teaches undergraduate and graduate courses on cybersecurity, data management, and business analytics.

Mike previously served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active-duty intelligence officer in the U.S. Air Force.

Mike earned both his BS and PhD degrees from Notre Dame in computer science and engineering. Mike also holds an MS in computer science from the University of Idaho and an MBA from Auburn University. Mike holds the Certified Information Systems Auditor (CISA), Cybersecurity Analyst+ (CySA+), Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP) certifications.

Learn more about Mike and his other security certification materials at his website, `https://CertMike.com`.

About the Technical Editors

Bobby E. Rogers is a senior cybersecurity professional with over 30 years in the field. He serves as a cybersecurity auditor and virtual Chief Information Security Officer (vCISO) for a variety of clients. He works with a major engineering company in Huntsville, Alabama, helping to secure networks and manage cyber risk for its customers. In addition to numerous educational institutions, Bobby's customers have included the U.S. Army, NASA, the State of Tennessee, and private/commercial companies and organizations. Bobby's specialties are cybersecurity engineering, security compliance, and cyber risk management, but he has worked in almost every area of cybersecurity, including network defense, computer forensics and incident response, and penetration testing.

He has narrated and produced over 30 computer training videos for several training companies. He is the author of McGraw-Hill Education's "CompTIA CySA+ Cybersecurity Analyst Certification Passport (Exam CS0-002)," 1st Edition, "CISSP Passport," 1st Edition, coauthor of "Certified in Risk and Information Systems Control (CRISC) All-in-One Exam Guide," 1st and 2nd editions, and contributing author/ technical editor for the popular "CISSP All-in-One Exam Guide," (7th, 8th, and 9th editions).

Jessica Chang is a licensed CPA in the state of Colorado with over 15 years of public accounting and general accounting experience in multiple leadership roles. She has worked in various industries, from telecommunications, hospitality, real estate, and e-commerce and has served as the chief audit executive for multiple companies.

Contents at a Glance

Contents

Introduction

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 200,000 professionals worldwide reached the same conclusion and have earned this well-respected certification. Welcome to the journey and the amazing opportunities that await you.

We have put together this information to help you understand the commitment needed, prepare for the exam, and maintain your certification. Not only is it our wish that you prepare for and pass the exam with flying colors, but we 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 180,000 professionals in more than 188 countries. ISACA administers several exam certifications, including:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Data Privacy Solutions Engineer (CDPSE)
- Certified in Governance of Enterprise IT (CGEIT)
- Certified Cybersecurity Operations Analyst (CCOA)

The certification program has been accredited under 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, we recommend that you tour the organization's website (`www.isaca.org`) and become familiar with the guides and resources available. In addition, if you're near one of the 225 local ISACA chapters in 99 countries worldwide, consider 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 their ability to conduct formal IS audits. Organizations seek qualified personnel for assistance with developing and maintaining strong control environments. A CISA-certified individual is a great candidate for these positions.

If you're preparing to take the CISA exam, you'll undoubtedly want to find as much information as you can about information systems and auditing. The more information you have at your disposal, the better off you'll be when attempting the exam. This study guide was written with that in mind. The goal was to provide enough information to prepare you for the test, but not so much that you'll be overloaded with information that's outside the scope of the exam.

This book presents the material at an intermediate technical level. Experience with and knowledge of security and auditing concepts will help you get a full understanding of the challenges you'll face as an information systems auditor.

We've included review questions at the end of each chapter to give you a taste of what it's like to take the exam. We recommend that you check out these questions first to gauge your level of expertise. You can then use the book mainly to fill in the gaps in your current knowledge. This study guide will help you round out your knowledge base before tackling the exam.

If you can answer 80 percent or more of the review questions correctly for a given chapter, you can feel safe moving on to the next chapter. If you're unable to answer that many correctly, reread the chapter and try the questions again. Your score should improve.

Don't just study the questions and answers! The questions on the actual exam will be different from the practice questions included in this book. The exam is designed to test your knowledge of a concept or objective, so use this book to learn the objectives behind the questions.

The CISA Exam

The CISA exam is designed to be a vendor-neutral certification for information systems auditors. ISACA recommends this certification for those who already have experience in auditing and want to demonstrate that experience to current and future employers.

The exam covers five major domains:

1. Information Systems Auditing Process
2. Governance and Management of IT
3. Information Systems Acquisition, Development and Implementation
4. Information Systems Operations and Business Resilience
5. Protection of Information Assets

These five areas include a range of topics, from enterprise risk management to evaluating cybersecurity controls. They focus heavily on scenario-based learning and the role of the information systems auditor in various scenarios. There's a lot of information that you'll need to learn, but you'll be well rewarded for possessing this credential. ISACA reports that the average salary of CISA credential holders is over $145,000.

The CISA exam includes only standard multiple-choice questions. Each question has four possible answer choices and only one of those answer choices is the correct answer. When you're taking the test, you'll likely find some questions where you think multiple answers might be correct. In those cases, remember that you're looking for the *best* possible answer to the question!

The exam costs $575 for ISACA members and $760 for non-members. More details about the CISA exam and how to take it can be found at:

`www.isaca.org/credentialing/cisa`

You'll have four hours to take the exam and will be asked to answer 150 questions during that time period. Your exam will be scored on a scale ranging from 200 to 800, with a passing score of 450.

ISACA frequently does what is called *item seeding*, which is the practice of including unscored questions on exams. It does so to gather psychometric data, which is then used when developing new versions of the exam. Before you take the exam, you will be told that your exam may include these unscored questions. So, if you come across a question that does not appear to map to any of the exam objectives—or for that matter, does not appear to belong in the exam—it is likely a seeded question. You never really know whether or not a question is seeded, however, so always make your best effort to answer every question.

Taking the Exam

Once you are fully prepared to take the exam, you can visit the ISACA website to register. Currently, ISACA offers two options for taking the exam: an in-person exam at a testing center and an at-home exam that you take on your own computer through a remote proctoring service.

In-Person Exams

ISACA partners with PSI Exams testing centers, so your next step will be to locate a testing center near you. In the United States, you can do this based on your address or your zip code, while non-U.S. test takers may find it easier to enter their city and country. You can search for a test center near you at the PSI Exams website:

`https://home.psiexams.com/#/test-center?p=Z97SE74H`

Now that you know where you'd like to take the exam, simply set up a PSI testing account and schedule an exam on their site.

On the day of the test, bring a government-issued identification card or passport that contains your full name (exactly matching the name on your exam registration), your signature, and your photograph. Make sure to show up with plenty of time before the exam starts. Remember that you will not be able to take your notes, electronic devices (including smartphones and watches), or other materials in with you.

At-Home Exams

ISACA also offers online exam proctoring. Candidates using this approach will take the exam at their home or office and be proctored over a webcam by a remote proctor.

Due to the rapidly changing nature of the at-home testing experience, candidates wishing to pursue this option should check the ISACA website for the latest details.

After the CISA Exam

Once you have taken the exam, you will be notified of your score immediately, so you'll know if you passed the test right away. You should keep track of your score report with your exam registration records and the email address you used to register for the exam.

Meeting the Experience Requirement

The CISA program is designed to demonstrate that an individual is a qualified information systems auditor. That requires more than just passing a test—it also requires real hands-on work experience.

The basic CISA work experience requirement is that you must have five years of work experience in information systems auditing, controls, assurance, or security. If the work you do aligns with any of the job practice statements found later in this introduction, that experience likely qualifies.

If you're a current information systems auditor or cybersecurity professional, you may find it easy to meet these requirements. If you don't yet meet the experience requirement, you may still take the exam and then you'll have five years to gain the experience and become fully certified after passing the test.

There are some waivers available that can knock 1, 2, or 3 years off your experience requirement:

- If you hold an associate's degree in any field, you qualify for a 1-year waiver.
- If you hold a bachelor's, master's, or doctoral degree in any field, you qualify for a 2-year waiver.
- If you hold a master's degree in information systems or a related field, you qualify for a 3-year waiver.
- If you hold full certification from the Chartered Institute of Management Accountants (CIMA), you qualify for a 2-year waiver.
- If you are a member of the Association of Chartered Certified Accountants (ACCA), you qualify for a 2-year waiver.

These waivers may not be combined. You may only use *one* of these waiver options against your certification requirements.

You must have earned all of the experience used toward your requirement within the 10 years preceding your application or within 5 years of the date you pass the exam.

Maintaining Your Certification

Information systems auditing is a constantly evolving field with new threats and controls arising regularly. All CISA holders must complete continuing professional education on an annual basis to keep their knowledge current and their skills sharp. The guidelines around continuing professional education are somewhat complicated, but they boil down to two main requirements:

- You must complete 120 hours of credit every three years to remain certified.
- You must have a minimum of 20 hours of credit every year during that cycle.

You must meet both of these requirements. For example, if you earn 120 credit hours during the first year of your certification cycle, you still must earn 20 additional credits in each of the next 2 years.

Continuing education requirements follow calendar years, and your clock will begin ticking on January 1 of the year after you earn your certification. You are allowed to begin earning credits immediately after you're certified. They'll just count for the next year.

There are many acceptable ways to earn CPE credits, many of which do not require travel or attending a training seminar. The important requirement is that you generally do not earn CPEs for work that you perform as part of your regular job. CPEs are intended to cover professional development opportunities outside of your day-to-day work. You can earn CPEs in several ways:

- Attending conferences
- Attending training programs
- Attending professional meetings and activities
- Taking self-study courses
- Participating in vendor marketing presentations
- Teaching, lecturing, or presenting
- Publishing articles, monographs, or books
- Participating in the exam development process
- Volunteering with ISACA
- Earning other professional credentials
- Contributing to the profession
- Mentoring

For more information on the activities that qualify for CPE credits, visit this site:

`www.isaca.org/credentialing/how-to-earn-cpe`

Study Guide Elements

This study guide uses a number of common elements to help you prepare. These include the following:

Summaries The Summary section of each chapter briefly explains the chapter, allowing you to easily understand what it covers.

Exam Essentials The Exam Essentials focus on major exam topics and critical knowledge that you should take in to the test. The Exam Essentials focus on the exam objectives provided by ISACA.

Chapter Review Questions A set of questions at the end of each chapter will help you assess your knowledge and if you are ready to take the exam based on your knowledge of that chapter's topics.

Additional Study Tools

This book comes with a number of additional study tools to help you prepare for the exam. They include the following.

Go to `www.wiley.com/go/Sybextestprep` to register and gain access to this interactive online learning environment and test bank with study tools.

Sybex Test Preparation Software

Sybex's test preparation software lets you prepare with electronic test versions of the review questions from each chapter, the practice exam, and the bonus exam that are included in this book. You can build and take tests on specific domains, by chapter, or cover the entire set of CISA exam objectives using randomized tests.

Electronic Flashcards

Our electronic flashcards are designed to help you prepare for the exam. Over 100 flashcards will ensure that you know critical terms and concepts.

Glossary of Terms

Sybex provides a full glossary of terms in PDF format, allowing quick searches and easy reference to materials in this book.

Bonus Practice Exams

In addition to the practice questions for each chapter, this book includes two full 150-question practice exams. We recommend that you use them both to test your preparedness for the certification exam.