CISM®

Certified Information Security Manager

STUDY GUIDE

COVERS JUNE 2022 OBJECTIVES

Includes interactive online learning environment and study tools:

2 custom practice exams

100 electronic flashcards

Searchable key term glossary

MIKE CHAPPLE, PHD, CISM

SYBEX®
A Wiley Brand

CISM®

Certified Information Security Manager

Study Guide

Mike Chapple, PhD, CISM

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

978-1-119-80193-1
978-1-119-80204-4 (ebk.)
978-1-119-80194-8 (ebk.)

Library of Congress Control Number: 2021948030

Cover image: ©Jeremy Woodhouse/Getty Images

Cover design: Wiley

To my wife, Renee. We are 22 years into this adventure together and every moment is better than the last. Here's to what's next!
—Mike

Acknowledgments

Books like this involve work from many people, and as an author, I truly appreciate the hard work and dedication that the team at Wiley shows. I would especially like to thank my acquisitions editor, Jim Minatel. I've worked with Jim for too many years to count and it's always an absolute pleasure working with a true industry pro.

I also greatly appreciated the editing and production team for the book, including David Clark, the project editor, who brought years of experience and great talent to the project; Ben Malisow, the technical editor, who provided insightful advice and gave wonderful feedback throughout the book; and Barath Kumar Rajasekaran, the production editor, who guided me through layouts, formatting, and final cleanup to produce a great book. I 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.

Victoria Mastagh, my production assistant at `CertMike.com`, was instrumental in preparing the glossary, and Matthew Howard, my research assistant at Notre Dame, played a crucial role in pulling together the class slides that accompany the book for instructors.

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

Finally, I would like to thank my family, who supported me through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

About the Author

Mike Chapple, Ph.D., CISM, is the author of over 30 books, including the best-selling *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide* (Sybex, 2021) and the *CISSP (ISC)² Official Practice Tests* (Sybex, 2021). He is an information security professional with two decades 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 is a technical editor for *Information Security Magazine* and has written more than 25 books. He earned both his B.S. and Ph.D. degrees from Notre Dame in computer science and engineering. Mike also holds an M.S. in computer science from the University of Idaho and an MBA from Auburn University. Mike holds the 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, `CertMike.com`.

About the Technical Editor

Ben Malisow has worked in the fields of education/training, communication, information technology, security, and/or some combination of these industries, for over 25 years. Prior to his current position, Ben has provided information security consulting services and training to a diverse host of clients, including the Defense Advanced Research Projects Agency (DARPA), the Department of Homeland Security (at TSA), and the FBI. He has also served as an Air Force officer, after graduating from the Air Force Academy.

An experienced trainer, Ben has been an adjunct professor of English at the College of Southern Nevada, a computer teacher for troubled junior/senior high school students in Las Vegas, a senior instructor for the University of Texas - San Antonio, and he has taught computer security certification prep classes for Carnegie-Mellon University's CERT/SEI.

Ben has published widely in many fields. His latest books include *Exposed: How Revealing Your Data and Eliminating Privacy Increases Trust and Liberates Humanity* (Wiley, 2020), the *CCSP (ISC)² Official Study Guide* (Sybex, 2020), the *CCSP Official (ISC)² Practice Tests* (Sybex, 2018), and *How to Pass Your INFOSEC Exam* from Amazon Direct. Updates to his work and his podcast, "The Sensuous Sounds of INFOSEC," can be found at `securityzed.com`. His certification-preparation courses can be found on `Udemy.com`.

Contents at a Glance

Contents

Introduction

If you're preparing to take the Certified Information Security Manager (CISM) exam, you'll undoubtedly want to find as much information as you can about information security and the art of leading and managing security teams. The more information you have at your disposal, the better off you'll be when taking 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 concepts, operating systems, and application systems will help you get a full understanding of the challenges you'll face as a security manager.

I've included review questions at the end of each chapter to give you a taste of what it's like to take the exam. I 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 90 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 CISM Exam

The CISM exam is designed to be a vendor-neutral certification for cybersecurity managers. ISACA recommends this certification for those who already have technical experience in the information security field and are either already serving in management roles or who want to shift from being an individual contributor into a management role.

The exam covers four major domains:

1. Information Security Governance
2. Information Security Risk Management
3. Information Security Program
4. Incident Management

These four areas include a range of topics, from enterprise risk management to responding to cybersecurity incidents. They focus heavily on scenario-based learning and the role

of the information security manager 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 CISM credential holders is over $118,000.

The CISM 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 nonmembers. More details about the CISM exam and how to take it can be found at:

`www.isaca.org/credentialing/cism`

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://isacaavailability.psiexams.com`

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 began offering online exam proctoring in 2020 in response to the coronavirus pandemic. When this book went to press, the at-home testing option was still available and appears likely to continue. 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. In fact, checking the ISACA website for exam policy changes is a good idea for all test takers.

After the CISM 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 CISM program is designed to demonstrate that an individual is a qualified information security manager. That requires more than just passing a test—it also requires real hands-on work experience managing cybersecurity teams.

The CISM work experience requirement has two different components:

- You must have five years of information security work experience.
- You must have at least three years of information security management work experience. That work experience must come from at least three of the four CISM domains.

If you're a current information security manager, you may find it easy to meet these requirements. If you've been in the field for five years and have been a manager for at least three of those years, you're probably good to go because your time as an information security manager also counts toward your general information security experience requirement.

There are some waivers available that can knock one or two years off your experience requirement. All of these waivers apply only to the general information security work experience requirement, not the management requirement.

If you hold any of the following credentials, you qualify for a two-year reduction in the experience requirement:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Master of Business Administration (MBA) degree
- Master's degree in information security or a related field

One year experience requirement waivers are available for holders of:

- Skill-based or general security certifications (such as the CompTIA Security+ credential)
- Bachelor's degree in information security or a related field
- One full year of general information systems management experience
- One full year of general security management experience

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 security is a constantly evolving field with new threats and controls arising regularly. All CISM 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 two 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 several 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 into 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 some 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 CISM exam objectives using randomized tests.

Audio Reviews

The author of this book recorded files containing the exam essentials for each chapter in a convenient audio form. Use these audio reviews in the car, on the train, when you're out for a run, or whenever you have a few minutes to review what you've learned.

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.

Like all exams, the CISM certification from ISACA is updated periodically and may eventually be retired or replaced. At some point after ISACA is no longer offering this exam, the old editions of our books and online tools will be retired. If you have purchased this book after the exam was retired, or are attempting to register in the Sybex online learning environment after the exam was retired, please know that we make no guarantees that this exam's online Sybex tools will be available once the exam is no longer available.

CISM Exam Objectives

ISACA publishes relative weightings for each of the exam's objectives. The following table lists the four CISM domains and the extent to which they are represented on the exam.

Domain	% of Exam
1. Information Security Governance	17%
2. Information Security Risk Management	20%
3. Information Security Program	33%
4. Incident Management	30%

CISM Certification Exam Objective Map

The CISM exam covers two different types of objectives: topics and supporting tasks. I recommend that instead of focusing on these objectives in the order they appear in the exam objectives that you instead learn them in the order they are presented in this book. In my 25 years of experience teaching information security topics, I've found that approaching these topics in a more logical order will better prepare you for the exam.

If you're looking for where I've covered a specific objective in the book, use the following two tables to find the appropriate chapter.

Topic Mapping

Topic	Chapter(s)
Domain 1: Information Security Governance	
A. Enterprise Governance	**1,2**
1A1. Organizational Culture	1
1A2. Legal, Regulatory, and Contractual Requirements	2
1A3. Organizational Structures, Roles, and Responsibilities	1
B. Information Security Strategy	**1,2**
1B1. Information Security Strategy Development	1
1B2. Information Governance Frameworks and Standards	2
1B3. Strategic Planning (e.g., budgets, resources, business case)	2
Domain 2: Information Security Risk Management	
A. Information Security Risk Assessment	**3,4,6**
2A1. Emerging Risk and Threat Landscape	4
2A2. Vulnerability and Control Deficiency Analysis	6
2A3. Risk Assessment and Analysis	3
B. Information Security Risk Response	**3**
2B1. Risk Treatment/Risk Response Options	3
2B2. Risk and Control Ownership	3
2B3. Risk Monitoring and Reporting	3
Domain 3: Information Security Program	
A. Information Security Program Development	**2,3,5**
3A1. Information Security Program Resources (e.g., people, tools, technologies)	5
3A2. Information Asset Identification and Classification	3
3A3. Industry Standards and Frameworks for Information Security	2
3A4. Information Security Policies, Procedures, and Guidelines	2
3A5. Information Security Program Metrics	5

Topic	Chapter(s)
B. Information Security Program Management	**5,6,7**
3B1. Information Security Control Design and Selection	7
3B2. Information Security Control Implementation and Integrations	7
3B3. Information Security Control Testing and Evaluation	6
3B4. Information Security Awareness and Training	5
3B5. Management of External Services (e.g., providers, suppliers, third parties, fourth parties)	5
3B6. Information Security Program Communications and Reporting	5
Domain 4: Incident Management	
A. Incident Management Readiness	**8,9**
4A1. Incident Response Plan	8
4A2. Business Impact Analysis (BIA)	9
4A3. Business Continuity Plan (BCP)	9
4A4. Disaster Recovery Plan (DRP)	9
4A5. Incident Classification/Categorization	8
4A6. Incident Management Training, Testing, and Evaluation	8
B. Incident Management Operations	**8**
4B1. Incident Management Tools and Techniques	8
4B2. Incident Investigation and Evaluation	8
4B3. Incident Containment Methods	8
4B4. Incident Response Communications (e.g., reporting, notification, escalation)	8
4B5. Incident Eradication and Recovery	8
4B6. Post-incident Review Practices	8