CC℠ Certified in Cybersecurity

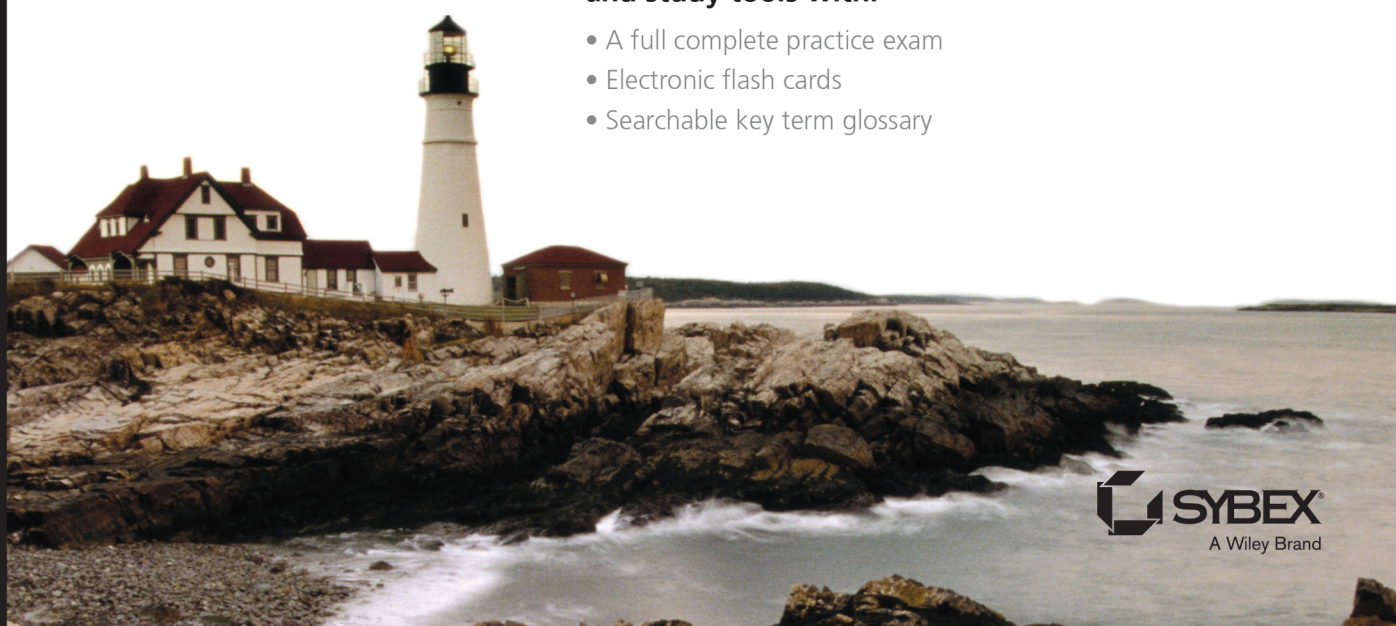
Study Guide

Mike Chapple, CISSP, CCSP

FULL COLOR easy to follow coverage of ALL objectives for the Certified in Cybersecurity credential to get you ready for a new career in cybersecurity FAST!

Includes interactive online learning environment and study tools with:

- A full complete practice exam
- Electronic flash cards
- Searchable key term glossary



SYBEX®
A Wiley Brand

CC℠ Certified in Cybersecurity Study Guide

CC℠ Certified in Cybersecurity
Study Guide

Mike Chapple, CISSP, CCSP

SYBEX®
A Wiley Brand

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

ISBNs: 9781394213832 (paperback), 9781394213863 (ePDF), 9781394213849 (ePub)

Library of Congress Control Number: 2023948599

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

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 appreciate the editing and production team for the book, including Kelly Talbot, the project editor, who brought years of experience and great talent to the project; and Shahla Pirnia, the technical editor, who provided insightful advice and gave wonderful feedback throughout the 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.

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, CISSP, CCSP, is an author of the best-selling *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide* (Sybex, 2021), now in its ninth edition. He is an information security professional with 25 years of experience in higher education, the private sector, and government.

Mike currently serves as Teaching Professor of IT, Analytics, and Operations at the University of Notre Dame's Mendoza College of Business. He previously served as Senior Director for IT Service Delivery at Notre Dame, where he oversaw the information security, data governance, IT architecture, project management, strategic planning, and product management functions for the university.

Before returning to Notre Dame, Mike 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.

He is a technical editor for *Information Security Magazine* and has written more than 30 books, including *Cyberwarfare: Information Operations in a Connected World* (Jones & Bartlett, 2022), *ISC2 CISSP Official Study Guide* (Wiley, 2021), and *CompTIA Cybersecurity Analyst+ (CySA+) Study Guide* (Wiley, 2023) and *Practice Tests* (Wiley, 2023).

Mike earned both his BS and PhD degrees from Notre Dame in computer science and engineering. He also holds an MS in computer science from the University of Idaho and an MBA from Auburn University. His IT certifications include the CC, CISSP, Security+, CySA+, CISA, PenTest+, CIPP/US, CISM, CCSP, and PMP credentials.

Mike provides books, video-based training, and free study groups for a wide variety of IT certifications at his website, `CertMike.com`.

About the Technical Editor

Shahla Pirnia is a freelance technical editor and proofreader with a focus on cybersecurity and certification topics.

Starting her career at Montgomery College's computer labs, Shahla quickly acquired a foundational grasp of technology in her role as a Student Aide. This foundational experience set the stage for subsequent roles: She managed a childcare provider database for a referral agency for 5 years, and then spent 9 years with a document conversion bureau. Shahla later ventured into clerical temp roles via a staffing agency and freelance writing for a digital content company.

Shahla currently serves as a technical editor for `CertMike.com`, where she works on projects including books, video courses, and practice tests.

Shahla earned BS degrees in computer and information science and psychology from the University of Maryland Global Campus, coupled with an AA degree in information systems from Montgomery College, Maryland. Shahla's IT certifications include the ISC2 Certified in Cybersecurity and the CompTIA Security+, Network+, and A+ credentials.

Contents at a Glance

Contents

Introduction

If you're preparing to take the Certified in Cybersecurity (CC) exam, you'll undoubtedly want to find as much information as you can about information security. 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 is 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 entry level. You don't need any prior experience with cybersecurity to read this book or take the exam. The CC certification is designed for newcomers to the field, and this book will give you all the information you need to know to pass it.

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 the review questions correctly for a given chapter, you can feel safe moving on to the next chapter. If you're unable to answer them correctly, reread the chapter and try the questions again. Your score should improve.

NOTE

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.

CC CERTIFICATION

The CC certification is offered by the International Information System Security Certification Consortium, or ISC2, a global nonprofit organization. The mission of ISC2 is to support and provide members and constituents with credentials, resources, and leadership to address cyber, information, software, and infrastructure security to deliver value to society. ISC2 achieves this mission by delivering the world's leading information security certification program. The CC is the flagship credential in this series and is accompanied by several other ISC2 programs:

- Certified Information Systems Security Professional (CISSP)
- Systems Security Certified Practitioner (SSCP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certified Cloud Security Professional (CCSP)
- Certified in Governance, Risk, and Compliance (CGRC)

The CC certification covers five domains of information security knowledge. These domains are meant to serve as the broad knowledge foundation required to succeed in the information security profession:

- Security Principles (26% of exam questions)
- Business Continuity (BC), Disaster Recovery (DR) & Incident Response (IR) Concepts (10% of exam questions)
- Access Control Concepts (22% of exam questions)
- Network Security (24% of exam questions)
- Security Operations (18% of exam questions)

Complete details about the CC exam objectives are contained in the Exam Outline. It includes a full outline of exam topics and can be found on the ISC2 website at www.isc2.org/Certifications/cc/cc-certification-exam-outline.

TAKING THE CC EXAM

The CC exam includes only standard multiple-choice questions. Each question has four possible answers, and only one of the answers is correct. When 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 CC exam is currently available for free to the first one million candidates through an ISC2 initiative called One Million Certified in Cybersecurity. You can find more details about the CC exam and how to take it at www.isc2.org/Certifications/CC.

You'll have 2 hours to take the exam and will be asked to answer 100 questions. Your exam will be scored on a scale of 1,000 possible points, with a passing score of 700.

NOTE

The CC exam includes 25 unscored questions, meaning that only 75 of the questions actually count toward your score. ISC2 does this to gather research data, which it then uses when developing new versions of the exam. 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.

COMPUTER-BASED TESTING ENVIRONMENT

The CC exam is administered in a computer-based testing (CBT) format. You can register for the exam through the ISC2 and Pearson VUE websites.

You take the exam in a Pearson VUE testing center located near your home or office. The centers administer many different exams, so you may find yourself sitting in the same room as a student taking a school entrance examination and a health care professional earning a medical certification. If you'd like to become more familiar with the testing environment, the Pearson VUE website offers a virtual tour of a testing center at `home.pearsonvue.com/test-taker/Pearson-Professional-Center-Tour.aspx`.

When you take the exam, you'll be seated at a computer that has the exam software already loaded and running. It's a pretty straightforward interface that allows you to navigate through the exam. You can download a practice exam and tutorial from the Pearson VUE website at `www.vue.com/athena/athena.asp`.

EXAM TIP

At the beginning of the exam, you'll be asked to agree to the terms. This section of the exam has its own 5-minute timer. If you don't agree within 5 minutes, your exam will automatically end and you will not be able to restart it!

EXAM RETAKE POLICY

If you don't pass the CC exam, you shouldn't panic. Many individuals don't reach the bar on their first attempt but gain valuable experience that helps them succeed the second time around. When retaking the exam, you'll have the benefit of familiarity with the CBT environment and CC exam format. You'll also have time to study the areas where you felt less confident.

After your first exam attempt, you must wait 30 days before retaking it. If you're not successful on that attempt, you must then wait 60 days before your third attempt and 90 days before your fourth attempt. You cannot take the exam more than three times in a single calendar year.

RECERTIFICATION REQUIREMENTS

Once you've earned your CC credential, you'll need to maintain your certification by paying maintenance fees and participating in continuing professional education (CPE). As long as you maintain your certification in good standing, you will not need to retake the CC exam.

Currently, the annual maintenance fee for the CC credential is $50 for those who do not hold another ISC2 certification. Members who hold another credential pay a $125 maintenance fee each year. This fee covers the renewal for all ISC2 certifications held by an individual.

The CC CPE requirement mandates earning at least 45 CPE credits during each three-year renewal cycle. ISC2 provides an online portal where certificate holders can submit CPE completion for review and approval. The portal also tracks annual maintenance fee payments and progress toward recertification.

USING THE ONLINE PRACTICE TEST

All the questions in this book are also available in Sybex's online practice test tool, along with a full-length 100-question CC practice test. To get access to this online format, go to `www.wiley.com/go/sybextestprep` and start by registering your book. You'll receive a PIN code and instructions on where to create an online test bank account. Once you have access, you can use the online version to create your own sets of practice tests from the book questions and practice in a timed and graded setting.

In addition to the questions and practice test, the Sybex online learning environment includes an extensive set of electronic flashcards to improve your exam preparation. Each flashcard has one question and one correct answer. These are great as last minute drills. And there is an online glossary is a searchable list of key terms introduced in this study guide that you should know for the CC certification exam.

HOW TO CONTACT THE PUBLISHER

If you believe you have found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

PART I

Domain 1: Security Principles

Security Principles is the first domain of ISC2's Certified in Cybersecurity exam. It provides the foundational knowledge that anyone in information technology needs to understand as they begin their careers. The domain includes the following five objectives:

1.1 Understand the security concepts of information assurance
1.2 Understand the risk management process
1.3 Understand security controls
1.4 Understand the ISC2 Code of Ethics
1.5 Understand governance processes

Questions from this domain make up 26 percent of the questions on the CC exam, so you should expect to see 26 questions on your test covering the material in this part.

CHAPTER 1

Confidentiality, Integrity, Availability, and Non-repudiation

Objective 1.1 Understand the Security Concepts of Information Assurance

Information plays a vital role in the operations of modern business, and we find ourselves entrusted with sensitive information about our customers, employees, internal operations, and other critical matters. As information technology professionals, we must work with information security teams, other technology professionals, and business leaders to protect the security of that information.

In this chapter, you'll learn about four of the subobjectives of CC objective 1.1. The remaining material for this objective is covered in Chapter 2, "Authentication and Authorization," and Chapter 3, "Privacy." The following subobjectives are covered in this chapter:

- **Confidentiality**
- **Integrity**
- **Availability**
- **Non-repudiation**