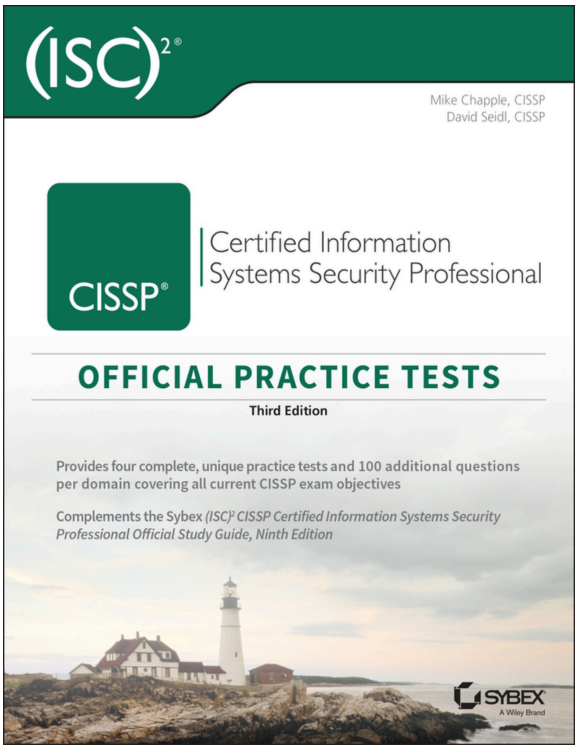



ebookbig.com

or scan the QR code to access the digital study portal.

# Acknowledgments

The authors would like to thank the many people who made this book possible. Jim Minatel at Wiley Publishing helped us extend the Sybex CISSP franchise to include this title and has continued to champion with the International Information Systems Security Certification Consortium $(ISC)^2$. Carole Jelen, our agent, tackles all the back-end magic for our writing efforts and worked on both the logistical details and the business side of the book with her usual grace and commitment to excellence. Ben Malisow and Jerry Rayome, our technical editors, pointed out many opportunities to improve our work and deliver a high-quality final product. Caroline Define served as our project manager and made sure everything fit together. Many other people we'll never meet worked behind the scenes to make this book a success, and we really appreciate their time and talents to make this next edition come together.

# About the Authors

**Mike Chapple, PhD, CISSP,** 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 two decades 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 20 books, including *Cyberwarfare: Information Operations in a Connected World* (Jones & Bartlett, 2015), *CompTIA Security+ Training Kit* (Microsoft Press, 2013), and *CompTIA Cybersecurity Analyst+ (CySA+) Study Guide* (Wiley, 2017) and *Practice Tests* (Wiley, 2018).

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 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`.

**David Seidl, CISSP,** is Vice President for Information Technology and CIO at Miami University. During his IT career, he has served in a variety of

technical and information security roles including serving at the Senior Director for Campus Technology Services at the University of Notre Dame where he co-led Notre Dame's move to the cloud, and oversaw cloud operations, ERP, databases, identity management, and a broad range of other technologies and service. He also served as Notre Dame's Director of Information Security and led Notre Dame's information security program. He has taught information security and networking undergraduate courses as an instructor for Notre Dame's Mendoza College of Business and has written books on security certification and cyberwarfare, including co-authoring the previous editions of *CISSP (ISC)*$^2$ *Official Practice Tests* (Sybex 2018) as well as *CompTIA CySA+ Study Guide: Exam CS0-002*, *CompTIA CySA+ Practice Tests: Exam CS0-002*, *CompTIA Security+ Study Guide: Exam SY0-601*, and *CompTIA Security+ Practice Tests: Exam SY0-601* as well as other certification guides and books on information security.

David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University, as well as CISSP, CySA+, Pentest+, GPEN, and GCIH certifications.

# About the Technical Editors

**Ben Malisow** is a consultant and writer with more than 25 years of experience in the fields of information, security, and information security. He teaches SSCP, CISSP, and CCSP preparation courses for (ISC)2 and has written the *Official (ISC)2 CCSP Study Guide* and the *Official (ISC)2 Practice Tests* books, among other titles; his latest works include *CCSK Practice Tests* and *Exposed: How Revealing Your Data and Eliminating Privacy Increases Trust and Liberates Humanity*. He and his partner Robin Cabe host the weekly podcast, "The Sensuous Sounds of INFOSEC," from his website www.securityzed.com.

**Jerry Rayome,** BS/MS Computer Science, CISSP, employed as a member of the Cyber Security Program at Lawrence Livermore National Laboratory for over 20 years providing cyber security services that include software development, penetrative testing, incident response, firewall implementation/administration, firewall auditing, honey net deployment/monitoring, cyber forensic investigations, NIST 900-53 control implementation/assessment, cloud risk assessment, and cloud security auditing.

# Introduction

*(ISC)*$^2$ ® *CISSP* ® *Certified Information Systems Security Professional Official Practice Tests* is a companion volume to *(ISC)*$^2$ *CISSP Certified Information Systems Security Professional Official Study Guide*. It includes questions that cover content from the CISSP Detailed Content Outline and exam that became effective on May 1, 2021. If you're looking to test your knowledge before you take the CISSP exam, this book will help you by providing more than 1,300 questions that cover the CISSP Common Body of Knowledge and easy-to-understand explanations of both right and wrong answers.

If you're just starting to prepare for the CISSP exam, we highly recommend that you use *(ISC)*$^2$ *CISSP Certified Information Systems Security Professional Official Study Guide* to help you learn about each of the domains covered by the CISSP exam. Once you're ready to test your knowledge, use this book to help find places where you may need to study more or to practice for the exam itself.

Since this is a companion to *CISSP Study Guide*, this book is designed to be similar to taking the CISSP exam. It contains multipart scenarios as well as standard multiple-choice and matching questions similar to those you may encounter on the certification exam. The book is broken up into 12 chapters: 8 domain-centric chapters with 100 or more questions about each domain, and 4 chapters that contain 125-question practice tests to simulate taking the exam.

# CISSP Certification

The CISSP certification is offered by the International Information System Security Certification Consortium, or (ISC)$^2$, a global nonprofit organization. The mission of (ISC)$^2$ 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. (ISC)$^2$ achieves this mission by delivering the world's leading information

security certification program, the CISSP. (ISC)2 also offered five additional certifications including: (ISC)2 also offered five additional certifications including:

- Systems Security Certified Practitioner (SSCP)
- Certified Authorization Professional (CAP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- HealthCare Information Security and Privacy Practitioner (HCISPP)
- Certified Cloud Security Professional (CSP)

There are also three advanced CISSP certifications for those who want to move on from the base credential to demonstrate advanced expertise in a domain of information security.

- Information Systems Security Architecture Professional (CISSP-ISSAP)
- Information Systems Security Engineering Professional (CISSP-ISSEP)
- Information Systems Security Management Professional (CISSP-ISSMP)

The CISSP certification covers eight 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 and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations

- Software Development Security

The CISSP domains are periodically updated by (ISC)$^2$. The most recent revision May 1, 2021 slightly modified the weighting for Communication and Network security from 14 percent to 13 percent while increasing the focus on Software Development Security from 10 percent to 11 percent. It also added or expanded coverage of topics such as the data management lifecycle, microservices, containerization, serverless computing, quantum computing, 5G networking, and modern security controls.

Complete details on the CISSP Common Body of Knowledge (CBK) are contained in the Exam Outline. It includes a full outline of exam topics, can be found on the (ISC)$^2$ website at www.isc2.org.

# Taking the CISSP Exam

The English version of the CISSP exam uses a technology called *computer adaptive testing* (CAT). With this format, you will face an exam containing between 100 to 150 questions with a three-hour time limit. You will not have the opportunity to skip back and forth because the computer selects the next questions that it asks you based upon your answers to previous questions. If you're doing well on the exam, it will get more difficult as you progress. Don't let that unnerve you!

Other versions of the exam in French, German, Brazilian Portuguese, Spanish, Japanese, Simplified Chinese, and Korean use a traditional linear format. The linear format exam includes 250 questions with a six-hour time limit. For either version of the exam, passing requires achieving a score of at least 700 out of 1,000 points. It's important to understand that this is a scaled score, meaning that not every question is worth the same number of points. Questions of differing difficulty may factor into your score more or less heavily, and adaptive exams adjust to the test taker.

That said, as you work through these practice exams, you might want to use 70 percent as a goal to help you get a sense of whether you're ready to sit for the actual exam. When you're ready, you can schedule an exam at a location near you through the (ISC)$^2$ website.

Questions on the CISSP exam are provided in both multiple-choice form and what (ISC)$^2$ calls *advanced innovative* questions, which are drag-and-drop and hotspot questions, both of which are offered in computer-based testing environments. Innovative questions are scored the same as traditional multiple-choice questions and have only one right answer.




(ISC)² exam policies are subject to change. Please be sure to check isc2.org for the current policies before you register and take the exam.

## Computer-Based Testing Environment

CISSP exams are now administered in a computer-based testing (CBT) format. You'll register for the exam through the Pearson Vue website and may take the exam in the language of your choice. It is offered in English, French, German, Portuguese, Spanish, Japanese, Simplified Chinese, Korean, and a visually impaired format.

You'll take the exam in a computer-based 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 healthcare 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.

`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.

`http://www.vue.com/athena/athena.asp`




At the time this book went to press, (ISC)$^2$ was conducting a pilot test of at-home computer-based exams for CISSP candidates in the United States. It is possible that this pilot will be extended to a permanent product and may become available in additional countries. Check the (ISC)$^2$ website for more information.

## Exam Retake Policy

If you don't pass the CISSP 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 you retake the exam, you'll have the benefit of familiarity with the CBT environment and CISSP 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 the computer-based exam. If you're not successful on that attempt, you may re-test after 60 days. If you don't pass after your third attempt, you can re-test after 90 days for that and any subsequent attempts. You can’t take the test more than 4 times within a single calendar year. You can obtain more information about (ISC)2 and its other certifications from its website at www.isc2.org.

## Work Experience Requirement

Candidates who want to earn the CISSP credential must not only pass the exam but also demonstrate that they have at least five years of work experience in the information security field. Your work experience must cover activities in at least two of the eight domains of the CISSP program and must be paid, full-time employment. Volunteer experiences or part-time duties are not acceptable to meet the CISSP experience requirement.