(ISC)²®

Mike Chapple, CISSP
David Seidl, CISSP

CISSP®

Certified Information Systems Security Professional

OFFICIAL PRACTICE TESTS

Third Edition

Provides four complete, unique practice tests and 100 additional questions per domain covering all current CISSP exam objectives

Complements the Sybex *(ISC)² CISSP Certified Information Systems Security Professional Official Study Guide, Ninth Edition*

SYBEX
A Wiley Brand

Table of Contents

(ISC)2®

CISSP® Certified Information Systems Security Professional

Official Practice Tests

Third Edition

Mike Chapple, CISSP

David Seidl, CISSP


SYBEX
A Wiley Brand

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

Published simultaneously in Canada and the United Kingdom

ISBN: 978-1-119-78763-1
ISBN: 978-1-119-79315-1 (ebk.)
ISBN: 978-1-119-78764-8 (ebk.)

Library of Congress Control Number: 2021935480

Cover image(s): © Getty Images Inc./Jeremy Woodhouse
Cover design: Wiley

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:

- 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 125 to 175 questions with a four-hour time limit as of June 1, 2022.

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.

You may be eligible to waive one of the five years of the work experience requirement based upon your educational achievements. If you hold a bachelor's degree or four-year equivalent, you may be eligible for a degree waiver that covers one of those years. Similarly, if you hold one of the information security certifications on the current $(ISC)^2$ credential waiver list (www.isc2.org/credential_waiver/default.aspx), you may also waive a year of the experience requirement. You may not combine these two programs. Holders of both a certification and an undergraduate degree must still demonstrate at least four years of experience.

If you haven't yet completed your work experience requirement, you may still attempt the CISSP exam. Individuals who pass the exam are designated Associates of $(ISC)^2$ and have six years to complete the work experience requirement.

Recertification Requirements

Once you've earned your CISSP 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 CISSP exam.

Currently, the annual maintenance fees for the CISSP credential are $125 per year. This fee covers the renewal for all $(ISC)^2$ certifications held by an individual.

The CISSP CPE requirement mandates earning at least 120 CPE credits during each three-year renewal cycle. Associates of $(ISC)^2$ must earn at least 15 CPE credits each year. $(ISC)^2$ provides an online portal where certificate holders may submit CPE completion for review and approval. The portal also tracks annual maintenance fee payments and progress toward recertification.

Using This Book to Practice

This book is composed of 12 chapters. Each of the first eight chapters covers a domain, with a variety of questions that can help you test your knowledge of real-world, scenario, and best-practice security knowledge. The final four chapters are complete practice exams that can serve as timed practice tests to help determine whether you're ready for the CISSP exam.

We recommend taking the first practice exam to help identify where you may need to spend more study time and then using the domain-specific chapters to test your domain knowledge where it is weak. Once you're ready, take the other practice exams to make sure you've covered all the material and are ready to attempt the CISSP exam.

Using the Online Practice Tests

All the questions in this book are also available in Sybex's online practice test tool. 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.

Chapter 1
Security and Risk Management (Domain 1)

SUBDOMAINS

1.1 Understand, adhere to, and promote professional ethics

1.2 Understand and apply security concepts

1.3 Evaluate and apply security governance principles

1.4 Determine compliance and other requirements

1.5 Understand legal and regulatory issues that pertain to information security in a holistic context

1.6 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

1.7 Develop, document, and implement security policy, standards, procedures, and guidelines

1.8 Identify, analyze, and prioritize Business Continuity (BC) requirements

1.9 Contribute to and enforce personnel security policies and procedures

1.10 Understand and apply risk management concepts

1.11 Understand and apply threat modeling concepts and methodologies

1.12 Apply Supply Chain Risk Management (SCRM) concepts

1.13 Establish and maintain a security awareness, education, and training program

1. Alyssa is responsible for her organization's security awareness program. She is concerned that changes in technology may make the content outdated. What control can she put in place to protect against this risk?

   A. Gamification

   B. Computer-based training

   C. Content reviews

   D. Live training

2. Gavin is creating a report to management on the results of his most recent risk assessment. In his report, he would like to identify the remaining level of risk to the organization after adopting security controls. What term best describes this current level of risk?

   A. Inherent risk

   B. Residual risk

   C. Control risk

   D. Mitigated risk

3. Francine is a security specialist for an online service provider in the United States. She recently received a claim from a copyright holder that a user is storing information on her service that violates the third party's copyright. What law governs the actions that Francine must take?

   A. Copyright Act

   B. Lanham Act

   C. Digital Millennium Copyright Act

   D. Gramm Leach Bliley Act

4. FlyAway Travel has offices in both the European Union (EU) and the United States and transfers personal information between those offices regularly. They have recently received a request from an EU customer requesting that their account be terminated. Under the General Data Protection Regulation (GDPR), which requirement for processing personal information states that individuals may request that their data no longer be disseminated or processed?

   A. The right to access

   B. Privacy by design

   C. The right to be forgotten

   D. The right of data portability

5. After conducting a qualitative risk assessment of her organization, Sally recommends purchasing cybersecurity breach insurance. What type of risk response behavior is she recommending?

   A. Accept

   B. Transfer

   C. Reduce

   D. Reject

6. Which one of the following elements of information is not considered personally identifiable information that would trigger most United States (U.S.) state data breach laws?

   A. Student identification number

   B. Social Security number

   C. Driver's license number

   D. Credit card number

7. Renee is speaking to her board of directors about their responsibilities to review cybersecurity controls. What rule requires that senior executives take personal responsibility for information security matters?

   A. Due diligence rule

   B. Personal liability rule

   C. Prudent man rule

   D. Due process rule

8. Henry recently assisted one of his co-workers in preparing for the CISSP exam. During this process, Henry disclosed confidential information about the content of the exam, in violation of Canon IV of the Code of Ethics: “Advance and protect the profession.” Who may bring ethics charges against Henry for this violation?

   A. Anyone may bring charges.

   B. Any certified or licensed professional may bring charges.

   C. Only Henry's employer may bring charges.

   D. Only the affected employee may bring charges.

9. Wanda is working with one of her organization's European Union business partners to facilitate the exchange of customer information. Wanda's organization is located in the United States. What would be the best method for Wanda to use to ensure GDPR compliance?

   A. Binding corporate rules

   B. Privacy Shield

   C. Standard contractual clauses

   D. Safe harbor

10. Yolanda is the chief privacy officer for a financial institution and is researching privacy requirements related to customer checking accounts. Which one of the following laws is most likely to apply to this situation?

    A. GLBA

    B. SOX

    C. HIPAA

    D. FERPA

11. Tim's organization recently received a contract to conduct sponsored research as a government contractor. What law now likely applies to the information systems involved in this contract?

    A. FISMA

    B. PCI DSS

    C. HIPAA

    D. GISRA

12. Chris is advising travelers from his organization who will be visiting many different countries overseas. He is concerned about compliance with export control laws. Which of the following technologies is most likely to trigger these regulations?

    A. Memory chips

    B. Office productivity applications

    C. Hard drives

    D. Encryption software

13. Bobbi is investigating a security incident and discovers that an attacker began with a normal user account but managed to exploit a system vulnerability to provide

that account with administrative rights. What type of attack took place under the STRIDE threat model?

A. Spoofing

B. Repudiation

C. Tampering

D. Elevation of privilege

14. You are completing your business continuity planning effort and have decided that you want to accept one of the risks. What should you do next?

A. Implement new security controls to reduce the risk level.

B. Design a disaster recovery plan.

C. Repeat the business impact assessment.

D. Document your decision-making process.

15. You are completing a review of the controls used to protect a media storage facility in your organization and would like to properly categorize each control that is currently in place. Which of the following control categories accurately describe a fence around a facility? (Select all that apply.)

A. Physical

B. Detective

C. Deterrent

D. Preventive

16. Tony is developing a business continuity plan and is having difficulty prioritizing resources because of the difficulty of combining information about tangible and intangible assets. What would be the most effective risk assessment approach for him to use?

A. Quantitative risk assessment

B. Qualitative risk assessment

C. Neither quantitative nor qualitative risk assessment

D. Combination of quantitative and qualitative risk assessment

17. Vincent believes that a former employee took trade secret information from his firm and brought it with him to a competitor. He wants to pursue legal action. Under what law could he pursue charges?

A. Copyright law

B. Lanham Act

C. Glass-Steagall Act

D. Economic Espionage Act

18. Which one of the following principles imposes a standard of care upon an individual that is broad and equivalent to what one would expect from a reasonable person under the circumstances?

A. Due diligence

B. Separation of duties

C. Due care

D. Least privilege

19. Brenda's organization recently completed the acquisition of a competitor firm. Which one of the following tasks would be LEAST likely to be part of the organizational processes addressed during the acquisition?

A. Consolidation of security functions

B. Integration of security tools

C. Protection of intellectual property

D. Documentation of security policies

20. Kelly believes that an employee engaged in the unauthorized use of computing resources for a side business. After consulting with management, she decides to launch an administrative investigation. What is the burden of proof that she must meet in this investigation?

    A. Preponderance of the evidence

    B. Beyond a reasonable doubt

    C. Beyond the shadow of a doubt

    D. There is no standard

21. Keenan Systems recently developed a new manufacturing process for microprocessors. The company wants to license the technology to other companies for use but wants to prevent unauthorized use of the technology. What type of intellectual property protection is best suited for this situation?

    A. Patent

    B. Trade secret

    C. Copyright

    D. Trademark

22. Which one of the following actions might be taken as part of a business continuity plan?

    A. Restoring from backup tapes

    B. Implementing RAID

    C. Relocating to a cold site

    D. Restarting business operations

23. When developing a business impact analysis, the team should first create a list of assets. What should happen next?

    A. Identify vulnerabilities in each asset.

    B. Determine the risks facing the asset.

    C. Develop a value for each asset.

    D. Identify threats facing each asset.

24. Mike recently implemented an intrusion prevention system designed to block common network attacks from affecting his organization. What type of risk management strategy is Mike pursuing?

    A. Risk acceptance

    B. Risk avoidance

    C. Risk mitigation

    D. Risk transference

25. Laura has been asked to perform an SCA. What type of organization is she most likely in?

    A. Higher education

    B. Banking

    C. Government

    D. Healthcare

26. Carl is a federal agent investigating a computer crime case. He identified an attacker who engaged in illegal conduct and wants to pursue a case against that individual that will lead to imprisonment. What standard of proof must Carl meet?

    A. Beyond the shadow of a doubt

    B. Preponderance of the evidence

C. Beyond a reasonable doubt

D. Majority of the evidence

27. The International Information Systems Security Certification Consortium uses the logo shown here to represent itself online and in a variety of forums. What type of intellectual property protection may it use to protect its rights in this logo?

A. Copyright

B. Patent

C. Trade secret

D. Trademark

28. Mary is helping a computer user who sees the following message appear on his computer screen. What type of attack has occurred?