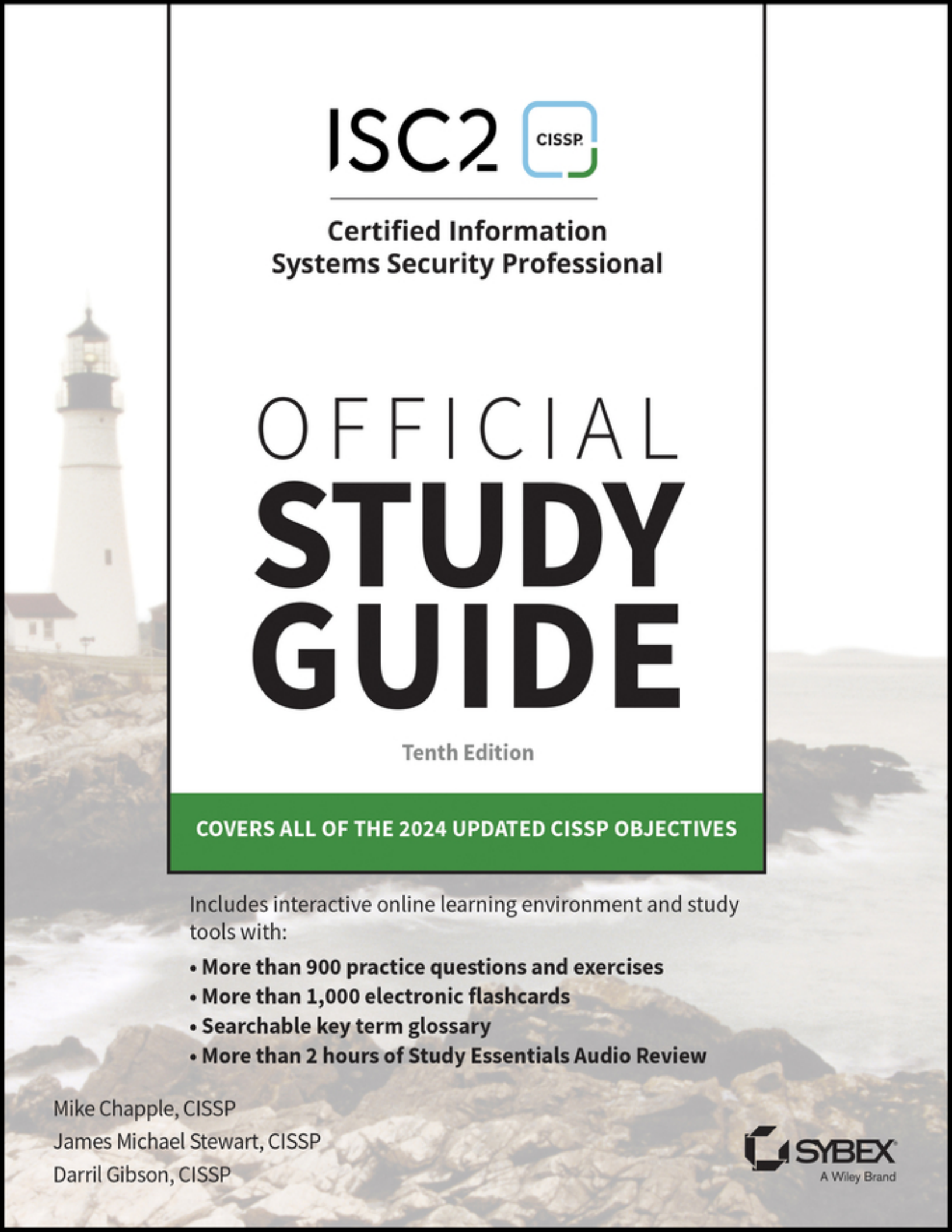

ISC2 CISSP

Certified Information Systems Security Professional

OFFICIAL STUDY GUIDE

Tenth Edition

COVERS ALL OF THE 2024 UPDATED CISSP OBJECTIVES

Includes interactive online learning environment and study tools with:

- **More than 900 practice questions and exercises**
- **More than 1,000 electronic flashcards**
- **Searchable key term glossary**
- **More than 2 hours of Study Essentials Audio Review**

Mike Chapple, CISSP
James Michael Stewart, CISSP
Darril Gibson, CISSP

SYBEX
A Wiley Brand

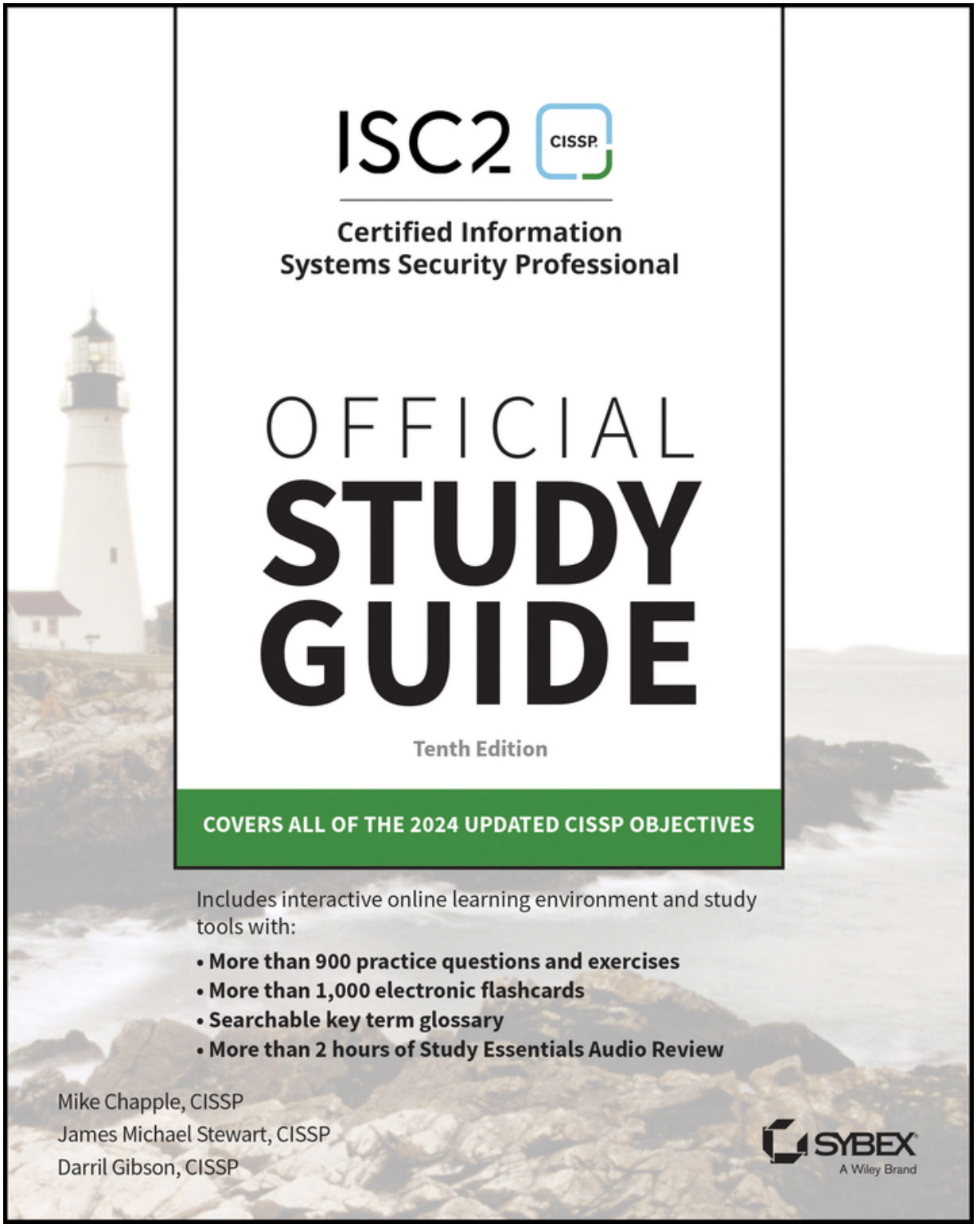
ISC2
CISSP
Certified Information Systems Security Professional
OFFICIAL
STUDY GUIDE
Tenth Edition
COVERS ALL OF THE 2024 UPDATED CISSP OBJECTIVES
Includes interactive online learning environment and study tools with:
• More than 900 practice questions and exercises
• More than 1,000 electronic flashcards
• Searchable key term glossary
• More than 2 hours of Study Essentials Audio Review
Mike Chapple, CISSP
James Michael Stewart, CISSP
Darril Gibson, CISSP
SYBEX
A Wiley Brand

Table of Contents

List of Tables

List of Illustrations

ISC2® CISSP®
Certified Information Systems Security Professional
Official Study Guide

Tenth Edition

Mike Chapple, CISSP
James Michael Stewart, CISSP
Darril Gibson, CISSP


SYBEX
A Wiley Brand

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

Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394254699 (paperback), 9781394254712 (ePDF), 9781394254705 (ePub)

Library of Congress Control Number: 2024935047

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

To Darril Gibson, my friend and co-author of many years. You made a tremendous impact on the cybersecurity field and we will be eternally grateful for your contributions.

—Mike Chapple

To Cathy, I continue to love threading the zigzaggednesses of life with you.

—James Michael Stewart

Acknowledgments

We'd like to express our thanks to Sybex for continuing to support this project. Extra thanks to the tenth edition developmental editor, Kelly Talbot, and technical editors, Shahla Pirnia and Rae Baker, who performed amazing feats in guiding us to improve this book.

We also owe a debt of gratitude to our literary agent, Carole Jelen of Waterside Productions, for continuing to assist in nailing down these projects. Thanks for all your hard work herding us authors.

We also want to express our condolences to the family and friends of Darril Gibson. Darril, you are missed.

—Mike and Michael

Special thanks go to my many friends and colleagues in the cybersecurity community who provided hours of interesting conversation and debate on security issues that inspired and informed much of the material in this book.

I would like to thank the team at Wiley who provided invaluable assistance throughout the book development process. My coauthors, James Michael Stewart and Darril Gibson, were great collaborators and I'd like to thank them both for their thoughtful contributions to my chapters over the years.

I'd also like to thank the many people who participated in the production of this book but whom I never had the chance to meet: the graphics team, the production staff, and all of those involved in bringing this book to press.

—Mike Chapple

Thanks to Mike Chapple for continuing your excellent contribution to this project. Thanks also to all my CISSP course students who have provided their insight and input to improve my training courseware and ultimately this tome. To my adoring wife, Cathy: every year is another wonderful experience with you. To Slayde and Remi: always remember that you are loved no matter where you go or what you

become. To my mom, Johnnie: it is wonderful to have you close by. To Mark: no matter how much time has passed or how little we see each other, I have been and always will be your friend. And finally, as always, to Elvis: I've heard that when you make a sandwich, it's called a peanut butter and banana “Hunka Hunka Burning Lunch”!

—James Michael Stewart

About the Authors

Mike Chapple, PhD, CISSP, Security+, CySA+, PenTest+, CISA, CISM, CCSP, CIPP/US, is a teaching professor of IT, analytics, and operations at the University of Notre Dame. In the past, he was chief information officer of Brand Institute and an information security researcher with the National Security Agency and the U.S. Air Force. His primary areas of expertise include network intrusion detection and access controls. Mike is the author of more than 200 books and video courses, including the companion book to this study guide: *CISSP Official ISC2 Practice Tests*, the *CompTIA CySA+ Study Guide*, the *CompTIA Security+ (SY0-701) Study Guide,* and *Cyberwarfare: Information Operations in a Connected World*. Mike offers study groups for the CISSP, SSCP, CCSP, Security+, and other major certifications on his website at www.certmike.com.

James Michael Stewart, CISSP, CEH, CHFI, ECSA, CND, ECIH, CySA+, PenTest+, CASP+, Security+, Network+, A+, CTT+, CEI, and CFR, has been writing and training for more than 25 years, with a focus on security. He has been teaching CISSP training courses since 2002, not to mention other courses on internet security and ethical hacking/penetration testing. He is the author of and contributor to more than 80 books on security certification, Microsoft topics, and network administration. Michael is the author of the official online virtual lab sets for CompTIA's Security+, CASP+, and PenTest+, as well as hundreds of other labs focusing on Microsoft Windows, Linux, internet, and security concepts. More information about Michael can be found at his website at www.impactonline.com.

Darril Gibson, CISSP (1958–2022), was the CEO of YCDA, LLC and regularly wrote and consulted on a wide variety of technical and security topics and held numerous other certifications, including MCSE, MCDBA, MCSD, MCITP, ITIL v3, and Security+. He authored or coauthored more than 30 books, including multiple prior editions of the *CISSP Study Guide*. Darril was greatly respected in the cybersecurity, training, and education fields and will be missed.

About the Technical Editors

Rae Baker is a senior open source intelligence analyst, public speaker, licensed private investigator, and Wiley author specializing in maritime intelligence and OSINT training. She is the owner of OSINT training company Kase Scenarios and she holds several prominent industry certificates, including SANS GOSI and Associate of ISC2 (CISSP). More information about Rae can be found at http://raebaker.net.

Shahla Pirnia is a freelance technical editor and proofreader with a focus on cybersecurity and certification topics. She currently serves as a technical editor for CertMike.com. Shahla earned BS degrees in computer and information science and psychology from the University of Maryland Global Campus and an Associate of Arts in information systems from Montgomery College, Maryland. Shahla's IT certifications include CompTIA Security+, Network+, A+, and ISC2 CC.

Introduction

The *ISC2® CISSP® Certified Information Systems Security Professional Official Study Guide, Tenth Edition,* offers you a solid foundation for the Certified Information Systems Security Professional (CISSP) exam. By purchasing this book, you've shown a willingness to learn and a desire to develop the skills you need to achieve this certification. This introduction provides you with a basic overview of this book and the CISSP exam.

This book is designed for readers and students who want to study for the CISSP certification exam. If your goal is to become a certified security professional, then the CISSP certification and this CISSP Study Guide are for you. The purpose of this book is to adequately prepare you to take the CISSP exam.

The information presented here in this Introduction was based on the publicly available documentation from ISC2 as of April 15, 2024. However, these details and exam parameters are subject to change at any time based upon ISC2 operational decisions. Please consult isc2.org to confirm, verify, or learn about updated exam specifics.

Before you dive into this book, you need to have accomplished a few tasks on your own. You need to have a general understanding of IT and of security. You should have the necessary five years of cumulative full-time work experience (or four years if you have a college degree) in two or more of the eight domains covered by the CISSP exam. Part-time work and internship experience is also acceptable with conditions; see www.isc2.org/certifications/cissp/cissp-experience-requirements. If you are qualified to take the CISSP exam according to ISC2, then you are sufficiently prepared to use this book to study for it. For more information on ISC2, see the next section.

Alternatively, ISC2 allows for a one-year reduction of the five-year experience requirement if you have earned one of the approved certifications from the ISC2 prerequisite pathway. As of Q1 2024, the qualified certifications are:

- AWS Certified Security - Specialty
- Certified in Governance, Risk and Compliance (CGRC)
- Certified Cloud Security Professional (CCSP)
- Certified Computer Examiner (CCE)
- Certified Ethical Hacker v8 or higher
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Internal Auditor (CIA)
- Certified Protection Professional (CPP) from ASIS
- Certified in Risk and Information Systems Control (CRISC)
- Certified Secure Software Life cycle Professional (CSSLP)
- Certified Wireless Security Professional (CWSP)
- Cisco Certified CyberOps Associate/Professional
- Cisco Certified Internetwork Expert (CCIE) Security
- Cisco Certified Network Associate Security (CCNA Security)
- Cisco Certified Network Professional Security (CCNP Security)
- CIW Web Security Professional
- CIW Web Security Specialist
- CompTIA Advanced Security Practitioner (CASP+)
- CompTIA CySA+
- CompTIA Security+
- Computer Hacking Forensic Investigator (CHFI)
- CSA Certificate of Cloud Security Knowledge (CCSK)

- EC-Council Certified Security Specialist (ECSS)
- EC-Council Certified SOC Analyst (CSA)
- GIAC Certified Enterprise Defender (GCED)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Cyber Threat Intelligence (GCTI)
- GIAC Global Industrial Cyber Security Professional (GICSP)
- GIAC Information Security Fundamentals (GISF)
- GIAC Information Security Professional (GISP)
- GIAC Security Essentials Certificate (GSEC)
- GIAC Security Leadership Certification (GSLC)
- GIAC Strategic Planning, Policy, and Leadership (GSTRT)
- GIAC Systems and Network Auditor (GSNA)
- HealthCare Information Security and Privacy Practitioner (HCISPP)
- Information Security Management Systems Lead Auditor (IRCA)
- Information Security Management Systems Principal Auditor (IRCA)
- Juniper Networks Certified Internet Expert (JNCIE-SEC)
- Microsoft Identity and Access Management
- Microsoft Security Operations Analyst
- Microsoft Certified Cybersecurity Architect
- Offensive Security Certified Professional/Expert (OSCP/E)
- Systems Security Certified Practitioner (SSCP)

For the complete and current list of qualifying certifications, visit www.isc2.org/certifications/cissp/cissp-experience-requirements.

You can use only one of the experience reduction measures, either a college degree or a certification, not both.

ISC2 offers an entry program known as an Associate of ISC2. This program allows someone without any or enough experience to qualify as a CISSP applicant to take the CISSP exam anyway and then obtain experience afterward. Associates are granted six years to obtain five years of security experience. Only after providing proof of such experience, usually by means of endorsement (discussed later), can the individual be awarded the full CISSP certification.

If you are just getting started on your journey to CISSP certification and do not yet have the work experience, then our book can still be a useful tool in your preparation for the exam. However, you may find that some of the topics covered assume knowledge that you don't have. For those topics, you may need to do some additional research using other materials, and then return to this book to continue learning about the CISSP topics.

ISC2

The CISSP exam is governed by the International Information System Security Certification Consortium ISC2. ISC2 is a global nonprofit organization. It has the mission of “ISC2 strengthens the influence, diversity and vitality of the field through advocacy, expertise and workforce empowerment that accelerates cyber safety and cybersecurity in an interconnected world.”

ISC2 is operated by a board of directors elected from the ranks of its certified practitioners.

ISC2 supports and provides a wide variety of certifications, including CISSP, ISSAP, ISSMP, ISSEP, SSCP, CC^{SM}, CCSP, CGRC^{SM}, and CSSLP. These certifications are designed to verify the knowledge and skills of IT security professionals across all industries. You can obtain more information about ISC2 and its other certifications from its website at isc2.org.

The CISSP credential is for security professionals “with the knowledge, skills and abilities to lead an organization's information security program.”

Topical Domains

The CISSP certification covers material from the eight topical domains. These eight domains are as follows:

- Domain 1: Security and Risk Management
- Domain 2: Asset Security
- Domain 3: Security Architecture and Engineering
- Domain 4: Communication and Network Security
- Domain 5: Identity and Access Management (IAM)
- Domain 6: Security Assessment and Testing
- Domain 7: Security Operations
- Domain 8: Software Development Security

These eight domains provide a vendor-independent overview of a common security framework. This framework is the basis for a discussion on security practices that can be supported in all types of organizations worldwide.

Prequalifications

ISC2 has defined the qualification requirements you must meet to become a CISSP. First, you must be a practicing security professional with at least five years’ work experience or with four years’ experience and a recent IT or IS degree or an approved security certification (as mentioned previously). Professional experience is defined as security work performed (with or without pay) within two or more of the eight CISSP domains.

Second, you must agree to adhere to a formal code of ethics. The ISC2 Code of Ethics is a set of guidelines ISC2 wants all certification candidates to follow to maintain professionalism in the field of

information systems security. You can find the ISC2 Code of Ethics at isc2.org/ethics.

Overview of the CISSP Exam

The CISSP exam focuses on security from an overview perspective; it deals more with theory and concept than implementation and procedure. It is very broad but not very deep. To successfully complete this exam, you'll need to be familiar with every domain but not necessarily be a master of each domain.

The CISSP exam is in an adaptive format that ISC2 calls CISSP CAT (Computerized Adaptive Testing). For complete details of this form of exam presentation, please see www.isc2.org/certifications/CISSP/CISSP-CAT.

The CISSP CAT exam has a minimum of 100 questions and a maximum of 150. Not all items (i.e., questions) presented count toward your proficiency level, competency requirements, or passing status. There are 25 unscored questions that are called *pre-test or unscored items* by ISC2, whereas the scored questions are called *operational items*. The questions are not labeled on the exam as to whether they are scored (i.e., operational items) or unscored (i.e., pre-test questions). Test candidates will receive 25 unscored items on their exam, regardless of whether they achieve a passing rank at question 100 or see all of the 150 questions. However, an exam's pass/fail report is determined by only the last 75 operational items answered by the test candidate.

The CISSP CAT grants a maximum of three (3) hours to take the exam. If you run out of time before achieving a passing rank, you will automatically fail.

The CISSP CAT does not allow you to return to a previous question to change your answer. Your answer selection is final once you leave a question by submitting your answer selection.

To pass the CISSP CAT exam, you must score 700 out of a possible 1000 points, within the last 75 operational items (i.e., questions). If you do not achieve the minimum passing score after submitting your

answer to question 150, then you fail. If you run out of time, then you fail.

If you do not pass the CISSP exam on your first attempt, you are allowed to retake the CISSP exam under the following conditions:

- You can take the CISSP exam a maximum of four times per 12-month period. (Note that on the CISSP CAT FAQ the limit is defined as 3 times per a 12-month period.)
- You must wait 30 days after your first attempt before trying a second time.
- You must wait an additional 60 days after your second attempt before trying a third time.
- You must wait an additional 90 days after your third or subsequent attempts before trying again.

The exam retake policy may be updated; you can read the most current version of the official policy here: www.isc2.org/Exams/After-Your-Exam.

You will need to pay full price for each additional exam attempt. However, ISC2 offers promotions from time to time that may allow you to retake an exam at no additional cost. This promotion has been called "Peace of Mind Protection," but could be renamed. It is limited to first-time test-takers only and has time restrictions. Be sure to read the fine print before acting on any such promotional offers.

The CISSP CAT exam is available in English, Chinese, German, Japanese, and Spanish.

For more details and the most up-to-date information on the CISSP exam direct from ISC2, please visit www.isc2.org/Certifications/CISSP and download the CISSP Ultimate Guide and visit www.isc2.org/certifications/cissp/cissp-certification-exam-outline to download the CISSP Exam Outline. You might also find useful information on the ISC2 Insights blog at www.isc2.org/Insights.

The total number of questions you may see on the exam, the total number of questions that count toward your score, the means and methods of scoring, and the time limit for the test are things that ISC2 reevaluates and changes from time to time. The best advice for preparing is to always recheck the ISC2 website for up to date exam specifications and policies.

CISSP Exam Question Types

Most of the questions on the CISSP exam are four-option, multiple-choice questions with a single correct answer. Some are straightforward, such as asking you to select a definition. Some are a bit more involved, asking you to select the appropriate concept or best practice. And some questions present you with a scenario or situation and ask you to select the best response.

You must select the one correct or best answer and mark it. In some cases, the correct answer will be obvious to you. In other cases, several answers may seem correct. In these instances, you must choose the best answer for the question asked. Watch for general, specific, universal, superset, and subset answer selections. In other cases, none of the answers will seem correct. In these instances, you'll need to select the least incorrect answer.

Some multiple-choice questions may require that you select more than one answer; if so, these will state what is necessary to provide a complete answer.

In addition to the standard multiple-choice question format, the exam may include a few advanced question formats, which ISC2 calls *advanced innovative questions*. These include drag-and-drop questions and hotspot questions. These types of questions require you to place topics or concepts in order of operations, in priority preference, or in relation to proper positioning for the needed solution. Specifically, the drag-and-drop questions require the test taker to move labels or icons to mark items on an image. The hotspot questions require the test-taker to pinpoint a location on an image

with a crosshair marker. These question concepts are easy to work with and understand, but be careful about your accuracy when dropping or marking.

ISC2 introduced the advanced innovative questions in 2014. They maintained a page describing these questions until 2017. While they still use this phrase to reference the question concepts, they no longer provide an explanation or examples of these questions on their website.

Advice on Taking the Exam

The CISSP exam consists of two key elements. First, you need to know the material from the eight domains. Second, you must have good test-taking skills. You have a maximum of 3 hours to achieve a passing standard with the potential to see up to 150 questions. Thus, you will have on average just over a minute for each question, so it is important to work quickly, without rushing, but also without wasting time.

Question skipping is not allowed on the CISSP CAT exam. You cannot return to view or change a previous question, and you're also not allowed to jump around, so one way or another, you have to come up with your best answer on each question as it is presented to you. If you don't know how to answer a question, then we recommend that you attempt to eliminate as many answer options as possible before making a guess. Then you can make educated guesses from a reduced set of options to increase your chance of getting a question correct. Since you have to answer every question presented, and you might not know the answer to some questions, you should develop a guessing strategy to select an answer promptly to minimize further wasting time.

Also note that ISC2 does not disclose if there is partial credit given for multiple-part questions if you get only some of the elements correct. So, pay attention to questions with checkboxes, and be sure

to select as many items as necessary to properly address the question.

You will be provided with a dry-erase board and a marker to jot down thoughts and make notes. But nothing written on that board will be used to alter your score. That board must be returned to the test administrator prior to departing the test facility.

To maximize your test-taking activities, here are some general guidelines:

- Read each question carefully, then read the answer options, and then reread the question.
- Eliminate wrong answers before selecting the correct one.
- Watch for double negatives.
- Pay attention to universal terms, such as always or never.
- Look for relationships between answer options, such as similes, antonyms, sets, groups, parent/child, category/example, etc.
- Be sure you understand what the question is asking.

Manage your time. You can take breaks during your test, but this will consume some of your test time. You might consider bringing a drink and snacks, but your food and drink will be stored for you away from the testing area, and that break time will count against your test time limit. Be sure to bring any medications or other essential items, but leave all things electronic at home or in your car. You should avoid wearing anything on your wrists, including watches, fitness trackers, and jewelry. You are not allowed to bring any form of noise-canceling headsets or earbuds, although you can use foam earplugs. We also recommend wearing comfortable clothes and taking a light jacket with you (some testing locations are a bit chilly).

You may want to review the ISC2 CISSP Glossary document at www.isc2.org/certifications/cissp/cissp-student-glossary.

Finally, ISC2 exam policies are subject to change. Please be sure to check isc2.org for the current policies before you register and take the exam.

Study and Exam Preparation Tips

We recommend planning for a month or so of nightly intensive study for the CISSP exam. Here are some suggestions to maximize your learning time; you can modify them as necessary based on your own learning habits:

- Take one or two evenings to read each chapter in this book.
- Read and understand the Study Essentials for each chapter.
- Complete the written labs from each chapter.
- Answer all the review questions for each chapter.
- Be sure to research each question that you get wrong in order to learn what you didn't know.
- Review ISC2's Exam Outline to make sure you understand each listed item.
- Use the flashcards included with the online study tools to reinforce your understanding of concepts.
- Take the 4 full-length bonus practice exams provided in the online test engine.

We recommend spending about half of your study time reading and reviewing concepts and the other half taking practice exams. Students have reported that the more time they spent taking practice exams, the better they retained test topics. In addition to the practice tests with this Study Guide, Sybex also publishes *ISC2 CISSP Certified Information Systems Security Professional Official Practice Tests, 4th Edition* (ISBN: 978-1-394-25507-8). It contains 100 or more practice questions for each domain and four additional full-sized practice exams. Like this Study Guide, it also comes with an online version of the questions.

Completing the Certification Process

Once you have been informed that you successfully passed the CISSP certification, there is one final step before you are actually awarded the CISSP certification. That final step is known as *endorsement*. Basically, this involves getting someone who holds any ISC2 certification in good standing and is familiar with your work history to endorse you. Endorsement is the evaluation of your prerequisite qualifications (i.e., work experience) and the recommendation to ISC2 to award you the certification. Once you pass the CISSP exam, you will receive an email with instructions. However, you can review the endorsement application process at isc2.org/Endorsement. This URL is also where you initiate the endorsement process. You will need to know the ISC2 membership number of the person who will endorse you.

If you registered for CISSP, then you must complete endorsement within nine months of your exam. If you registered for Associate of ISC2, then you have six years from your exam data to complete endorsement. Once ISC2 accepts your endorsement, the certification process will be completed and you will be sent a welcome packet with confirmation of the certification achieved. You should also receive an email confirmation of the endorsement process's completion and another when the certification is awarded to you.

Once you have achieved your CISSP certification, you must maintain it. You will need to earn 120 Continuing Professional Education (CPE) credits by your third-year anniversary. For details on earning and reporting CPEs, please consult the ISC2 Continuing Professional Education (CPE) Handbook (www.isc2.org/-/media/Project/ISC2/Main/Media/documents/members/CPE-Handbook-2023.pdf) and the CPE Opportunities page (www.isc2.org/members/cpe-opportunities). You will also be required to pay an annual maintenance fee (AMF) upon earning your certification and at each annual anniversary. For details on the AMF, please see the ISC2 CPE Handbook, www.isc2.org/Policies-Procedures/AMFs-Overview, and www.isc2.org/Policies-Procedures/Member-Policies.

The Elements of This Study Guide

Each chapter includes common elements to help you focus your studies and test your knowledge. Here are descriptions of those elements:

Tips and Notes Throughout each chapter you will see inserted statements that you should pay additional attention to. These items are often focused details related to the chapter section or related important material.

Summaries The summary is a brief review of the chapter to sum up what was covered.

Study Essentials The Study Essentials highlight topics that could appear on the exam in some form. This section reinforces significant concepts that are key to understanding the concepts and topics of the chapter. The Study Essentials point out specific knowledge you want to retain from a chapter.

Written Labs Each chapter includes written labs that synthesize various concepts and topics that appear in the chapter. These raise questions that are designed to help you put together various pieces you've encountered individually in the chapter and assemble them to propose or describe potential security strategies or solutions. We highly encourage you to write out your answers before viewing our suggested solutions in Appendix B.

Chapter Review Questions Each chapter includes practice questions that have been designed to measure your knowledge of key ideas that were discussed in the chapter. After you finish each chapter, answer the questions; if some of your answers are incorrect, it's an indication that you need to spend some more time studying the corresponding topics. The answers to the practice questions can be found in Appendix A.

Interactive Online Learning Environment and Test Bank

Studying the material in the *ISC2 CISSP: Certified Information Systems Security Professional Official Study Guide, Tenth Edition* is

an important part of preparing for the Certified Information Systems Security Professional (CISSP) certification exam, but we provide additional tools to help you prepare. The online Test Bank will help you understand the types of questions that will appear on the certification exam.

The sample tests in the Test Bank include all the questions in each chapter as well as the questions from the Assessment test in this Introduction section. In addition, there are four bonus practice exams that you can use to evaluate your understanding and identify areas that may require additional study. These four additional practice exams include 125 questions each and cover the breadth of domain topics in a similar percentage ratio as the real exam. They can be used as real exam simulations to evaluate your preparedness.

The online flashcards will push the limits of what you should know for the certification exam. The questions are provided in digital format. Each online flashcard has one question and one correct answer.

The downloadable PDF glossary is a searchable list of key terms from this exam guide that you should know for the CISSP certification exam.

A downloadble audio review is available where Mike Chapple reads aloud the Study Essentials from each chapter. You can listen to the audio review to keep your knowledge skills sharps as you go about your day. Its another means to sneak in a few more minutes of study time.

To start using these to study for the exam, go to www.wiley.com/go/sybextestprep, register your book to receive your unique PIN, and then once you have the PIN, return to www.wiley.com/go/sybextestprep and register a new account or add this book to an existing account.

Like all exams, the CISSP certification from ISC2 is updated periodically and may eventually be retired or replaced. At some point after ISC2 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.

Study Guide Exam Objectives

This table provides the extent, by percentage, to which each domain is represented on the actual examination.

Domain	% of exam
Domain 1: Security and Risk Management	16%
Domain 2: Asset Security	10%
Domain 3: Security Architecture and Engineering	13%
Domain 4: Communication and Network Security	13%
Domain 5: Identity and Access Management (IAM)	13%
Domain 6: Security Assessment and Testing	12%
Domain 7: Security Operations	13%
Domain 8: Software Development Security	10%
Total	100%

Objective Map

This book is designed to cover each of the eight CISSP Exam Outline domains in sufficient depth to provide you with a clear understanding of the material. The main body of this book consists

of 21 chapters. Here is a complete CISSP Exam Outline mapping each objective item to its location in this book's chapters.

Domain	Description	Chapter
1.0	**Security and Risk Management**	
1.1	Understand, adhere to, and promote professional ethics	19
1.1.1	ISC2 Code of Professional Ethics	19
1.1.2	Organizational code of ethics	19
1.2	Understand and apply security concepts	1
1.2.1	Confidentiality, integrity, and availability, authenticity, and nonrepudiation (5 Pillars of Information Security)	1
1.3	Evaluate and apply security governance principles	1
1.3.1	Alignment of the security function to business strategy, goals, mission, and objectives	1
1.3.2	Organizational processes (e.g., acquisitions, divestitures, governance committees)	1
1.3.3	Organizational roles and responsibilities	1
1.3.4	Security control frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI), Federal Risk and Authorization Management Program (FedRAMP))	1
1.3.5	Due care/due diligence	1
1.4	Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context	4
1.4.1	Cybercrimes and data breaches	4

Domain	Description	Chapter
1.4.2	Licensing and Intellectual Property requirements	4
1.4.3	Import/export controls	4
1.4.4	Transborder data flow	4
1.4.5	Issues related to privacy (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act)	4
1.4.6	Contractual, legal, industry standards, and regulatory requirements	4
1.5	Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)	19
1.6	Develop, document, and implement security policy, standards, procedures, and guidelines	1
1.7	Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements	3
1.7.1	Business Impact Analysis (BIA)	3
1.7.2	External dependencies	3
1.8	Contribute to and enforce personnel security policies and procedures	2
1.8.1	Candidate screening and hiring	2
1.8.2	Employment agreements and policy driven requirements	2
1.8.3	Onboarding, transfers, and termination processes	2
1.8.4	Vendor, consultant, and contractor agreements and controls	2
1.9	Understand and apply risk management concepts	**2**

Domain	Description	Chapter
1.9.1	Threat and vulnerability identification	2
1.9.2	Risk analysis, assessment, and scope	2
1.9.3	Risk response and treatment (e.g., cybersecurity insurance)	2
1.9.4	Applicable types of controls (e.g., preventive, detection, corrective)	2
1.9.5	Control assessments (e.g., security and privacy)	2
1.9.6	Continuous monitoring and measurement	2
1.9.7	Reporting (e.g., internal, external)	2
1.9.8	Continuous improvement (e.g., risk maturity modeling)	2
1.9.9	Risk frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI))	2
1.10	Understand and apply threat modeling concepts and methodologies	1
1.11	Apply supply chain risk management (SCRM) concepts	1
1.11.1	Risks associated with the acquisition of products and services from suppliers and providers (e.g., product tampering, counterfeits, implants)	1
1.11.2	Risk mitigations (e.g., third-party assessment and monitoring, minimum security requirements, service level requirements, silicon root of trust, physically unclonable function, software bill of materials)	1
1.12	Establish and maintain a security awareness, education, and training program	2

Domain	Description	Chapter
1.12.1	Methods and techniques to increase awareness and training (e.g., social engineering, phishing, security champions, gamification)	2
1.12.2	Periodic content reviews to include emerging technologies and trends (e.g., cryptocurrency, artificial intelligence (Al), blockchain)	2
1.12.3	Program effectiveness evaluation	2
2.0	**Asset Security**	
2.1	Identify and classify information and assets	5
2.1.1	Data classification	5
2.1.2	Asset classification	5
2.2	Establish information and asset handling requirements	5
2.3	Provision information and assets securely	16
2.3.1	Information and asset ownership	16
2.3.2	Asset inventory (e.g., tangible, intangible)	16
2.3.3	Asset management	16
2.4	Manage data lifecycle	5
2.4.1	Data roles (i.e., owners, controllers, custodians, processors, users/subjects)	5
2.4.2	Data collection	5
2.4.3	Data location	5
2.4.4	Data maintenance	5
2.4.5	Data retention	5
2.4.6	Data remanence	5
2.4.7	Data destruction	5
2.5	Ensure appropriate asset retention (e.g., End of Life (EOL), End of Support)	5
2.6	Determine data security controls and compliance requirements	5

Domain	Description	Chapter
2.6.1	Data states (e.g., in use, in transit, at rest)	5
2.6.2	Scoping and tailoring	5
2.6.3	Standards selection	5
2.6.4	Data protection methods (e.g., Digital Rights Management (DRM) data loss prevention (DLP), cloud access security broker (CASB))	5
3.0	**Security Architecture and Engineering**	
3.1	Research, implement, and manage engineering processes using secure design principles	1, 8, 9, 16
3.1.1	Threat modeling	1
3.1.2	Least privilege	16
3.1.3	Defense in depth	1
3.1.4	Secure defaults	8
3.1.5	Fail securely	8
3.1.6	Segregation of Duties (SoD)	16
3.1.7	Keep it simple and small	8
3.1.8	Zero trust or trust but verify	8
3.1.9	Privacy by design	8
3.1.10	Shared responsibility	9
3.1.11	Secure access service edge	8
3.2	Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)	8
3.3	Select controls based upon systems security requirements	8
3.4	Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)	8
3.5	Assess and mitigate the vulnerabilities of security architectures, designs, and solution	6, 7, 9, 16, 20

Domain	Description	Chapter
	elements	
3.5.1	Client-based systems	9
3.5.2	Server-based systems	9
3.5.3	Database systems	20
3.5.4	Cryptographic systems	6, 7
3.5.5	Industrial Control Systems (ICS)	9
3.5.6	Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))	16
3.5.7	Distributed systems	9
3.5.8	Internet of Things (IoT)	9
3.5.9	Microservices (e.g., application programming interface (API))	9
3.5.10	Containerization	9
3.5.11	Serverless	16
3.5.12	Embedded systems	9
3.5.13	High-Performance Computing systems	9
3.5.14	Edge computing systems	9
3.5.15	Virtualized systems	9
3.6	Select and determine cryptographic solutions	6, 7
3.6.1	Cryptographic life cycle (e.g., keys, algorithm selection)	6, 7
3.6.2	Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)	6, 7
3.6.3	Public Key Infrastructure (PKI) (e.g., quantum key distribution)	7
3.6.4	Key management practices (e.g., rotation)	7
3.6.5	Digital signatures and digital certificates (e.g., non-repudiation, integrity)	7
3.7	Understand methods of cryptanalytic attacks	7, 14, 21

Domain	Description	Chapter
3.7.1	Brute force	7
3.7.2	Ciphertext only	7
3.7.3	Known plaintext	7
3.7.4	Frequency analysis	7
3.7.5	Chosen ciphertext	7
3.7.6	Implementation attacks	7
3.7.7	Side-channel	7
3.7.8	Fault injection	7
3.7.9	Timing	7
3.7.10	Man-in-the-Middle (MITM)	7
3.7.11	Pass the hash	14
3.7.12	Kerberos exploitation	14
3.7.13	Ransomware	21
3.8	Apply security principles to site and facility design	10
3.9	Design site and facility security controls	10
3.9.1	Wiring closets/intermediate distribution frame	10
3.9.2	Server rooms/data centers	10
3.9.3	Media storage facilities	10
3.9.4	Evidence storage	10
3.9.5	Restricted and work area security	10
3.9.6	Utilities and Heating, Ventilation, and Air Conditioning (HVAC)	10
3.9.7	Environmental issues (e.g., natural disasters, man-made)	10
3.9.8	Fire prevention, detection, and suppression	10
3.9.9	Power (e.g., redundant, backup)	10
3.10	Manage the information system lifecycle	8
3.10.1	Stakeholders needs and requirements	8

Domain	Description	Chapter
3.10.2	Requirements analysis	8
3.10.3	Architectural design	8
3.10.4	Development /implementation	8
3.10.5	Integration	8
3.10.6	Verification and validation	8
3.10.7	Transition/deployment	8
3.10.8	Operations and maintenance/sustainment	8
3.10.9	Retirement/disposal	8
4.0	**Communication and Network Security**	
4.1	Apply secure design principles in network architectures	11, 12
4.1.1	Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models	11
4.1.2	Internet Protocol (IP) version 4 and 6 (IPv6) (e.g., unicast, broadcast, multicast, anycast)	11
4.1.3	Secure protocols (e.g., Internet Protocol Security (IPSec), Secure Shell (SSH), Secure Sockets Layer (SSL)]/Transport Layer Security (TLS))	11
4.1.4	Implications of multilayer protocols	11
4.1.5	Converged protocols (e.g., Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP), InfiniBand over Ethernet, Compute Express Link)	11
4.1.6	Transport architecture (e.g., topology, data/control/management plane, cut-through/store-and-forward)	11
4.1.7	Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)	12
4.1.8	Traffic flows (e.g., north-south, east-west)	11

Domain	Description	Chapter
4.1.9	Physical segmentation (e.g., in-band, out-of-band, air-gapped)	11
4.1.10	Logical segmentation (e.g., virtual local area networks (VLANs), virtual private networks (VPNs), virtual routing and forwarding, virtual domain)	11
4.1.11	Micro-segmentation (e.g., network overlays/encapsulation; distributed firewalls, routers, intrusion detection system (IDS)/intrusion prevention system (IPS), zero trust)	11
4.1.12	Edge networks (e.g., ingress/egress, peering)	11
4.1.13	Wireless networks (e.g., Bluetooth, Wi-Fi, Zigbee, satellite)	11
4.1.14	Cellular/mobile networks (e.g., 4G, 5G)	11
4.1.15	Content distribution networks (CDN)	11
4.1.16	Software defined networks (SDN), (e.g., application programming interface (API), Software-Defined Wide-Area Network, network functions virtualization)	11
4.1.17	Virtual Private Cloud (VPC)	11
4.1.18	Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)	12
4.2	Secure network components	11
4.2.1	Operation of infrastructure (e.g., redundant power, warranty, support)	11
4.2.2	Transmission media (e g. physical security of media, signal propagation quality)	11
4.2.3	Network Access Control (NAC) systems (e.g., physical, and virtual solutions)	11
4.2.4	Endpoint security (e.g., host-based)	11

Domain	Description	Chapter
4.3	Implement secure communication channels according to design	12
4.3.1	Voice, video, and collaboration (e.g., conferencing, Zoom rooms)	12
4.3.2	Remote access (e.g., network administrative functions)	12
4.3.3	Data communications (e.g., backhaul networks satellite)	12
4.3.4	Third-party connectivity (e.g., telecom providers, hardware support)	12
5.0	**Identity and Access Management (IAM)**	
5.1	Control physical and logical access to assets	13
5.1.1	Information	13
5.1.2	Systems	13
5.1.3	Devices	13
5.1.4	Facilities	13
5.1.5	Applications	13
5.1.6	Services	13
5.2	Design identification and authentication strategy (e.g., people, devices, and services)	13
5.2.1	Groups and Roles	13
5.2.2	Authentication, Authorization and Accounting (AAA) (e.g., multi-factor authentication (MFA), password-less authentication)	13
5.2.3	Session management	13
5.2.4	Registration, proofing, and establishment of identity	13
5.2.5	Federated Identity Management (FIM)	13
5.2.6	Credential management systems (e.g., Password vault)	13
5.2.7	Single sign-on (SSO)	13

Domain	Description	Chapter
5.2.8	Just-ln-Time	13
5.3	Federated identity with a third-party service	13
5.3.1	On-premise	13
5.3.2	Cloud	13
5.3.3	Hybrid	13
5.4	Implement and manage authorization mechanisms	14
5.4.1	Role-based access control (RBAC)	14
5.4.2	Rule based access control	14
5.4.3	Mandatory access control (MAC)	14
5.4.4	Discretionary access control (DAC)	14
5.4.5	Attribute-based access control (ABAC)	14
5.4.6	Risk based access control	14
5.4.7	Access policy enforcement (e.g., policy decision point, policy enforcement point)	14
5.5	Manage the identity and access provisioning lifecycle	13, 14
5.5.1	Account access review (e.g., user, system, service)	13
5.5.2	Provisioning and deprovisioning (e.g., on/off boarding and transfers)	13
5.5.3	Role definition and transition (e.g., people assigned to new roles)	13
5.5.4	Privilege escalation (e.g., use of sudo, auditing its use)	14
5.5.5	Service accounts management	13
5.6	Implement authentication systems	14
6.0	**Security Assessment and Testing**	
6.1	Design and validate assessment, test, and audit strategies	15

Domain	Description	Chapter
6.1.1	Internal (e.g., within organization control)	15
6.1.2	External (e.g., outside organization control)	15
6.1.3	Third-party (e.g., outside of enterprise control)	15
6.1.4	Location (e.g., on-premise, cloud, hybrid)	15
6.2	Conduct security controls testing	15
6.2.1	Vulnerability assessment	15
6.2.2	Penetration testing (e.g., red, blue, and/or purple team exercises)	15
6.2.3	Log reviews	15
6.2.4	Synthetic transactions/benchmarks	15
6.2.5	Code review and testing	15
6.2.6	Misuse case testing	15
6.2.7	Coverage analysis	15
6.2.8	Interface testing (e.g., user interface, network interface, application programming interface (API))	15
6.2.9	Breach attack simulations	15
6.2.10	Compliance checks	15
6.3	Collect security process data (e.g., technical and administrative)	15, 18
6.3.1	Account management	15
6.3.2	Management review and approval	15
6.3.3	Key performance and risk indicators	15
6.3.4	Backup verification data	15
6.3.5	Training and awareness	15, 18
6.3.6	Disaster Recovery (DR) and Business Continuity (BC)	15, 18
6.4	Analyze test output and generate report	15
6.4.1	Remediation	15

Domain	Description	Chapter
6.4.2	Exception handling	15
6.4.3	Ethical disclosure	15
6.5	Conduct or facilitate security audits	15
6.5.1	Internal (e.g., within organization control)	15
6.5.2	External (e.g., outside organization control)	15
6.5.3	Third-party (e.g., outside of enterprise control)	15
6.5.4	Location (e.g., on-premise, cloud, hybrid)	15
7.0	**Security Operations**	
7.1	Understand and comply with investigations	19
7.1.1	Evidence collection and handling	19
7.1.2	Reporting and documentation	19
7.1.3	Investigative techniques	19
7.1.4	Digital forensics tools, tactics, and procedures	19
7.1.5	Artifacts (e.g., data, computer, network, mobile device)	19
7.2	Conduct logging and monitoring activities	17, 21
7.2.1	Intrusion detection and prevention system (IDPS)	17
7.2.2	Security information and event management (SIEM)	17
7.2.3	Continuous monitoring and tuning	17
7.2.4	Egress monitoring	17
7.2.5	Log management	17
7.2.6	Threat intelligence (e.g., threat feeds, threat hunting)	17
7.2.7	User and Entity Behavior Analytics (UEBA)	21
7.3	Perform configuration management (CM) (e.g., provisioning, baselining, automation)	16
7.4	Apply foundational security operations concepts	16

Domain	Description	Chapter
7.4.1	Need-to-know/least privilege	16
7.4.2	Segregation of Duties (SoD) and responsibilities	16
7.4.3	Privileged account management	16
7.4.4	Job rotation	16
7.4.5	Service-level agreements (SLA)	16
7.5	Apply resource protection	16
7.5.1	Media management	16
7.5.2	Media protection techniques	16
7.5.3	Data at rest/data in transit	16
7.6	Conduct incident management	17
7.6.1	Detection	17
7.6.2	Response	17
7.6.3	Mitigation	17
7.6.4	Reporting	17
7.6.5	Recovery	17
7.6.6	Remediation	17
7.6.7	Lessons learned	17
7.7	Operate and maintain detection and preventative measures	11, 17, 21
7.7.1	Firewalls (e.g., next generation, web application, network)	11
7.7.2	Intrusion detection systems (IDS) and intrusion prevention systems (IPS)	17
7.7.3	Whitelisting/blacklisting	17
7.7.4	Third-party provided security services	17
7.7.5	Sandboxing	17
7.7.6	Honeypots/honeynets	17
7.7.7	Anti-malware	17, 21

Domain	Description	Chapter
7.7.8	Machine learning and Artificial Intelligence (Al) based tools	17
7.8	Implement and support patch and vulnerability management	16
7.9	Understand and participate in change management processes	16
7.10	Implement recovery strategies	18
7.10.1	Backup storage strategies (e.g., cloud storage, onsite, offsite)	18
7.10.2	Recovery site strategies (e.g., cold vs. hot, resource capacity agreements)	18
7.10.3	Multiple processing sites	18
7.10.4	System resilience, high availability (HA), Quality of Service (QoS), and fault tolerance	18
7.11	Implement disaster recovery (DR) processes	18
7.11.1	Response	18
7.11.2	Personnel	18
7.11.3	Communications (e.g., methods)	18
7.11.4	Assessment	18
7.11.5	Restoration	18
7.11.6	Training and awareness	18
7.11.7	Lessons learned	18
7.12	Test disaster recovery plan (DRP)	18
7.12.1	Read-through/tabletop	18
7.12.2	Walkthrough	18
7.12.3	Simulation	18
7.12.4	Parallel	18
7.12.5	Full interruption	18
7.12.6	Communications (e.g., stakeholders, test status, regulators)	18

Domain	Description	Chapter
7.13	Participate in Business Continuity (BC) planning and exercises	3
7.14	Implement and manage physical security	10
7.14.1	Perimeter security controls	10
7.14.2	Internal security controls	10
7.15	Address personnel safety and security concerns	16
7.15.1	Travel	16
7.15.2	Security training and awareness (e.g., insider threat, social media impacts, two-factor authentication (2FA) fatigue)	16
7.15.3	Emergency management	16
7.15.4	Duress	16
8.0	**Software Development Security**	
8.1	Understand and integrate security in the Software Development Life Cycle (SDLC)	20
8.1.1	Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps, Scaled Agile Framework)	20
8.1.2	Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))	20
8.1.3	Operation and maintenance	20
8.1.4	Change management	20
8.1.5	Integrated Product Team	20
8.2	Identify and apply security controls in software development ecosystems	15, 20, 21
8.2.1	Programming languages	20
8.2.2	Libraries	20
8.2.3	Tool sets	20
8.2.4	Integrated Development Environment	20

Domain	Description	Chapter
8.2.5	Runtime	20
8.2.6	Continuous Integration and Continuous Delivery (Cl/CD)	20
8.2.7	Software Configuration Management (CM)	20
8.2.8	Code repositories	20
8.2.9	Application security testing (e.g., static application security testing (SAST), dynamic application security testing (DAST), software composition analysis, interactive application security testing (IAST))	15
8.3	Assess the effectiveness of software security	20, 21
8.3.1	Auditing and logging of changes	20
8.3.2	Risk analysis and mitigation	21
8.4	Assess security impact of acquired software	16, 20
8.4.1	Commercial-off-the-shelf (COTS)	20
8.4.2	Open source	20
8.4.3	Third-party	20
8.4.4	Managed services (e.g., enterprise applications)	16
8.4.5	Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service [IaaS], Platform as a Service (PaaS))	16
8.5	Define and apply secure coding guidelines and standards	20, 21
8.5.1	Security weaknesses and vulnerabilities at the source-code level	21
8.5.2	Security of application programming interfaces (API)	20
8.5.3	Secure coding practices	20
8.5.4	Software-defined security	20

How to Contact the Publisher

If you believe you've 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.”

Assessment Test

1. Which of the following types of access control seeks to discover evidence of unwanted, unauthorized, or illicit behavior or activity?
    A. Preventive
    B. Deterrent
    C. Detection
    D. Corrective
2. Define and detail the aspects of password selection that distinguish good password choices from ultimately poor password choices.
    A. Is difficult to guess or unpredictable
    B. Meets minimum length requirements
    C. Meets specific complexity requirements
    D. All of the above
3. Some adversaries use DoS attacks as their primary weapon to harm targets, whereas others may use them as weapons of last resort when all other attempts to intrude on a target fail. Which of the following is most likely to detect DoS attacks?
    A. Host-based IDS
    B. Network-based IDS

C. Vulnerability scanner

D. Penetration testing

4. Unfortunately, attackers have many options of attacks to perform against their targets. Which of the following is considered a denial-of-service (DoS) attack?

   A. Pretending to be a technical manager over the phone and asking a receptionist to change their password

   B. While surfing the web, sending to a web server a malformed URL that causes the system to consume 100 percent of the CPU

   C. Intercepting network traffic by copying the packets as they pass through a specific subnet

   D. Sending message packets to a recipient who did not request them, simply to be annoying

5. Hardware networking devices operate within the protocol stack just like protocols themselves. Thus, hardware networking devices can be associated with an OSI model layer related to the protocols they manage or control. At which layer of the OSI model does a router operate?

   A. Network Layer

   B. Layer 1

   C. Transport Layer

   D. Layer 5

6. Which type of firewall automatically adjusts its filtering rules based on the content and context of the traffic of existing sessions? (Choose all that apply.)

   A. Static packet filtering

   B. Application-level gateway

   C. Circuit-level gateway

   D. Stateful inspection firewall

7. A VPN can be a significant security improvement for many communication links. A VPN can be established over which of the following?

    A. Wireless LAN connection

    B. Remote access dial-up connection

    C. WAN link

    D. All of the above

8. Adversaries will use any and all means to harm their targets. This includes mixing attack concepts together to make a more effective campaign. What type of malware uses social engineering to trick a victim into installing it?

    A. Virus

    B. Worm

    C. Trojan horse

    D. Logic bomb

9. Security is established by understanding the assets of an organization that need protection and understanding the threats that could cause harm to those assets. Then, controls are selected that provide protection for the CIA Triad of the assets at risk. The CIA Triad consists of what elements?

    A. Contiguousness, interoperable, arranged

    B. Authentication, authorization, accountability

    C. Capable, available, integral

    D. Availability, confidentiality, integrity

10. The security concept of AAA services describes the elements that are necessary to establish subject accountability. Which of the following is not a required component in the support of accountability?

    A. Logging

    B. Privacy

    C. Identification verification

D. Authorization

11. Collusion is when two or more people work together to commit a crime or violate a company policy. Which of the following is not a defense against collusion?

    A. Separation of duties

    B. Restricted job responsibilities

    C. Group shared user accounts

    D. Job rotation

12. A data custodian is responsible for securing resources after _____ has assigned the resource a security label.

    A. Senior management

    B. The data owner

    C. An auditor

    D. Security staff

13. In what phase of the Capability Maturity Model for Software (SW-CMM) are quantitative measures used to gain a detailed understanding of the software development process?

    A. Repeatable

    B. Defined

    C. Managed

    D. Optimizing

14. Which one of the following is a layer of the protection ring model design concept that is not normally implemented?

    A. Ring 0

    B. Ring 1

    C. Ring 3

    D. Ring 4

15. TCP operates at the Transport Layer and is a connection-oriented protocol. It uses a special process to establish a session

each time a communication takes place. What is the last phase of the TCP three-way handshake sequence?

A. SYN flagged packet

B. ACK flagged packet

C. FIN flagged packet

D. SYN/ACK flagged packet

16. The lack of secure coding practices has enabled an uncountable number of software vulnerabilities that attackers have discovered and exploited. Which one of the following vulnerabilities would be best countered by adequate parameter checking?

A. Time-of-check to time-of-use

B. Buffer overflow

C. SYN flood

D. Distributed denial of service (DDoS)

17. Computers are based on binary mathematics. All computer functions are derived from the basic set of Boolean operations. What is the value of the logical operation shown here?

```
X:      0 1 1 0 1 0
Y:      0 0 1 1 0 1

____________________
X ⊕ Y:    ?
```

A. 0 1 0 1 1 1

B. 0 0 1 0 0 0

C. 0 1 1 1 1 1

D. 1 0 0 1 0 1

18. Which of the following are considered standard data type classifications used in either a government/military or a private sector organization? (Choose all that apply.)

A. Public

B. Healthy

C. Private

D. Inside only

E. Sensitive

F. Proprietary

G. Essential

H. Certified

I. Critical

J. Confidential

K. For Your Eyes Only

19. The General Data Protection Regulation (GDPR) has defined several roles in relation to the protection and management of personally identifiable information (PII). Which of the following statements is true?

    A. A data processor is the entity assigned specific responsibility for a data asset in order to ensure its protection for use by the organization.

    B. A data custodian is the entity that performs operations on data.

    C. A data controller is the entity that makes decisions about the data they are collecting.

    D. A data owner is the entity assigned or delegated the day-to-day responsibility of proper storage and transport as well as protecting data, assets, and other organizational objects.

20. If Renee receives a digitally signed message from Mike, what key does she use to verify that the message truly came from Mike?

    A. Renee's public key

    B. Renee's private key

    C. Mike's public key

    D. Mike's private key

21. A systems administrator is setting up a new data management system. It will be gathering data from numerous locations across the network, even from remote offsite locations. The data will be moved to a centralized facility, where it will be stored on a massive RAID array. The data will be encrypted on the storage system using AES-256, and most files will be signed as well. The location of this data warehouse is secured so that only authorized personnel can enter the room and all digital access is limited to a set of security administrators. Which of the following describes the data?

    A. The data is encrypted in transit.

    B. The data is encrypted in processing.

    C. The data is redundantly stored.

    D. The data is encrypted at rest.

22. The _____ is the entity assigned specific responsibility for a data asset in order to ensure its protection for use by the organization.

    A. Data owner

    B. Data controller

    C. Data processor

    D. Data custodian

23. A security auditor is seeking evidence of how sensitive documents made their way out of the organization and onto a public document distribution site. It is suspected that an insider exfiltrated the data over a network connection to an external server, but this is only a guess. Which of the following would be useful in determining whether this suspicion is accurate? (Choose two.)

    A. NAC

    B. DLP alerts

    C. Syslog

    D. Log analysis

E. Malware scanner reports

F. Integrity monitoring

24. A new Wireless Access Point (WAP) is being installed to add wireless connectivity to the company network. The configuration policy indicates that WPA3 is to be used and thus only newer or updated endpoint devices can connect. The policy also states that ENT authentication will not be implemented. What authentication mechanism can be implemented in this situation?

    A. IEEE 802.1X

    B. IEEE 802.1q

    C. Simultaneous authentication of equals (SAE)

    D. EAP-FAST

25. When securing a mobile device, what types of authentication can be used that depend on the user's physical attributes? (Choose all that apply.)

    A. Fingerprint

    B. TOTP (time-based one-time password)

    C. Voice

    D. SMS (short message service)

    E. Retina or iris

    F. Gait

    G. Phone call

    H. Facial recognition

    I. Smartcard

    J. Password

26. A recently acquired piece of equipment is not working properly. Your organization does not have a trained repair technician on staff, so you have to bring in an outside expert. What type of account should be issued to a trusted third-party repair technician?

A. Guest account

B. Privileged account

C. Service account

D. User account

27. Security should be designed and integrated into the organization as a means to support and maintain the business objectives. However, the only way to know if the implemented security is sufficient is to test it. Which of the following is a procedure designed to test and perhaps bypass a system's security controls?

A. Logging usage data

B. War dialing

C. Penetration testing

D. Deploying secured desktop workstations

28. Security needs to be designed to support the business objectives, but it also needs to be legally defensible. To defend the security of an organization, a log of events and activities must be created. Auditing is a required factor to sustain and enforce what?

A. Accountability

B. Confidentiality

C. Accessibility

D. Redundancy

29. Risk assessment is a process by which the assets, threats, probabilities, and likelihoods are evaluated in order to establish criticality prioritization. What is the formula used to compute the ALE?

A. ALE = AV * EF * ARO

B. ALE = ARO * EF

C. ALE = AV * ARO

D. ALE = EF * ARO

30. Incident response plans, business continuity plans, and disaster recovery plans are crafted when implementing business-level redundancy. These plans are derived from the information obtained when performing a business impact assessment (BIA). What is the first step of the BIA process?

    A. Identification of priorities

    B. Likelihood assessment

    C. Risk identification

    D. Resource prioritization

31. Many events can threaten the operation, existence, and stability of an organization. Some of those threats are human caused, whereas others are from natural events. Which of the following represent natural events that can pose a threat or risk to an organization?

    A. Earthquake

    B. Flood

    C. Tornado

    D. All of the above

32. What kind of recovery facility enables an organization to resume operations as quickly as possible, if not immediately, upon failure of the primary facility?

    A. Hot site

    B. Warm site

    C. Cold site

    D. All of the above

33. During an account review, an auditor provided the following report:

User	Last Login Length	Last Password Change
Bob	4 hours	87 days
Sue	3 hours	38 days
John	1 hour	935 days

User	Last Login Length	Last Password Change
Kesha	3 hours	49 days

The security manager reviews the account policies of the organization and takes note of the following requirements:

- Passwords must be at least 12 characters long.
- Passwords must include at least one example of three different character types.
- Passwords must be changed every 180 days.
- Passwords cannot be reused.

Which of the following security controls should be corrected to enforce the password policy?

A. Minimum password length

B. Account lockout

C. Password history and minimum age

D. Password maximum age

34. Any evidence to be used in a court proceeding must abide by the Rules of Evidence to be admissible. What type of evidence refers to written documents that are brought into court to prove a fact?

A. Best evidence

B. Parol evidence

C. Documentary evidence

D. Testimonial evidence

35. DevOps manager John is concerned with the CEO's plan to minimize his department and outsource code development to a foreign programming group. John has a meeting scheduled with the board of directors to encourage them to retain code development in house due to several concerns. Which of the following should John include in his presentation? (Choose all that apply.)

A. Code from third parties will need to be manually reviewed for function and security.

B. If the third party goes out of business, existing code may need to be abandoned.

C. Third-party code development is always more expensive.

D. A software escrow agreement should be established.

36. When TLS is being used to secure web communications, what URL prefix appears in the web browser address bar to signal this fact?

A. `SHTTP://`

B. `TLS://`

C. `FTPS://`

D. `HTTPS://`

37. A new update has been released by the vendor of an important software product that is an essential element of a critical business task. The chief security officer (CSO) indicates that the new software version needs to be tested and evaluated in a virtual lab, which has a cloned simulation of many of the company's production systems. Furthermore, the results of this evaluation must be reviewed before a decision is made as to whether the software update should be installed and, if so, when to install it. What security principle is the CSO demonstrating?

A. Business continuity planning (BCP)

B. Onboarding

C. Change management

D. Static analysis

38. What type of token device produces new time-derived passwords on a specific time interval that can be used only a single time when attempting to authenticate?

A. HOTP

B. HMAC

C. SAML

D. TOTP

39. Your organization is moving a significant portion of their data processing from an on-premises solution to the cloud. When evaluating a cloud service provider (CSP), which of the following is the most important security concern?

    A. Data retention policy

    B. Number of customers

    C. Hardware used to support VMs

    D. Whether they offer MaaS, IDaaS, and SaaS

40. Most software vulnerabilities exist because of a lack of secure or defensive coding practices used by the developers. Which of the following is considered a secure coding technique? (Choose all that apply.)

    A. Using immutable systems

    B. Using stored procedures

    C. Using code signing

    D. Using server-side validation

    E. Optimizing file sizes

    F. Using third-party software libraries

Answers to Assessment Test

1. C. Detection access controls are used to discover (and document) unwanted or unauthorized activity. Preventive access controls block the ability to perform unwanted activity. Deterrent access controls attempt to persuade the perpetrator not to perform unwanted activity. Corrective access controls restore a system to normal function in the event of a failure or system interruption.
2. D. Strong password choices are difficult to guess, unpredictable, and of specified minimum lengths to ensure that password

entries cannot be computationally determined. They may be randomly generated and use any of the alphabetic, numeric, and allowed special characters; they should never be written down or shared; they should not be stored in publicly accessible or generally readable locations; and they shouldn't be transmitted in the clear.

3. B. Network-based IDSs are usually able to detect the initiation of an attack or the ongoing attempts to perpetrate an attack (including denial of service, or DoS). They are, however, unable to provide information about whether an attack was successful or which specific systems, user accounts, files, or applications were affected. Host-based IDSs have some difficulty with detecting and tracking down DoS attacks. Vulnerability scanners don't detect DoS attacks; they test for possible vulnerabilities. Penetration testing may cause a DoS or test for DoS vulnerabilities, but it is not a detection tool.
4. B. Not all instances of DoS are the result of a malicious attack. Errors in coding OSs, services, and applications have resulted in DoS conditions. Some examples of this include a process failing to release control of the CPU or a service consuming system resources out of proportion to the service requests it is handling. Social engineering (i.e., pretending to be a technical manager) and sniffing (i.e., intercepting network traffic) are typically not considered DoS attacks. Sending message packets to a recipient who did not request them simply to be annoying may be a type of social engineering, and it is definitely spam, but unless the volume of the messages is significant, it does not warrant the label of DoS.
5. A. Routers function at Layer 3, the Network Layer. Layer 1, the Physical Layer, is where repeaters and hubs operate, not routers. Network devices usually do not operate at the transport layer alone, but across layers, such as firewalls, proxies, and load balancers. Layer 5, the Session Layer, does not actually exist in a modern TCP/IP network, and thus no hardware directly operates at this layer, but its functions are performed by TCP in the Transport Layer, Layer 4, when sessions are in use.

6. B, D. Stateful inspection firewalls (aka dynamic packet-filtering firewalls) enable the real-time modification of the filtering rules based on traffic content and context. An application-level gateway is a type of stateful firewall. Static packet filtering and circuit-level firewalls are both stateless and thus do not consider the context when applying filtering rules.
7. D. A virtual private network (VPN) link can be established over any network communication connection. This could be a typical LAN cable connection, a wireless LAN connection, a remote access dial-up connection, a WAN link, or an internet connection used by a client for access to the office LAN.
8. C. A Trojan horse is a form of malware that uses social engineering tactics to trick a victim into installing it—the trick is to make the victim believe that the only thing they have downloaded or obtained is the host file, when in fact it has a malicious hidden payload. Viruses and logic bombs do not typically use social engineering as an element in their means of infecting a system. A worm sometimes is designed to take advantage of social engineering, such as when the worm is an executable email attachment and the message tricks the victim into opening it. However, not all worms are designed this way—this is a core design concept of a Trojan horse.
9. D. The components of the CIA Triad are confidentiality, integrity, and availability. The other options are not the terms that define the CIA Triad, although they are security concepts that need to be evaluated when establishing a security infrastructure.
10. B. Privacy is not necessary to provide accountability. The required elements of accountability, as defined in AAA services, are as follows: identification (which is sometimes considered an element of authentication, a silent first step of AAA services, or represented by IAAA), authentication (i.e., identification verification), authorization (i.e., access control), auditing (i.e., logging and monitoring), and accounting.
11. C. Group shared user accounts allow for multiple people to log in under a single user account. This allows collusion because it prevents individual accountability. Separation of duties,

restricted job responsibilities, and job rotation help establish individual accountability and control access (especially to privileged capabilities), which in turn limits or restricts collusion.

12. B. The data owner must first assign a security label to a resource before the data custodian can secure the resource appropriately. Senior management is ultimately responsible for the success or failure of a security endeavor. An auditor is responsible for reviewing and verifying that the security policy is properly implemented, that the derived security solutions are adequate, and that user events are in compliance with security policy. The security staff is responsible for designing, implementing, and managing the security infrastructure once approved by senior management.
13. C. The Managed phase (level 4) of the SW-CMM involves the use of quantitative development metrics. The Software Engineering Institute (SEI) defines the key process areas for this level as Quantitative Process Management and Software Quality Management. The Repeatable phase (level 2) is where basic life cycle processes are introduced. The Defined phase (level 3) is where developers operate according to a set of formal, documented development processes. The Optimizing phase (level 5) is where a process of continuous improvement is achieved.
14. B. Rings 1 and 2 contain device drivers but are not normally implemented in practice, since they are often collapsed into Ring 0. Ring 0 always contains the security kernel. Ring 3 contains user applications. Ring 4 does not exist in the design concept, but it may exist in customized implementations.
15. B. The SYN flagged packet is first sent from the initiating host to the destination host. The destination host then responds with a SYN/ACK flagged packet. The initiating host sends an ACK flagged packet, and the connection is then established. The FIN flagged packet is not used in the TCP three-way handshake to establish a session; it is used in the session teardown process.
16. B. Parameter checking (i.e., confirming input is within reasonable boundaries) is used to prevent the possibility of

buffer overflow attacks. Time-of-check to time-of-use (TOCTOU) attacks are not directly addressed by parameter checking or input filtering; defensive coding practices are needed to eliminate or reduce this issue. SYN flood attacks are a type of DoS, which is not fully protected against with just improved coding practices. A DDoS is also not prohibited by just improved coding practices such as parameter checking. For any type of DoS, adequate filtering and processing capacity are the most effective security responses.

17. A. The ⊕ symbol represents the XOR function and returns a true value when only one of the input values is true. If both values are false or both values are true, the output of the XOR function is false. Option B is the result if these two values were combined using the AND (the ∧ symbol) function, which returns a value of true if the two values are both true. Option C is the result if these two values were combined using the OR (the ∨ symbol) function, which returns a value of true if either input values is true. Option D is the result if only the X value was subjected to the NOR (the ~ symbol) function, which reverses the value of an input.

18. A, C, E, F, I, J. There are six standard data type classifications used in either a government/military or a private sector organization in this list of options: public, private, sensitive, proprietary, critical, and confidential. The other options (healthy, inside only, essential, certified, and for your eyes only) are incorrect since they are not typical or standard classifications. Note: There is a “For internal use only” classification, but the option here is “Inside only,” which while it may express the same sentiment/intention, is not the exact classification label.

19. C. The correct statement is regarding the data controller. The other statements are incorrect. The correct versions of those statements are as follows. A data owner is the entity assigned specific responsibility for a data asset in order to ensure its protection for use by the organization. A data processor is the entity that performs operations on data. A data custodian is the entity assigned or delegated the day-to-day responsibility for

proper storage and transport as well as protecting data, assets, and other organizational objects.

20. C. Any recipient can use Mike's public key to verify the authenticity of the digital signature. Renee's (the recipient's) public key is not used in this scenario. However, it could be used to create a digital envelope to protect a symmetric session encryption key sent from Mike to Renee. Renee's (the recipient's) private key is not used in this scenario. However, it could be used if Renee becomes a sender to send Mike a digitally signed message. Mike's (the sender's) private key was used to encrypt the hash of the data to be sent to Renee, and this is what creates the digital signature.
21. D. In this scenario, the data is encrypted at rest with AES-256. There is no mention of encryption for transfer or processing. The data is not stored redundantly, since it is being moved, not copied, to the central data warehouse, and there is no mention of a backup.
22. A. The data owner is the person(s) (or entity) assigned specific responsibility for a data asset in order to ensure its protection for use by the organization. The data controller is the entity that makes decisions about the data they are collecting. A data processor is the entity that performs operations on data on behalf of a data controller. A data custodian is a subject who has been assigned or delegated the day-to-day responsibility for proper storage and transport as well as protecting data, assets, and other organizational objects.
23. B, D. In this scenario, the data loss prevention (DLP) alerts and log analysis are the only options that would potentially include useful information in regard to an insider exfiltrating the sensitive documents. The other options are incorrect because they do not provide relevant information. Network access control (NAC) is a security mechanism to prevent rogue devices and ensure authorized systems meet minimum security configuration requirements. Syslog is a logging service used to maintain centralized real-time copies of active log files. Malware scanner reports are not relevant here since there is no suspicious or malicious code being used but only access abuses and

unauthorized file distribution. Integrity monitoring is also not relevant to this situation, since there is no indication that the documents were altered, just that they were released to the public.

24. C. WPA3 supports ENT (Enterprise Wi-Fi authentication, aka IEEE 802.1X) and SAE authentication. Simultaneous authentication of equals (SAE) still uses a password, but it no longer encrypts and sends that password across the connection to perform authentication. Instead, SAE performs a zero-knowledge proof process known as Dragonfly Key Exchange, which is itself a derivative of Diffie–Hellman. IEEE 802.1X defines port-based network access control that ensures that clients can't communicate with a resource until proper authentication has taken place. It's based on Extensible Authentication Protocol (EAP) from Point-to-Point Protocol (PPP). However, this is the technology behind the label of ENT; thus, it is not an option in this scenario. IEEE 802.1q defines the use of virtual local area network (VLAN) tags and thus is not relevant to Wi-Fi authentication. Flexible Authentication via Secure Tunneling (EAP-FAST) is a Cisco protocol proposed to replace Lightweight Extensible Authentication Protocol (LEAP), which is now obsolete, thanks to the development of WPA2, and is not supported in WPA3 either.

25. A, C, E, H. Biometrics are authentication factors that are based on a user's physical attributes; they include fingerprints, voice, retina, iris, and facial recognition. Gait is a form of biometrics, but it is not appropriate for use as authentication on a mobile device; it is used from a stationary position to monitor people walking toward or past a security point. The other options are valid authentication factors, but they are not biometrics.

26. B. A repair technician typically requires more than a normal level of access to perform their duties, so a privileged account for even a trusted third-party technician is appropriate. A guest account or user (normal, limited) account is insufficient for this scenario. A service account is to be used by an application or background service, not a repair technician or other user.

27. C. Penetration testing is the attempt to bypass security controls to test overall system security. Logging usage data is a type of auditing and is useful in the authentication, authorization, accounting (AAA) service process in order to hold subjects accountable for their actions. However, it is not a means to test security. War dialing is an attempt to locate modems and fax machines by dialing phone numbers. This process is sometimes still used by penetration testers and adversaries to find targets to attack, but it is not an actual attack or stress test itself. Deploying secured desktop workstations is a security response to the results of a penetration test, not a security testing method.
28. A. Auditing is a required factor to sustain and enforce accountability. Auditing is one of the elements of the AAA services concept of identification, authentication, authorizations, auditing, and accounting. Confidentiality is a core security element of the CIA Triad, but it is not dependent on auditing. Accessibility is the assurance that locations and systems are able to be used by the widest range of people/users possible. Redundancy is the implementation of alternatives, backup options, and recovery measures and methods to avoid single points of failure to ensure that downtime is minimized while maintaining availability.
29. A. The annualized loss expectancy (ALE) is computed as the product of the asset value (AV) times the exposure factor (EF) times the annualized rate of occurrence (ARO). This is the longer form of the formula ALE = SLE * ARO, since SLE = AV * EF. The other formulas displayed here do not accurately reflect this calculation, since they are not valid or typical risk formulas.
30. A. Identification of priorities is the first step of the business impact assessment process. Likelihood assessment is the third step or phase of BIA. Risk identification is the second step of BIA. Resource prioritization is the last step of BIA.
31. D. Natural events that can threaten organizations include earthquakes, floods, hurricanes, tornadoes, wildfires, and other acts of nature. Thus options A, B, and C are correct because they are natural and not human caused.

32. A. Hot sites provide backup facilities maintained in constant working order and fully capable of taking over business operations. Warm sites consist of preconfigured hardware and software to run the business, neither of which possesses the vital business information. Cold sites are simply facilities designed with power and environmental support systems but no configured hardware, software, or services. Disaster recovery services can facilitate and implement any of these sites on behalf of a company.
33. D. The issue revealed by the audit report is that one account has a password that is older than the requirements allow for; thus, correcting the password maximum age security setting should resolve this. There is no information in regard to password length, lockout, or password reuse in the audit report, so these options are not of concern in this situation.
34. C. Written documents brought into court to prove the facts of a case are referred to as documentary evidence. Best evidence is a form of documentary evidence, but specifically it is the original document rather than a copy or description. Parol evidence is based on a rule stating that when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement, and no verbal agreements may modify the written agreement. Testimonial evidence consists of the testimony of a witness's experience, either verbal testimony in court or written testimony in a recorded deposition.
35. A, B. If your organization depends on custom-developed software or software products produced through outsourced code development, then the risks of that arrangement need to be evaluated and mitigated. First, the quality and security of the code needs to be assessed. Second, if the third-party development group goes out of business, can you continue to operate with the code as is? You may need to abandon the existing code to switch to a new development group. It is not true that third-party code development is always more expensive; it is often less expensive. A software escrow agreement (SEA) is not an issue that John would want to bring

up as a reason to keep development in-house, since a SEA is a means to reduce the risk of a third-party developer group ceasing to exist.

36. D. `HTTPS://` is the correct prefix for the use of HTTP (Hypertext Transfer Protocol) over TLS (Transport Layer Security). This was the same prefix when SSL (Secure Sockets Layer) was used to encrypt HTTP, but SSL has been deprecated. `SHTTP://` is for Secure HTTP, which was SSH, but SHTTP is also deprecated. `TLS://` is an invalid prefix. `FTPS://` is a valid prefix that can be used in some web browsers, and it uses TLS to encrypt the connection, but it is for securing FTP file exchange rather than web communications.

37. C. The CSO in this scenario is demonstrating the need to follow the security principle of change management. Change management usually involves extensive planning, testing, logging, auditing, and monitoring of activities related to security controls and mechanisms. This scenario is not describing a BCP event. A BCP event would involve the evaluation of threats to business processes and then the creation of response scenarios to address those issues. This scenario is not describing onboarding. Onboarding is the process of integrating a new element (such as an employee or device) into an existing system of security infrastructure. Although loosely similar to change management, onboarding focuses more on ensuring compliance with existing security policies by the new member, rather than testing updates for an existing member. Static analysis is used to evaluate source code as a part of a secure development environment. Static analysis may be used as an evaluation tool in change management, but it is a tool, not the principle of security referenced in this scenario.

38. D. The two main types of token devices are TOTP and HOTP. Time-based one-time password (TOTP) tokens or synchronous dynamic password tokens are devices or applications that generate passwords at fixed time intervals, such as every 60 seconds. Thus, TOTP produces new time-derived passwords on a specific time interval that can be used only a single time when attempting to authenticate. HMAC-based one-time password

(HOTP) tokens or asynchronous dynamic password tokens are devices or applications that generate passwords not based on fixed time intervals but instead based on a nonrepeating one-way function, such as a hash or hash-based message authentication code (HMAC—a type of hash that uses a symmetric key in the hashing process) operation. HMAC is a hashing function, not a means to authenticate. Security Assertions Markup Language (SAML) is used to create authentication federation (i.e., sharing) links; it is not itself a means to authenticate.

39. A. The most important security concern from this list of options in relation to a CSP is the data retention policy. The data retention policy defines what information or data is being collected by the CSP, how long it will be kept, how it is destroyed, why it is kept, and who can access it. The number of customers and what hardware is used are not significant security concerns in comparison to data retention. Whether the CSP offers MaaS, IDaaS, and SaaS is not as important as data retention, especially if these are not services your organization needs or wants. One of the keys to answering this question is to consider the range of CSP options, including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), and the type of organizations that are technically CSP SaaS but that we don't often think of as such (examples include Facebook, Google, and Amazon). These organizations absolutely have access to customer/user data, and thus, their data retention policies are of utmost concern (at least compared to the other options provided).

40. B, C, D. Programmers need to adopt secure coding practices, which include using stored procedures, code signing, and server-side validation. A stored procedure is a subroutine or software module that can be called on or accessed by applications interacting with a relational database management system (RDBMS). Code signing is the activity of crafting a digital signature of a software program in order to confirm that it was not changed and who it is from. Server-side data validation is suited for protecting a system against input submitted by a malicious user. Using immutable systems is not a secure coding

technique; instead, an immutable system is a server or software product that, once configured and deployed, is never altered in place. File size optimization may be efficient but is not necessarily a secure coding technique. Using third-party software libraries may reduce workload to minimize the amount of new code to author, but third-party software libraries are a risk because they can introduce vulnerabilities, especially when closed source libraries are used. Thus, use of third-party software libraries is not a secure coding technique unless the security posture of the externally sourced code is verified, which was not mentioned as an answer option.

Chapter 1
Security Governance Through Principles and Policies

THE CISSP TOPICS COVERED IN THIS CHAPTER INCLUDE:

- ✓ **Domain 1.0: Security and Risk Management**
  - 1.2 Understand and apply security concepts
    - 1.2.1 Confidentiality, integrity, and availability, authenticity, and nonrepudiation (5 Pillars of Information Security)
  - 1.3 Evaluate and apply security governance principles
    - 1.3.1 Alignment of the security function to business strategy, goals, mission, and objectives
    - 1.3.2 Organizational processes (e.g., acquisitions, divestitures, governance committees)
    - 1.3.3 Organizational roles and responsibilities
    - 1.3.4 Security control frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI), Federal Risk and Authorization Management Program (FedRAMP))
    - 1.3.5 Due care/due diligence
  - 1.6 Develop, document, and implement security policy, standards, procedures, and guidelines
  - 1.10 Understand and apply threat modeling concepts and methodologies
  - 1.11 Apply supply chain risk management (SCRM) concepts
    - 1.11.1 Risks associated with the acquisition of products and services from suppliers and providers (e.g., product tampering, counterfeits, implants)

- 1.11.2 Risk mitigations (e.g., third-party assessment and monitoring, minimum security requirements, service level requirements, silicon root of trust, physically unclonable function, software bill of materials)

✓ **Domain 3.0 Security Architecture and Engineering**

- 3.1 Research, implement, and manage engineering processes using secure design principles
  - 3.1.1 Threat modeling
  - 3.1.3 Defense in depth

The Security and Risk Management domain encompasses many of the foundational elements of security solutions. Additional elements of this domain are discussed in various chapters:

- Chapter 2, "Personnel Security and Risk Management Concepts"
- Chapter 3, "Business Continuity Planning"
- Chapter 4, "Laws, Regulations, and Compliance"
- Chapter 19, "Investigations and Ethics"

Please review all these chapters to have a complete perspective on the topics of this domain.

Security 101

We often hear how important security is, but we don't always understand why. Security is essential because it helps to ensure that an organization can continue to exist and operate despite any attempts to steal its data or compromise its physical or logical elements. Security is an element of business management rather than only an IT concern. Furthermore, IT and security are different. *Information technology (IT)* or even *information systems (IS)* is the hardware and software that support the operations or functions of a business. Security is the business management tool that ensures the

reliable and protected operation of IT/IS. Security exists to support the organization's objectives, mission, and goals.

Generally, a security framework that provides a starting point for implementing security should be adopted. Once security is initiated, fine-tuning that security is accomplished through continuous evaluation and stress testing. There are three common types of security evaluation: risk assessment, vulnerability assessment, and penetration testing (these are covered in detail in Chapter 2 and Chapter 15, "Security Assessment and Testing"). *Risk assessment* is identifying assets, threats, and vulnerabilities to calculate risk. Once risk is understood, it is used to guide the improvement of the existing security infrastructure. *Vulnerability assessment* uses automated tools to locate known security weaknesses, which can be addressed by adding more defenses or adjusting the current protections. *Penetration testing* uses trusted teams to stress-test the security infrastructure to find issues that may not be discovered by the prior two means and to find those concerns before an adversary takes advantage of them.

Security should be cost-effective. Organizations do not have infinite budgets and, thus, must allocate their funds appropriately. Additionally, an organizational budget includes a percentage of monies dedicated to security, just as most other business tasks and processes require capital, not to mention payments to employees, insurance, retirement, etc. You should select security controls that provide the most significant protection for the lowest resource cost.

Security should be legally defensible. The laws of your jurisdiction are the backstop of organizational security. When someone intrudes into your environment and breaches security, especially when such activities are illegal, prosecution in court may be the only available response for compensation or closure. Also, many decisions made by an organization will have legal liability issues. If required to defend a security action in the courtroom, legally supported security will go a long way toward protecting your organization from facing significant fines, penalties, or charges of negligence.

Security is a journey, not a finish line. It is not a process that will ever be concluded. It is impossible to fully secure something because security issues are always changing. Our deployed technology is

changing with the passage of time, by users' activities, and by adversaries discovering flaws and developing exploits. The defenses that were sufficient yesterday may not be sufficient tomorrow. As new vulnerabilities are discovered, new means of attack are crafted, and new exploits are built, we have to respond by reassessing our security infrastructure and responding appropriately.

Understand and Apply Security Concepts

Security management concepts and principles are inherent elements in a security policy and solution deployment. They define the basic parameters needed for a secure environment. They also define the goals and objectives that both policy designers and system implementers must achieve to create a secure solution.

The 5 Pillars of Information Security are confidentiality, integrity, availability, authenticity, and nonrepudiation. The first three of these, namely confidentiality, integrity, and availability, are so commonly discussed as a group they have been labeled with their own phrase, the *CIA Triad*. The elements of the CIA Triad are often perceived as the primary goals and objectives of a security infrastructure (see Figure 1.1).

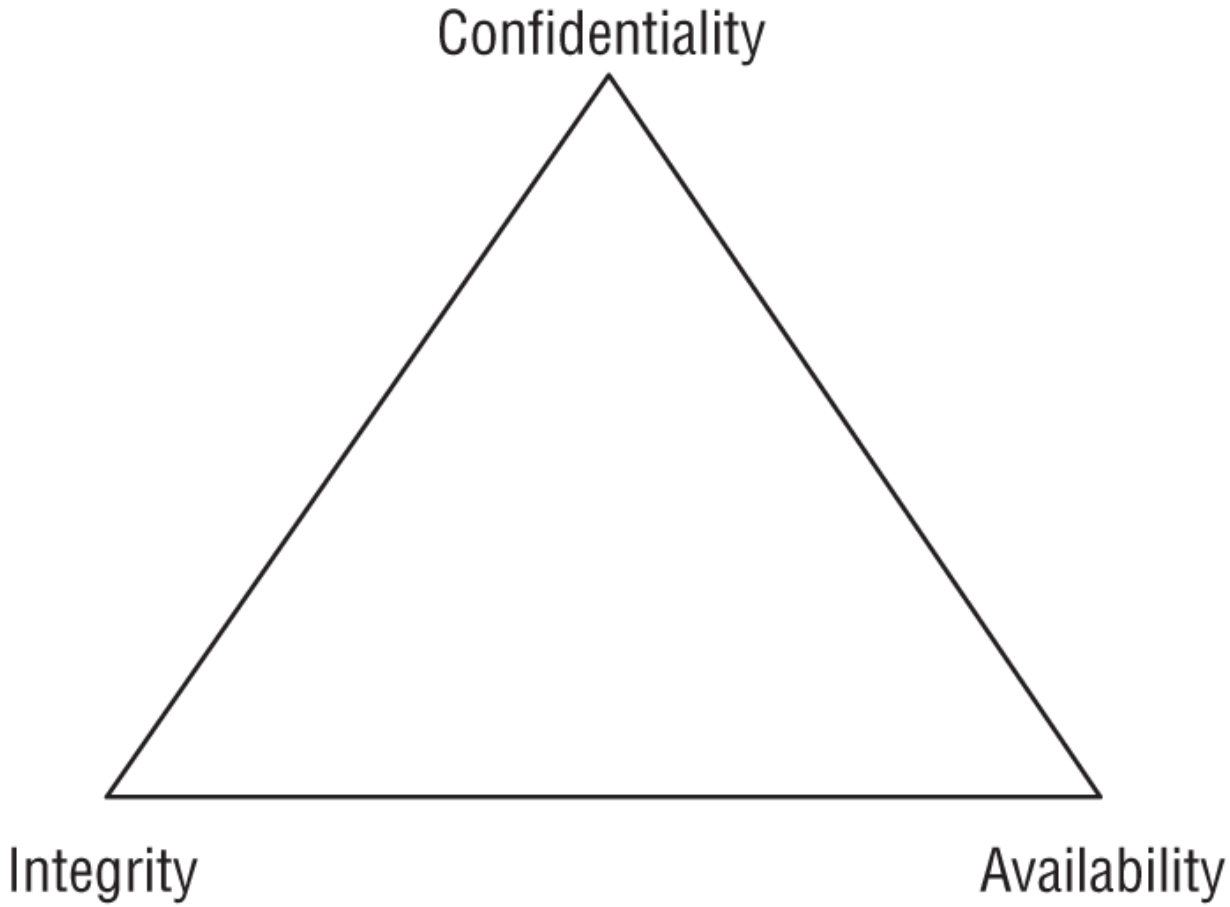

FIGURE 1.1 The CIA Triad

Security controls are typically evaluated on how well they address these three core information security tenets. Vulnerabilities and risks are also evaluated based on the threat they pose against one or more of the CIA Triad principles.

Confidentiality

The first principle of the CIA Triad is confidentiality. *Confidentiality* is the concept of the measures used to ensure the protection of the secrecy of data, objects, or resources. The goal of confidentiality protection is to prevent or minimize unauthorized access to data. Confidentiality protections prevent disclosure while protecting authorized access.

Violations of confidentiality are not limited to directed intentional attacks. Many instances of unauthorized disclosure of sensitive or confidential information are the result of human error, oversight, or

ineptitude. Confidentiality violations can result from the actions of an end user or a system administrator. They can also occur because of an oversight in a security policy or a misconfigured security control.

Numerous countermeasures can help ensure confidentiality against possible threats. These include encryption, network traffic padding, strict access control, rigorous authentication procedures, data classification, and extensive personnel training.

Concepts, conditions, and aspects of confidentiality include the following:

Sensitivity *Sensitivity* refers to the quality of information that could cause harm or damage if disclosed.

Discretion *Discretion* is a decision where an operator can influence or control disclosure to minimize harm or damage.

Criticality The level to which information is mission critical is its measure of *criticality*. The higher the level of criticality, the more likely the need to maintain the confidentiality of the information.

Concealment *Concealment* is the act of hiding or preventing disclosure. Concealment is often viewed as a means of cover, obfuscation, or distraction. A related concept to concealment is *security through obscurity*, which attempts to gain protection through hiding, silence, or secrecy.

Secrecy *Secrecy* is the act of keeping something a secret or preventing the disclosure of information.

Privacy *Privacy* refers to keeping information confidential that is personally identifiable or that might cause harm, embarrassment, or disgrace to someone if revealed.

Seclusion *Seclusion* involves storing something in an out-of-the-way location, likely with strict access controls.

Isolation *Isolation* is the act of keeping something separated from others.

Organizations should evaluate the nuances of confidentiality they wish to enforce. Tools and technology that implement one form of confidentiality might not support or allow other forms.

Integrity

Integrity is the concept of protecting the reliability and correctness of data. Integrity protection prevents unauthorized alterations of data. Properly implemented integrity protection provides a means for authorized changes while protecting against intended and malicious unauthorized activities (such as viruses and intrusions) and mistakes made by authorized users (such as accidents or oversights).

Integrity can be examined from three perspectives:

- Preventing unauthorized subjects from making modifications
- Preventing authorized subjects from making unauthorized modifications, such as mistakes
- Maintaining the internal and external consistency of objects so that their data is a correct and true reflection of the real world and any relationship with any other object is valid, consistent, and verifiable

For integrity to be maintained on a system, controls must be in place to restrict access to data, objects, and resources. Maintaining and validating object integrity across storage, transport, and processing requires numerous variations of controls and oversight.

Numerous attacks focus on the violation of integrity. These include viruses, logic bombs, unauthorized access, errors in coding and applications, malicious modification, intentional replacement, and system backdoors.

Human error, oversight, or ineptitude accounts for many instances of unauthorized alteration of sensitive information. They can also occur because of an oversight in a security policy or a misconfigured security control.

Numerous countermeasures can ensure integrity against possible threats. These include strict access control, rigorous authentication

procedures, intrusion detection systems, object/data encryption, hash verifications (see Chapter 6, "Cryptography and Symmetric Key Algorithms," and Chapter 7, "PKI and Cryptographic Applications"), interface restrictions, input/function checks, and extensive personnel training.

Concepts, conditions, and aspects of integrity include the following:

- *Accuracy*: Being correct and precise
- *Truthfulness*: Being a true reflection of reality
- *Validity*: Being factually or logically sound
- *Accountability*: Being responsible or obligated for actions and results
- *Responsibility*: Being in charge or having control over something or someone
- *Completeness*: Having all necessary components or parts
- *Comprehensiveness*: Being complete in scope; the full inclusion of all needed elements

Availability

Availability means authorized subjects are granted timely and uninterrupted access to objects. Often, availability protection controls support sufficient bandwidth and timeliness of processing as deemed necessary by the organization or situation. Availability includes efficient, uninterrupted access to objects and prevention of denial-of-service (DoS) attacks. Availability also implies that the supporting infrastructure—including network services, communications, and access control mechanisms—is functional and allows authorized users to gain access.

For availability to be maintained on a system, controls must be in place to ensure authorized access and an acceptable level of performance, to quickly handle interruptions, provide for redundancy, maintain reliable backups, and prevent data loss or destruction.

There are numerous threats to availability. These include device failure, software errors, and environmental issues (heat, static electricity, flooding, power loss, and so on). Some forms of attack focus on the violation of availability, including DoS attacks, object destruction, and communication interruptions.

Many availability breaches are caused by human error, oversight, or ineptitude. They can also occur because of an oversight in a security policy or a misconfigured security control.

Numerous countermeasures can ensure availability against possible threats. These include designing intermediary delivery systems properly, using access controls effectively, monitoring performance and network traffic, using firewalls and routers to prevent DoS attacks, implementing redundancy for critical systems, and maintaining and testing backup systems. Most security policies, as well as business continuity planning (BCP), focus on the use of fault tolerance features at the various levels of access/storage/security (that is, disk, server, or site) with the goal of eliminating single points of failure to maintain the availability of critical systems.

Availability depends on both integrity and confidentiality. Without integrity and confidentiality, availability cannot be maintained.

Concepts, conditions, and aspects of availability include the following:

- *Usability*: The state of being easy to use or learn or being able to be understood and controlled by a subject
- *Accessibility*: The assurance that the widest range of subjects can interact with a resource regardless of their capabilities or limitations
- *Timeliness*: Being prompt, on time, within a reasonable time frame, or providing a low-latency response

DAD, Overprotection, Authenticity, Nonrepudiation, and AAA Services

In addition to the CIA Triad, you need to consider a plethora of other security-related concepts and principles when designing a security

policy and deploying a security solution. These include the DAD Triad, the risks of overprotection, authenticity, nonrepudiation, and AAA services.

One interesting security concept is the opposite of the CIA Triad, which is the DAD Triad. Disclosure, alteration, and destruction make up the *DAD Triad*. The DAD Triad represents the failures of security protections in the CIA Triad. It may be useful to recognize what to look for when a security mechanism fails. Disclosure occurs when sensitive or confidential material is accessed by unauthorized entities. It is a violation of confidentiality. Alteration occurs when data is either maliciously or accidentally changed. It is a violation of integrity. Destruction occurs when a resource is damaged or made inaccessible to authorized users (technically, we usually call the latter denial of service [DoS]). Destruction is a violation of availability.

It may also be worthwhile to know that too much security can be its own problem. Overprotecting confidentiality can result in a restriction of availability. Overprotecting integrity can result in a restriction of availability. Overproviding availability can result in a loss of confidentiality and integrity.

Authenticity is the security concept that data is authentic or genuine and originates from its alleged source. This is related to integrity but more closely related to verifying that it is from a claimed origin. When data has authenticity, the recipient can have a high level of confidence that the data is from whom it claims to be and did not change in transit (or storage).

Nonrepudiation ensures that the subject of an activity or who caused an event cannot deny that the event occurred. Nonrepudiation prevents a subject from claiming not to have sent a message, not to have performed an action, or not to have been the cause of an event. It is made possible through identification, authentication, authorization, auditing, and accounting. Nonrepudiation can be established using digital certificates, session identifiers, transaction logs, and numerous other transactional and access control mechanisms. A system built without proper enforcement of nonrepudiation does not provide verification that a specific entity performed a certain action. Nonrepudiation is an essential part of

accounting. A suspect cannot be held accountable if they can repudiate the claim against them.

AAA services are a core security mechanism of all security environments. The three As in this abbreviation refer to authentication, authorization, and accounting (or sometimes auditing). However, what is not as clear is that although there are three letters in the acronym, it actually refers to five elements: identification, authentication, authorization, auditing, and accounting. These five elements represent the following processes of security:

Identification *Identification* is claiming to be an identity when attempting to access a secured area or system.

Authentication *Authentication* is proving that you are that claimed identity.

Authorization *Authorization* defines the permissions (i.e., allow/grant and/or deny) of a resource and object access for a specific identity or subject.

Auditing *Auditing* is recording a log of the events and activities related to the system and subjects.

Accounting *Accounting* (aka *accountability*) is reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions, especially violations of organizational security policy.

Although AAA is typically referenced in relation to authentication systems, it is actually a foundational concept for security. Missing any of these five elements can result in an incomplete security mechanism. The following sections discuss identification, authentication, authorization, auditing, and accounting (see Figure 1.2).

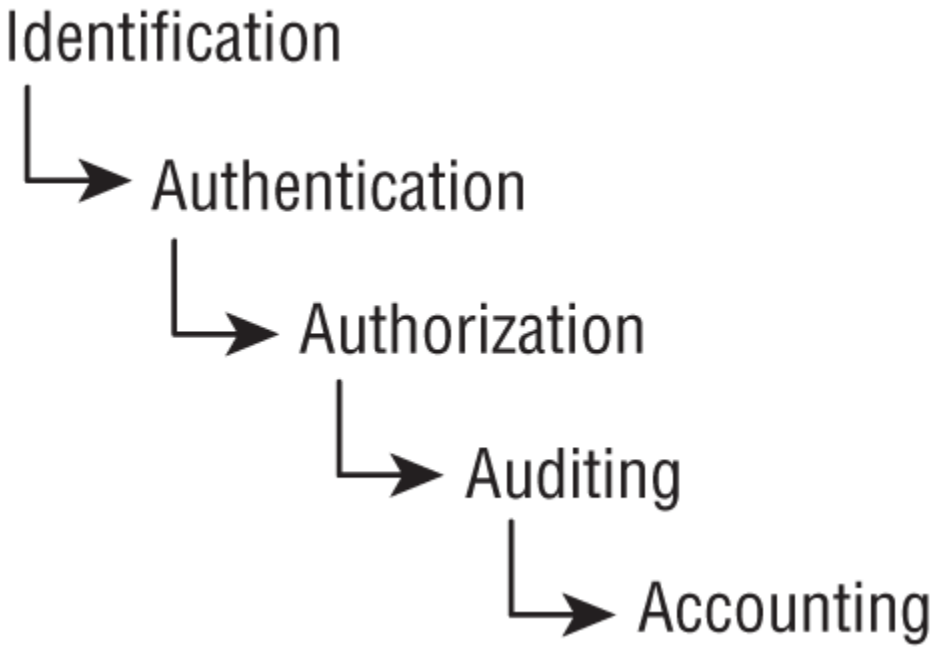

FIGURE 1.2 The five elements of AAA services

Identification

A subject must perform identification to start the process of authentication, authorization, and accounting (AAA). Providing an identity can involve typing in a username; swiping a smartcard; waving a proximity device; speaking a phrase; or positioning your face, hand, or finger for a camera or scanning device. Without an identity, a system has no way to correlate an authentication factor with the subject.

Once a subject has been identified (that is, once the subject's identity has been recognized and verified), the identity is accountable for any further actions by that subject. IT systems track activity by identities, not by the subjects themselves. A computer doesn't know one individual from another, but it does know that your user account is different from all other user accounts. Simply claiming an identity does not imply access, authorization, or authority. The identity must be proven before use is allowed or access is granted. That process is authentication.

Authentication

The process of verifying whether a claimed identity is valid is authentication. Authentication requires the subject to provide additional information that corresponds to the identity they are claiming. The most common form of authentication is using a password. Authentication verifies the identity of the subject by comparing one or more factors against the database of valid identities (that is, user accounts). The capability of the subject and system to maintain the secrecy of the authentication factors for identities directly reflects the level of security of that system.

Identification and authentication are often used together as a single two-step process. Providing an identity is the first step, and providing the authentication factors is the second step. Without both, a subject cannot gain access to a system—neither element alone is useful in terms of security. In some systems, it may seem as if you are providing only one element but gaining access, such as when keying in an ID code or a PIN. However, in these cases, either the identification is handled by another means, such as physical location, or authentication is assumed by your ability to access the system physically. Both identification and authentication take place, but you might not be as aware of them as when you manually type in both a username and a password.

Each authentication technique or factor has its unique benefits and drawbacks. Thus, it is important to evaluate each mechanism in light of the environment in which it will be deployed to determine viability. We discuss authentication at length in Chapter 13, "Managing Identity and Authentication."

Authorization

Once a subject is authenticated, access must be authorized. The process of authorization ensures that the requested activity or access to an object is possible, given the rights and privileges assigned to the authenticated identity. In most cases, the system evaluates the subject, the object, and the assigned permissions related to the intended activity. If the specific action is allowed, the subject is authorized. If the specific action is not allowed, the subject is not authorized.

Keep in mind that just because a subject has been identified and authenticated does not mean they have been authorized to perform any function or access all resources within the controlled environment. Identification and authentication are all-or-nothing aspects of access control. Authorization has a wide range of variations between all or nothing for each object within the environment. A user may be able to read a file but not delete it, print a document but not alter the print queue, or log on to a system but not access any resources. Authorization is discussed in Chapter 13.

Auditing

Auditing is the programmatic means by which a subject's actions are tracked and recorded to hold the subject accountable for their actions while authenticated on a system through the documentation or recording of subject activities. It is also the process of detecting unauthorized or abnormal activities on a system. Auditing is recording the activities of a subject and its objects and the activities of application and system functions. Log files provide an audit trail for re-creating the history of an event, intrusion, or system failure. Auditing is needed to detect malicious actions by subjects, attempted intrusions, and system failures. Auditing is also necessary to reconstruct timelines of compromise events, provide evidence for prosecution, and produce problem reports and analyses. Auditing is usually a native feature of operating systems and most applications and services. Thus, configuring the system to record information about specific types of events is fairly straightforward.

Monitoring is part of what is needed for audits, and audit logs are part of a monitoring system, but the two terms have different meanings. Monitoring is a type of watching or oversight, whereas auditing is recording the information into a record or file. It is possible to monitor without auditing, but you can't audit without some form of monitoring.

Accounting

An organization's security policy can be properly enforced only if accounting is maintained. In other words, you can maintain security only if subjects are held accountable for their actions. Effective accounting relies on the capability to prove a subject's identity and track their activities. Accountability is established by linking an individual to the activities of an online identity through the security services and mechanisms of auditing, authorization, authentication, and identification. Thus, individual accountability is ultimately dependent on the strength of these processes. Without a strong authentication process, there is doubt that the person associated with a specific user account was the actual entity controlling that user account when the undesired action took place.

To have viable accountability, you must be able to support your security decisions and their implementation in a court of law. If you are unable to legally support your security efforts, then you will be unlikely to be able to hold an individual accountable for actions linked to a user account. With only a password as authentication, there is significant room for doubt. Passwords are the least secure form of authentication, with dozens of different methods available to compromise them. However, with the use of multifactor authentication (MFA), such as a password, smartcard, and fingerprint scan in combination, there is very little possibility that any other individual could have compromised the authentication process in order to impersonate the person responsible for the user account.

Protection Mechanisms

Another aspect of understanding and applying security controls is the concept of protection mechanisms or protection controls. Not all security controls must have them, but many controls offer their protection through the use of these mechanisms. Some common examples of these mechanisms are defense in depth, abstraction, data hiding, and using encryption.

Defense in Depth

Defense in depth, also known as *layering*, is the use of multiple controls in a series. No one control can protect against all possible threats. Using a multilayered solution allows for numerous different controls to guard against whatever threats come to pass. When security solutions are designed in layers, a single failed control should not result in the exposure of systems or data.

Using layers in a series rather than in parallel is important. Performing security restrictions in a series means linearly enforcing one after the other. Only through a series configuration will each attack be scanned, evaluated, or mitigated by every security control. In a series configuration, failure of a single security control does not render the entire solution ineffective. If security controls were implemented in parallel, a threat could pass through a single checkpoint that did not address its particular malicious activity.

Serial configurations are very narrow but deep, whereas parallel configurations are very wide but shallow. Parallel systems are useful in distributed computing applications, but parallelism is not often a useful concept in the realm of security.

Within the context of defense in depth, the terms levels, multilevel, and layers are often used. Additionally, there are numerous other terms that also relate to this concept, including classifications, zones, realms, compartments, silos, segmentations, lattice structures, and protection rings. You will see these terms used often throughout this book. When you see them, think about the concept of defense in depth in relation to the context of where the term is used.

Defense in breadth or *diversity of defense* is also an important related concept to defense in depth. It can be problematic if elements of several security layers are from the same vendor or share common code, since a vulnerability could affect numerous layers simultaneously. Using a range of security products from varied vendors significantly reduces or avoids the risk of a single exploit compromising several layers at once.

Abstraction

Abstraction is used for efficiency. Similar elements are put into groups, classes, or roles that are collectively assigned security controls, restrictions, or permissions. Abstraction simplifies security by enabling you to assign security controls to a group of objects collected by type or function. Thus, the concept of abstraction is used when classifying objects or assigning roles to subjects.

Abstraction is one of the fundamental principles behind the field known as object-oriented programming (OOP). In OOP, the unknown environment doctrine states that users of an object (or operating system component) don't necessarily need to know the details of how the object works; they just need to know the proper syntax for using the object and the type of data that will be returned as a result (that is, how to send input and receive output). This is very much what's involved in mediated access to data or services, such as when user-mode applications use system calls to request administrator-mode services or data (and such mediated access requests may be granted or denied depending on the requester's credentials and permissions) rather than obtaining direct, unmediated access. (See the “Protection Rings” section of Chapter 9, “Security Vulnerabilities, Threats, and Countermeasures,” for more on the topic of mediated access.)

Another way in which abstraction applies to security is the introduction of object groups, sometimes called classes, where access controls and operation rights are assigned to groups of objects rather than on a per-object basis. This approach allows security administrators to define and name groups easily (the names are often related to job roles or responsibilities) and helps make the administration of rights and privileges easier (when you add an object to a class, you confer rights and privileges rather than having to manage rights and privileges for each object separately).

Data Hiding

Data hiding is preventing data from being discovered or accessed by a subject by positioning the data in a logical storage compartment that is not accessible to nor seen by the subject. This means the subject cannot see or access the data, not just that it is unseen. Data

hiding includes keeping a database from being accessed by unauthorized visitors and restricting a subject at a lower classification level from accessing data at a higher classification level. Preventing an application from accessing hardware directly is also a form of data hiding. Data hiding is often a key element in security controls as well as in programming. Steganography is an example of data hiding (see Chapter 7).

Data hiding is a vital characteristic in multilevel secure systems. It ensures that data existing at one level of security is not visible to processes running at different security levels. From a security perspective, data hiding relies on placing objects in security containers different from those that subjects occupy to hide object details from those without the need to know about them or the means to access them.

The term *security through obscurity* may seem relevant here. However, that concept is different. Data hiding is intentionally positioning data so that it is not viewable or accessible to an unauthorized subject, whereas security through obscurity is the idea of not informing a subject about an object being present and thus hoping that the subject will not discover the object. In other words, in security through obscurity, the subject could access the data if they find it. It is digital hide and seek. Security through obscurity does not actually implement any form of protection. It is instead an attempt to hope something important is not discovered by keeping knowledge of it a secret. An example of security though obscurity is when a programmer is aware of a flaw in their software code, but they release the product anyway hoping that no one discovers the issue and exploits it.

Encryption

Encryption is the science of hiding the meaning or intent of a communication from unintended recipients. Encryption can take many forms and should be applied to every type of electronic communication and storage. Encryption is discussed at length in Chapters 6 and 7.

Security Boundaries

A *security boundary* is the line of intersection between areas, subnets, or environments with different security requirements or needs. A security boundary exists between high-security and low-security areas, such as between a LAN (local area network) and the Internet. Recognizing the security boundaries on your network and in the physical world is essential to establishing reliable security barriers. Once you identify a security boundary, you must deploy mechanisms to control the flow of information across that boundary.

Divisions between security areas can take many forms. For example, objects may have different classifications. Each classification defines which subjects can perform functions on which objects. The distinction between classifications is a security boundary.

Security boundaries also exist between the physical environment and the logical environment. To provide logical security, you must provide security mechanisms different from those used to provide physical security. Both must be present to provide a complete security structure, and both must be addressed in a security policy. However, they are different and must be assessed as separate elements of a security solution.

Security boundaries, such as a perimeter between protected and unprotected areas, should always be clearly defined. In a security policy, it's important to state the point at which control ends or begins and to identify that point in both the physical and logical environments. Logical security boundaries are where electronic communications interface with devices or services for which your organization is legally responsible. In most cases, that interface is clearly marked, and unauthorized subjects are informed that they do not have access, and that attempts to gain access will result in prosecution.

The security perimeter in the physical environment often reflects the security perimeter of the logical environment. In most cases, the area for which the organization is legally responsible determines the reach of a security policy in the physical realm. This can be the walls of an office, the walls of a building, or the fence around a campus. In secured environments, warning signs are posted indicating that