"All-in-One Is All You Need."

ALL-IN-ONE

CISSP®

EXAM GUIDE

NINTH EDITION

Online content includes:

- 1400+ practice exam questions
- Graphical question quizzes
- Test engine that provides full-length practice exams and customizable quizzes by chapter or exam domain
- Access to Flash cards

Fully updated coverage of all 8 domains for the 2021 Certified Information Systems Security Professional exam

Ideal as both a study guide and an on-the-job reference

Filled with practice exam questions and in-depth explanations

Mc Graw Hill

FERNANDO MAYMÍ, PhD, CISSP
SHON HARRIS, CISSP

Praise for *CISSP® All-in-One Exam Guide*

Fernando's latest update to the *CISSP All-In-One Exam Guide* continues the tradition started in past collaborations with Shon Harris of breaking down key concepts and critical skills in a way that prepares the reader for the exam. Once again the material proves to be not only a vital asset to exam preparation but a valued resource reference for use well after the exam has been passed.

Stefanie Keuser, CISSP,
Chief Information Officer,
Military Officers Association of America

The *CISSP All-in-One Exam Guide* is the only book one needs to pass the CISSP exam. Fernando Maymí is not just an author, he is a leader in the cybersecurity industry. His insight, knowledge, and expertise is reflected in the content provided in this book. The book will not only give you what you need to pass the exam, it can also be used to help you further your career in cybersecurity.

Marc Coady, CISSP,
Compliance Analyst,
Costco Wholesale

A must-have reference for any cyber security practitioner, this book provides invaluable practical knowledge on the increasingly complex universe of security concepts, controls, and best practices necessary to do business in today's world.

Steve Zalewski,
Former Chief Information Security Officer,
Levi Strauss & Co.

Shon Harris put the CISSP certification on the map with this golden bible of the CISSP. Fernando Maymí carries that legacy forward beautifully with clarity, accuracy, and balance. I am sure that Shon would be proud.

David R. Miller, CISSP, CCSP, GIAC GISP GSEC GISF,
PCI QSA, LPT, ECSA, CEH, CWNA, CCNA, SME, MCT,
MCIT Pro EA, MCSE: Security, CNE, Security+, etc.

An excellent reference. Written clearly and concisely, this book is invaluable to students, educators, and practitioners alike.

Dr. Joe Adams,
Founder and Executive Director,
Michigan Cyber Range

A lucid, enlightening, and comprehensive tour de force through the breadth of cyber security. Maymí and Harris are masters of the craft.

Dr. Greg Conti,
Founder,
Kopidion LLC

I wish I found this book earlier in my career. It certainly was the single tool I used to pass the CISSP exam, but more importantly it has taught me about security from many aspects I did not even comprehend previously. I think the knowledge that I gained from this book is going to help me in many years to come. Terrific book and resource!

Janet Robinson,
Chief Security Officer

ALL ■ IN ■ ONE

CISSP®

EXAM GUIDE

ABOUT THE AUTHORS

Fernando Maymí, PhD, CISSP, is a security practitioner with over 25 years' experience in the field. He is currently Vice President of Training at IronNet Cybersecurity, where, besides developing cyber talent for the company, its partners, and customers, he has led teams providing strategic consultancy, security assessments, red teaming, and cybersecurity exercises around the world. Previously, he led advanced research and development projects at the intersection of artificial intelligence and cybersecurity, stood up the U.S. Army's think tank for strategic cybersecurity issues, and was a West Point faculty member for over 12 years. Fernando worked closely with Shon Harris, advising her on a multitude of projects, including the sixth edition of the *CISSP All-in-One Exam Guide*.

Shon Harris, CISSP, was the founder and CEO of Shon Harris Security LLC and Logical Security LLC, a security consultant, a former engineer in the Air Force's Information Warfare unit, an instructor, and an author. Shon owned and ran her own training and consulting companies for 13 years prior to her death in 2014. She consulted with Fortune 100 corporations and government agencies on extensive security issues. She authored three best-selling CISSP books, was a contributing author to *Gray Hat Hacking: The Ethical Hacker's Handbook* and *Security Information and Event Management (SIEM) Implementation*, and a technical editor for *Information Security Magazine.*

About the Contributor/Technical Editor

Bobby E. Rogers is an information security engineer working as a contractor for Department of Defense agencies, helping to secure, certify, and accredit their information systems. His duties include information system security engineering, risk management, and certification and accreditation efforts. He retired after 21 years in the U.S. Air Force, serving as a network security engineer and instructor, and has secured networks all over the world. Bobby has a master's degree in information assurance (IA) and is pursuing a doctoral degree in cybersecurity from Capitol Technology University in Maryland. His many certifications include CISSP-ISSEP, CEH, and MCSE: Security, as well as the CompTIA A+, Network+, Security+, and Mobility+ certifications.

ALL IN ONE

CISSP®

EXAM GUIDE

Ninth Edition

Fernando Maymí
Shon Harris

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

ISBN: 978-1-26-046736-9
MHID: 1-26-046736-8

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-046737-6, MHID: 1-26-046737-6.

eBook conversion by codeMantra
Version 1.0

We dedicate this book to all those
who have served others selflessly.

This page intentionally left blank

CONTENTS AT A GLANCE

CONTENTS

FROM THE AUTHOR

Thank you for investing your resources in this ninth edition of the *CISSP All-in-One Exam Guide*. I am confident you'll find it helpful, not only as you prepare for the CISSP exam, but as a reference in your future professional endeavors. That was one of the overarching goals of Shon Harris when she wrote the first six editions and is something I've strived to uphold in the last three. It is not always easy, but I think you'll be pleased with how we've balanced these two requirements.

(ISC)^2 does a really good job of grounding the CISSP Common Body of Knowledge (CBK) in real-world applications, but (let's face it) there's always a lot of room for discussion and disagreements. There are very few topics in cybersecurity (or pretty much any other field) on which there is universal agreement. To balance the content of this book between exam preparation and the murkiness of real-world applications, we've included plenty of comments and examples drawn from our experiences.

I say "our experiences" deliberately because the voice of Shon remains vibrant, informative, and entertaining in this edition, years after her passing. I've preserved as many of her insights as possible while ensuring the content is up to date and relevant. I also strove to maintain the conversational tone that was such a hallmark of her work. The result is a book that (I hope) reads more like an essay (or even a story) than a textbook but is grounded in good pedagogy. It should be easy to read but still prepare you for the exam.

Speaking of the exam, the changes that (ISC)^2 made to the CBK in 2021 are not dramatic but are still significant. Each domain was tweaked in some way, and seven of the eight domains had multiple topics added (domain 1 was the exception here). These changes, coupled with the number of topics that were growing stale in the eighth edition of this book, prompted me to completely restructure this edition. I tore each domain and topic down to atomic particles and then re-engineered the entire book to integrate the new objectives, which are listed in Table 1.

Domain 2: Asset Security	
2.4	Manage data lifecycle
2.4.1	Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
2.4.3	Data location
2.4.4	Data maintenance
2.5	Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))
Domain 3: Security Architecture and Engineering	
(Under 3.7 Understand methods of cryptanalytic attacks)	
3.7.1	Brute force
3.7.4	Frequency analysis

Table 1 CBK 2021: New Objectives (*continued*)

Domain 3: Security Architecture and Engineering	
3.7.6	Implementation attacks
3.7.8	Fault injection
3.7.9	Timing
3.7.10	Man-in-the-Middle (MITM)
3.7.11	Pass the hash
3.7.12	Kerberos exploitation
3.7.13	Ransomware
(Under 3.9 Design site and facility security controls)	
3.9.9	Power (e.g., redundant, backup)
Domain 4: Communication and Network Security	
(Under 4.1 Assess and implement secure design principles in network architectures)	
4.1.3	Secure protocols
4.1.6	Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
4.1.8	Cellular networks (e.g., 4G, 5G)
(Under 4.3 Implement secure communication channels according to design)	
4.3.6	Third-party connectivity
Domain 5: Identity and Access Management (IAM)	
(Under 5.1 Control physical and logical access to assets)	
5.1.5	Applications
(Under 5.2 Manage identification and authentication of people, devices, and services)	
5.2.8	Single Sign On (SSO)
5.2.9	Just-In-Time (JIT)
(Under 5.4 Implement and manage authorization mechanisms)	
5.4.6	Risk based access control
(Under 5.5 Manage the identity and access provisioning lifecycle)	
5.5.3	Role definition (e.g., people assigned to new roles)
5.5.4	Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)
5.6	Implement authentication systems
5.6.1	OpenID Connect (OIDC)/Open Authorization (OAuth)
5.6.2	Security Assertion Markup Language (SAML)
5.6.3	Kerberos
5.6.4	Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)
Domain 6: Security Assessment and Testing	
(Under 6.2 Conduct security control testing)	
6.2.9	Breach attack simulations
6.2.10	Compliance checks

Table 1 CBK 2021: New Objectives

Domain 6: Security Assessment and Testing	
(Under 6.3 Collect security process data (e.g., technical and administrative))	
6.3.6	Disaster Recovery (DR) and Business Continuity (BC)
(Under 6.4 Analyze test output and generate report)	
6.4.1	Remediation
6.4.2	Exception handling
6.4.3	Ethical disclosure
Domain 7: Security Operations	
(Under 7.1 Understand and comply with investigations)	
7.1.5	Artifacts (e.g., computer, network, mobile device)
(Under 7.2 Conduct logging and monitoring activities)	
7.2.5	Log management
7.2.6	Threat intelligence (e.g., threat feeds, threat hunting)
7.2.7	User and Entity Behavior Analytics (UEBA)
(Under 7.7 Operate and maintain detective and preventative measures)	
7.7.8	Machine learning and Artificial Intelligence (AI) based tools
(Under 7.11 Implement Disaster Recovery (DR) processes)	
7.11.7	Lessons learned
Domain 8: Software Development Security	
(Under 8.2 Identify and apply security controls in software development ecosystems)	
8.2.1	Programming languages
8.2.2	Libraries
8.2.3	Tool sets
8.2.5	Runtime
8.2.6	Continuous Integration and Continuous Delivery (CI/CD)
8.2.7	Security Orchestration, Automation, and Response (SOAR)
8.2.10	Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))
(Under 8.4 Assess security impact of acquired software)	
8.4.1	Commercial-off-the-shelf (COTS)
8.4.2	Open source
8.4.3	Third-party
8.4.4	Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
(Under 8.5 Define and apply secure coding guidelines and standards)	
8.5.4	Software-defined security

Table 1 CBK 2021: New Objectives (*continued*)

Note that some of these objectives were implicit in the previous (2018) version of the CBK and were therefore covered in the eighth edition of this book. The fact that they are now explicit is an indication of their increased importance both in the exam and in the real world. (Please pay particular attention to these as you prepare for the exam.) All in all, this ninth edition is significantly different (and improved) when compared to the previous one. I think you'll agree. Thank you, again, for investing in this ninth edition.

ACKNOWLEDGMENTS

I would like to thank all the people who work in the information security industry who are driven by their passion, dedication, and a true sense of doing right. These selfless professionals sacrifice their personal time to prevent, block, and respond to the relentless efforts of malicious actors around the world. We all sleep more peacefully at night because you remain at the ready.

In this ninth edition, I would also like to thank the following:

- Ronald C. Dodge, Jr., who introduced me to Shon Harris and, in so doing, started me off on one of the best adventures of my life
- Kathy Conlon, who, more than anyone else, set the conditions that led to nine editions of this book
- Carol Remicci
- David Harris
- The men and women of our armed forces, who selflessly defend our way of life

This page intentionally left blank

WHY BECOME A CISSP?

As our world changes, the need for improvements in security and technology continues to grow. Organizations around the globe are desperate to identify and recruit talented and experienced security professionals to help protect their assets and remain competitive. As a Certified Information Systems Security Professional (CISSP), you will be seen as a security professional of proven ability who has successfully met a predefined standard of knowledge and experience that is well understood and respected throughout the industry. By keeping this certification current, you will demonstrate your dedication to staying abreast of security developments.

Consider some of the reasons for attaining a CISSP certification:

- To broaden your current knowledge of security concepts and practices
- To demonstrate your expertise as a seasoned security professional
- To become more marketable in a competitive workforce
- To increase your salary and be eligible for more employment opportunities
- To bring improved security expertise to your current occupation
- To show a dedication to the security discipline

The CISSP certification helps organizations identify which individuals have the ability, knowledge, and experience necessary to implement solid security practices; perform risk analysis; identify necessary countermeasures; and help the organization as a whole protect its facility, network, systems, and information. The CISSP certification also shows potential employers you have achieved a level of proficiency and expertise in skill sets and knowledge required by the security industry. The increasing importance placed on security by organizations of all sizes will only continue in the future, leading to even greater demands for highly skilled security professionals. The CISSP certification shows that a respected third-party organization has recognized an individual's technical and theoretical knowledge and expertise, and distinguishes that individual from those who lack this level of knowledge.

Understanding and implementing security practices is an essential part of being a good network administrator, programmer, or engineer. Job descriptions that do not specifically target security professionals still often require that a potential candidate have a good understanding of security concepts and how to implement them. Due to staff size and budget restraints, many organizations can't afford separate network and security staffs. But they still believe security is vital to their organization. Thus, they often try to combine knowledge of technology and security into a single role. With a CISSP designation, you can put yourself head and shoulders above other individuals in this regard.

The CISSP Exam

Because the CISSP exam covers the eight domains making up the CISSP CBK, it is often described as being "an inch deep and a mile wide," a reference to the fact that many questions on the exam are not very detailed and do not require you to be an expert in every subject. However, the questions do require you to be familiar with many *different* security subjects.

The CISSP exam comes in two versions depending on the language in which the test is written. The English version uses Computerized Adaptive Testing (CAT) in which the number of questions you are asked depends on your measured level of knowledge but ranges from 100 to 150. Of these, 25 questions will not count toward your score, as they are being evaluated for inclusion in future exams (this is why they are sometimes called pre-test questions). Essentially, the easier it is for the test software to determine your level of proficiency, the fewer questions you'll get. Regardless of how many questions you are presented, though, you will have no more than three hours to complete the test. When the system has successfully assessed your level of knowledge, the test will end regardless of how long you've been at it.

EXAM TIP CAT questions are intentionally designed to "feel" hard (based on the system's estimate of your knowledge), so don't be discouraged. Just don't get bogged down because you must answer at least 100 questions in three hours.

The non-English version of the CISSP exam is also computer-based but is linear, fixed-form (not adaptive) and comprises 250 questions, which must be answered in no more than six hours. Like the CAT version, 25 questions are pre-test (unscored), so you will be graded on the other 225 questions. The 25 research questions are integrated into the exam, so you won't know which go toward your final grade.

Regardless of which version of the exam you take, you need a score of 700 points out of a possible 1,000. In both versions, you can expect multiple choice and innovative questions. Innovative questions incorporate drag-and-drop (i.e., take a term or item and drag it to the correct position in the frame) or hotspot (i.e., click the item or term that correctly answers the question) interfaces, but are otherwise weighed and scored just like any other question. The questions are pulled from a much larger question bank to ensure the exam is as unique as possible for each examinee. In addition, the test bank constantly changes and evolves to more accurately reflect the real world of security. The exam questions are continually rotated and replaced in the bank as necessary. Questions are weighted based on their difficulty; not all questions are worth the same number of points. The exam is not product or vendor oriented, meaning no questions will be specific to certain products or vendors (for instance, Windows, Unix, or Cisco). Instead, you will be tested on the security models and methodologies used by these types of systems.

EXAM TIP There is no penalty for guessing. If you can't come up with the right answer in a reasonable amount of time, then you should guess and move on to the next question.

$(ISC)^2$, which stands for International Information Systems Security Certification Consortium, also includes scenario-based questions in the CISSP exam. These questions

present a short scenario to the test taker rather than asking the test taker to identify terms and/or concepts. The goal of the scenario-based questions is to ensure that test takers not only know and understand the concepts within the CBK but also can apply this knowledge to real-life situations. This is more practical because in the real world you won't be challenged by having someone asking you, "What is the definition of collusion?" You need to know how to detect and prevent collusion from taking place, in addition to knowing the definition of the term.

After passing the exam, you will be asked to supply documentation, supported by a sponsor, proving that you indeed have the type of experience required to obtain CISSP certification. The sponsor must sign a document vouching for the security experience you are submitting. So, make sure you have this sponsor lined up prior to registering for the exam and providing payment. You don't want to pay for and pass the exam, only to find you can't find a sponsor for the final step needed to achieve your certification.

The reason behind the sponsorship requirement is to ensure that those who achieve the certification have real-world experience to offer organizations. Book knowledge is extremely important for understanding theory, concepts, standards, and regulations, but it can never replace hands-on experience. Proving your practical experience supports the relevance of the certification.

A small sample group of individuals selected at random will be audited after passing the exam. The audit consists mainly of individuals from $(ISC)^2$ calling on the candidates' sponsors and contacts to verify the test taker's related experience.

One of the factors that makes the CISSP exam challenging is that most candidates, although they work in the security field, are not necessarily familiar with all eight CBK domains. If a security professional is considered an expert in vulnerability testing or application security, for example, she may not be familiar with physical security, cryptography, or forensics. Thus, studying for this exam will broaden your knowledge of the security field.

The exam questions address the eight CBK security domains, which are described in Table 2.

Domain	Description
Security and Risk Management	This domain covers many of the foundational concepts of information systems security. Some of the topics covered include • Professional ethics • Security governance and compliance • Legal and regulatory issues • Personnel security policies • Risk management
Asset Security	This domain examines the protection of assets throughout their life cycle. Some of the topics covered include • Identifying and classifying information and assets • Establishing information and asset handling requirements • Provisioning resources securely • Managing the data life cycle • Determining data security controls and compliance requirements

Table 2 Security Domains that Make Up the CISSP CBK (*continued*)

Domain	Description
Security Architecture and Engineering	This domain examines the development of information systems that remain secure in the face of a myriad of threats. Some of the topics covered include • Secure design principles • Security models • Selection of effective controls • Cryptography • Physical security
Communication and Network Security	This domain examines network architectures, communications technologies, and network protocols with the goal of understanding how to secure them. Some of the topics covered include • Secure network architectures • Secure network components • Secure communications channels
Identity and Access Management (IAM)	Identity and access management is one of the most important topics in information security. This domain covers the interactions between users and systems as well as between systems and other systems. Some of the topics covered include • Controlling physical and logical access to assets • Identification and authentication • Authorization mechanisms • Identity and access provisioning life cycle • Implementing authentication systems
Security Assessment and Testing	This domain examines ways to verify the security of our information systems. Some of the topics covered include • Assessment and testing strategies • Testing security controls • Collecting security process data • Analyzing and reporting results • Conducting and facilitating audits
Security Operations	This domain covers the many activities involved in the daily business of maintaining the security of our networks. Some of the topics covered include • Investigations • Logging and monitoring • Change and configuration management • Incident management • Disaster recovery
Software Development Security	This domain examines the application of security principles to the acquisition and development of software systems. Some of the topics covered include • The software development life cycle • Security controls in software development • Assessing software security • Assessing the security implications of acquired software • Secure coding guidelines and standards

Table 2 Security Domains that Make Up the CISSP CBK (*continued*)

What Does This Book Cover?

This book covers everything you need to know to become an (ISC)²-certified CISSP. It teaches you the hows and whys behind organizations' development and implementation of policies, procedures, guidelines, and standards. It covers network, application, and system vulnerabilities; what exploits them; and how to counter these threats. This book explains physical security, operational security, and why systems implement the security mechanisms they do. It also reviews the U.S. and international security criteria and evaluations performed on systems for assurance ratings, what these criteria mean, and why they are used. This book also explains the legal and liability issues that surround computer systems and the data they hold, including such subjects as computer crimes, forensics, and what should be done to properly prepare computer evidence associated with these topics for court.

While this book is mainly intended to be used as a study guide for the CISSP exam, it is also a handy reference guide for use after your certification.

Tips for Taking the CISSP Exam

Many people feel as though the exam questions are tricky. Make sure to read each question and its answer choices thoroughly instead of reading a few words and immediately assuming you know what the question is asking. Some of the answer choices may have only subtle differences, so be patient and devote time to reading through the question more than once.

A common complaint heard about the CISSP exam is that some questions seem a bit subjective. For example, whereas it might be easy to answer a technical question that asks for the exact mechanism used in Transport Layer Security (TLS) that protects against man-in-the-middle attacks, it's not quite as easy to answer a question that asks whether an eight-foot perimeter fence provides low, medium, or high security. Many questions ask the test taker to choose the "best" approach, which some people find confusing and subjective. These complaints are mentioned here not to criticize (ISC)² and the exam writers, but to help you better prepare for the exam. This book covers all the necessary material for the exam and contains many questions and self-practice tests. Most of the questions are formatted in such a way as to better prepare you for what you will encounter on the actual exam. So, make sure to read all the material in the book, and pay close attention to the questions and their formats. Even if you know the subject well, you may still get some answers wrong—it is just part of learning how to take tests.

In answering many questions, it is important to keep in mind that some things are inherently more valuable than others. For example, the protection of human lives and welfare will almost always trump all other responses. Similarly, if all other factors are equal and you are given a choice between an expensive and complex solution and a simpler and cheaper one, the second will win most of the time. Expert advice (e.g., from an attorney) is more valuable than that offered by someone with lesser credentials. If one of the possible responses to a question is to seek or obtain advice from an expert, pay close attention to that question. The correct response may very well be to seek out that expert.

Familiarize yourself with industry standards and expand your technical knowledge and methodologies outside the boundaries of what you use today. We cannot stress enough that being the "top dog" in your particular field doesn't mean you are properly prepared for all eight domains the exam covers.

When you take the CISSP exam at the Pearson VUE test center, other certification exams may be taking place simultaneously in the same room. Don't feel rushed if you see others leaving the room early; they may be taking a shorter exam.

How to Use This Book

Much effort has gone into putting all the necessary information into this book. Now it's up to you to study and understand the material and its various concepts. To best benefit from this book, you might want to use the following study method:

- Study each chapter carefully and make sure you understand each concept presented. Many concepts must be fully understood, and glossing over a couple here and there could be detrimental to your success on the exam. The CISSP CBK contains hundreds of individual topics, so take the time needed to understand them all.
- Make sure to study and answer all of the questions. If any questions confuse you, go back and study the corresponding sections again. Remember, you will encounter questions on the actual exam that do not seem straightforward. Do not ignore the confusing questions, thinking they're not well worded. Instead, pay even closer attention to them because they are included for a reason.
- If you are not familiar with specific topics, such as firewalls, laws, physical security, or protocol functionality, use other sources of information (books, articles, and so on) to attain a more in-depth understanding of those subjects. Don't just rely solely on what you think you need to know to pass the CISSP exam.
- After reading this book, study the questions and answers, and take the practice tests. Then review the $(ISC)^2$ exam objectives and make sure you are comfortable with each bullet item presented. If you are not comfortable with some items, revisit the chapters in which they are covered.
- If you have taken other certification exams—such as Cisco or Microsoft—you might be used to having to memorize details and configuration parameters. But remember, the CISSP test is "an inch deep and a mile wide," so make sure you understand the concepts of each subject *before* trying to memorize the small, specific details.
- Remember that the exam is looking for the "best" answer. On some questions test takers do not agree with any or many of the answers. You are being asked to choose the best answer out of the four being offered to you.

PART I

Security and Risk Management

This page intentionally left blank

CHAPTER 1

Cybersecurity Governance

This chapter presents the following:

- Fundamental cybersecurity concepts
- Security governance principles
- Security policies, standards, procedures, and guidelines
- Personnel security policies and procedures
- Security awareness, education, and training

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts.

—Eugene H. Spafford

While some of us may revel in thinking about and implementing cybersecurity, the fact is that most organizations would much rather focus on many other things. Businesses exist to generate profits for their shareholders. Most nonprofit organizations are dedicated to furthering particular social causes such as charity, education, or religion. Apart from security service providers, organizations don't exist specifically to deploy and maintain firewalls, intrusion detection systems, identity management technologies, and encryption devices. No corporation really wants to develop hundreds of security policies, deploy antimalware products, maintain vulnerability management systems, constantly update its incident response capabilities, and have to comply with the myriad of security laws, regulations, and standards that exist worldwide. Business owners would like to be able to make their widgets, sell their widgets, and go home with a nice profit in their pockets. But things are not that simple.

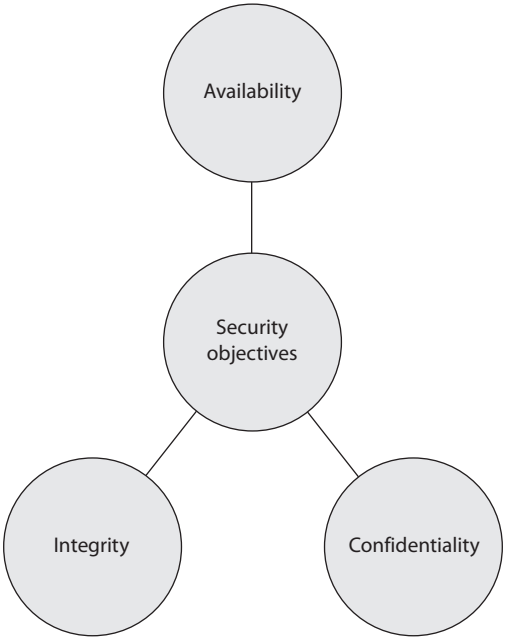
Organizations are increasingly faced with attackers who want to steal customer data to carry out identity theft and banking fraud. Company secrets are commonly being stolen by internal and external entities for economic espionage purposes. Systems are being hijacked and used within botnets to attack other organizations, mine cryptocurrencies, or spread spam. Company funds are being secretly siphoned off through complex and hard-to-identify digital methods, commonly by organized criminal rings in different countries. And organizations that find themselves in the crosshairs of attackers may come under constant attack that brings their systems and websites offline for hours or days. Companies are required to practice a wide range of security disciplines today to keep

their market share, protect their customers and bottom line, stay out of jail, and still sell their widgets.

As we start our exploration of the Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) in this chapter, we will define what cybersecurity means and how it must be governed by, well, CISSPs. Each organization must develop an enterprise-wide security program that consists of technologies, procedures, and processes covered throughout this book. As you go along in your security career, you will find that most organizations have some (but rarely all) pieces to the puzzle of an "enterprise-wide security program" in place. Many of the security programs in place today can be thought of as lopsided or lumpy. The security programs excel within the disciplines that the team is most familiar with, and the other disciplines are found lacking. It is your responsibility to become as well rounded in security as possible so that you can identify these deficiencies in security programs and help improve upon them. This is why the CISSP exam covers a wide variety of technologies, methodologies, and processes—you must know and understand them holistically if you are going to help an organization carry out security holistically.

Fundamental Cybersecurity Concepts and Terms

As cybersecurity professionals, our efforts are ultimately focused on the protection of our information systems. These systems consist of people, processes, and technologies designed to operate on information. To protect them means to ensure the confidentiality, integrity, and availability (the CIA triad) of all assets in our information systems as well as the authenticity and nonrepudiation of tasks performed in them. Each asset will require different levels of these types of protection, as we will see in the following sections.



Confidentiality

Confidentiality means keeping unauthorized entities (be they people or processes) from gaining access to information assets. It ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This level of secrecy should prevail while data resides on systems and devices within the network, as it is transmitted, and once it reaches its destination. Confidentiality can be provided by encrypting data as it is stored and transmitted, by enforcing strict access control and data classification, and by training personnel on the proper data protection procedures.

Attackers can thwart confidentiality mechanisms by network monitoring, shoulder surfing, stealing credentials, breaking encryption schemes, and social engineering. These topics will be addressed in more depth in later chapters, but briefly, *shoulder surfing* is when a person looks over another person's shoulder and watches their keystrokes or views data as it appears on a computer screen. *Social engineering* is when one person tricks another person into sharing confidential information, for example, by posing as someone authorized to have access to that information. Social engineering can take many forms. Any one-to-one communication medium can be used to perform social engineering attacks.

Users can intentionally or accidentally disclose sensitive information by not encrypting it before sending it to another person, by falling prey to a social engineering attack, by sharing a company's trade secrets, or by not using extra care to protect confidential information when processing it.

Integrity

Integrity means that an asset is free from unauthorized alterations. Only authorized entities should be able to modify an asset, and only in specific authorized ways. For example, if you are reviewing orders placed by customers on your online store, you should not be able to increase the price of any items in those orders after they have been purchased. It is your store, so you can clearly change prices as you wish. You just shouldn't be able to do it after someone agrees to buy an item at a certain price and gives you authorization to charge their credit card.

Environments that enforce and provide this attribute of security ensure that attackers, or mistakes by users, do not compromise the integrity of systems or data. When an attacker inserts malware or a back door into a system, the system's integrity is compromised. This can, in turn, harm the integrity of information held on the system by way of corruption, malicious modification, or the replacement of data with incorrect data. Strict access controls, intrusion detection, and hashing can combat these threats.

Authorized users can also affect a system or its data's integrity by mistake (although internal users may also commit malicious deeds). For example, a user with a full hard drive may unwittingly delete a configuration file under the mistaken assumption that deleting a file must be okay because the user doesn't remember ever using it. Or a user may insert incorrect values into a data-processing application that ends up charging a customer $3,000 instead of $300. Incorrectly modifying data kept in databases is another common way users may accidentally corrupt data—a mistake that can have lasting effects.

Security should streamline users' capabilities and give them only certain choices and functionality, so errors become less common and less devastating. System-critical files

should be restricted from viewing and access by users. Applications should provide mechanisms that check for valid and reasonable input values. Databases should let only authorized individuals modify data, and data in transit should be protected by encryption or other mechanisms.

Availability

Availability protection ensures reliable and timely access to data and resources to authorized individuals. Network devices, computers, and applications should provide adequate functionality to perform in a predictable manner with an acceptable level of performance. They should be able to recover from disruptions in a secure and quick fashion, so productivity is not negatively affected. Necessary protection mechanisms must be in place to protect against inside and outside threats that could affect the availability and productivity of all business-processing components.

Like many things in life, ensuring the availability of the necessary resources within an organization sounds easier to accomplish than it really is. Networks have many pieces that must stay up and running (routers, switches, proxies, firewalls, and so on). Software has many components that must be executing in a healthy manner (operating system, applications, antimalware software, and so forth). And an organization's operations can potentially be negatively affected by environmental aspects (such as fire, flood, HVAC issues, or electrical problems), natural disasters, and physical theft or attacks. An organization must fully understand its operational environment and its availability weaknesses so that it can put in place the proper countermeasures.

Authenticity

One of the curious features of the modern Internet is that sometimes we are unsure of who is putting out the things we read and download. Does that patch really come from Microsoft? Did your boss really send you that e-mail asking you to buy $10,000 worth of gift cards? *Authenticity* protections ensure we can trust that something comes from its claimed source. This concept is at the heart of authentication, which establishes that an entity trying to log into a system is really who it claims to be.

Authenticity in information systems is almost always provided through cryptographic means. As an example, when you connect to your bank's website, the connection should be encrypted using Transport Layer Security (TLS), which in turn uses your bank's digital certificate to authenticate to your browser that it truly is that bank on the other end and not an impostor. When you log in, the bank takes a cryptographic hash of the credentials you provide and compares them to the hash the bank has in your records to ensure it really is you on the other end.

Nonrepudiation

While authenticity establishes that an entity is who it claims to be at a particular point in time, it doesn't really provide historical proof of what that entity did or agreed to. For example, suppose Bob logs into his bank and then applies for a loan. He doesn't read the fine print until later, at which point he decides he doesn't like the terms of the transaction,

so he calls up the bank to say he never signed the contract and to please make it go away. Although the session was authenticated, Bob could claim that he walked away from his computer while logged into the bank's website, that his cat walked over the keyboard and stepped on ENTER, executing the transaction, and that Bob never intended to sign the loan application. It was the cat. Sadly, his claim could hold up in court.

Nonrepudiation, which is closely related to authenticity, means that someone cannot disavow being the source of a given action. For example, suppose Bob's bank had implemented a procedure for loan applications that required him to "sign" the application by entering his personal identification number (PIN). Now the whole cat defense falls apart unless Bob could prove he trained his cat to enter PINs.

Most commonly, nonrepudiation is provided through the use of digital signatures. Just like your physical signature on a piece of paper certifies that you either authored it or agree to whatever is written on it (e.g., a contract), the digital version attests to your sending an e-mail, writing software, or agreeing to a contract. We'll discuss digital signatures later in this book, but for now it will be helpful to remember that they are cryptographic products that, just like an old-fashioned physical signature, can be used for a variety of purposes.

EXAM TIP A good way to differentiate authenticity and nonrepudiation is that authenticity proves to *you* that you're talking to a given person at a given point in time. Nonrepudiation proves to *anyone* that a given person did or said something in the past.

Balanced Security

In reality, when information security is considered, it is commonly only through the lens of keeping secrets secret (confidentiality). The integrity and availability threats tend to be overlooked and only dealt with after they are properly compromised. Some assets have a critical confidentiality requirement (e.g., company trade secrets), some have critical integrity requirements (e.g., financial transaction values), and some have critical availability requirements (e.g., e-commerce web servers). Many people understand the concepts of the CIA triad, but may not fully appreciate the complexity of implementing the necessary controls to provide all the protection these concepts cover. The following provides a *short* list of some of these controls and how they map to the components of the CIA triad.

Availability:

- Redundant array of independent disks (RAID)
- Clustering
- Load balancing
- Redundant data and power lines
- Software and data backups

- Disk shadowing
- Co-location and offsite facilities
- Rollback functions
- Failover configurations

Integrity:

- Hashing (data integrity)
- Configuration management (system integrity)
- Change control (process integrity)
- Access control (physical and technical)
- Software digital signing
- Transmission cyclic redundancy check (CRC) functions

Confidentiality:

- Encryption for data at rest (whole disk, database encryption)
- Encryption for data in transit (IPSec, TLS, PPTP, SSH, described in Chapter 4)
- Access control (physical and technical)

All of these control types will be covered in this book. What is important to realize at this point is that while the concept of the CIA triad may seem simplistic, meeting its requirements is commonly more challenging.

Other Security Terms

The words "vulnerability," "threat," "risk," and "exposure" are often interchanged, even though they have different meanings. It is important to understand each word's definition and the relationships between the concepts they represent.

A *vulnerability* is a weakness in a system that allows a threat source to compromise its security. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

A *threat* is any potential danger that is associated with the exploitation of a vulnerability. If the threat is that someone will identify a specific vulnerability and use it against the organization or individual, then the entity that takes advantage of a vulnerability is referred to as a *threat agent* (or *threat actor*). A threat agent could be an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy, or an employee circumventing controls in order to copy files to a medium that could expose confidential information.

A *risk* is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact. If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method. If users are not educated on processes and procedures, there is a higher likelihood that an employee will make an unintentional mistake that may destroy data. If an intrusion detection system (IDS) is not implemented on a network, there is a higher likelihood an attack will go unnoticed until it is too late. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.

An *exposure* is an instance of being exposed to losses. A vulnerability exposes an organization to possible damages. If password management is lax and password rules are not enforced, the organization is exposed to the possibility of having users' passwords compromised and used in an unauthorized manner. If an organization does not have its wiring inspected and does not put proactive fire prevention steps into place, it exposes itself to potentially devastating fires.

A *control*, or *countermeasure*, is put into place to mitigate (reduce) the potential risk. A countermeasure may be a software configuration, a hardware device, or a procedure that eliminates a vulnerability or that reduces the likelihood a threat agent will be able to exploit a vulnerability. Examples of countermeasures include strong password management, firewalls, a security guard, access control mechanisms, encryption, and security awareness training.

NOTE The terms "control," "countermeasure," and "safeguard" are interchangeable terms. They are mechanisms put into place to reduce risk.

If an organization has antimalware software but does not keep the signatures up to date, this is a vulnerability. The organization is vulnerable to more recent malware attacks. The threat is that a threat agent will insert malware into the environment and disrupt productivity. The risk is the likelihood of a threat agent using malware in the environment and the resulting potential damage. If this happens, then a vulnerability has been exploited and the organization is exposed to loss. The countermeasures in this situation are to update the signatures and install the antimalware software on all computers. The relationships among risks, vulnerabilities, threats, and countermeasures are shown in Figure 1-1.

Applying the right countermeasure can eliminate the vulnerability and exposure, and thus reduce the risk. The organization cannot eliminate the threat agent, but it can protect itself and prevent this threat agent from exploiting vulnerabilities within the environment.

Many people gloss over these basic terms with the idea that they are not as important as the sexier things in information security. But you will find that unless a security team has an agreed-upon language in place, confusion will quickly take over. These terms embrace the core concepts of security, and if they are confused in any manner, then the activities that are rolled out to enforce security are commonly confused.