"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.

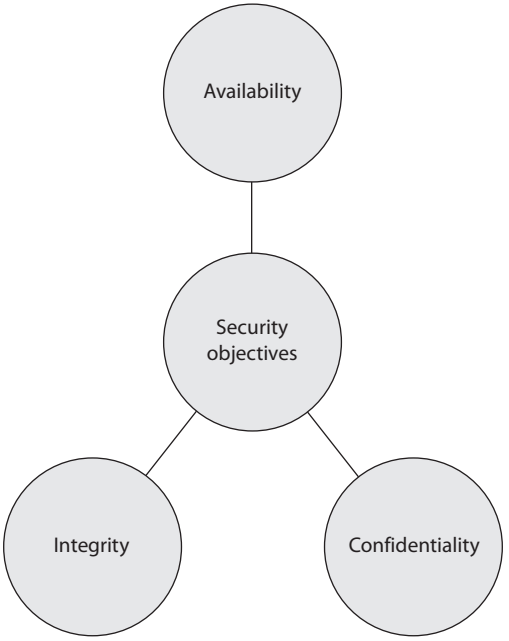
Organizations are increasingly faced with attackers who want to steal customer data to carry out identity theft and banking fraud. Company secrets are commonly being stolen by internal and external entities for economic espionage purposes. Systems are being hijacked and used within botnets to attack 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.

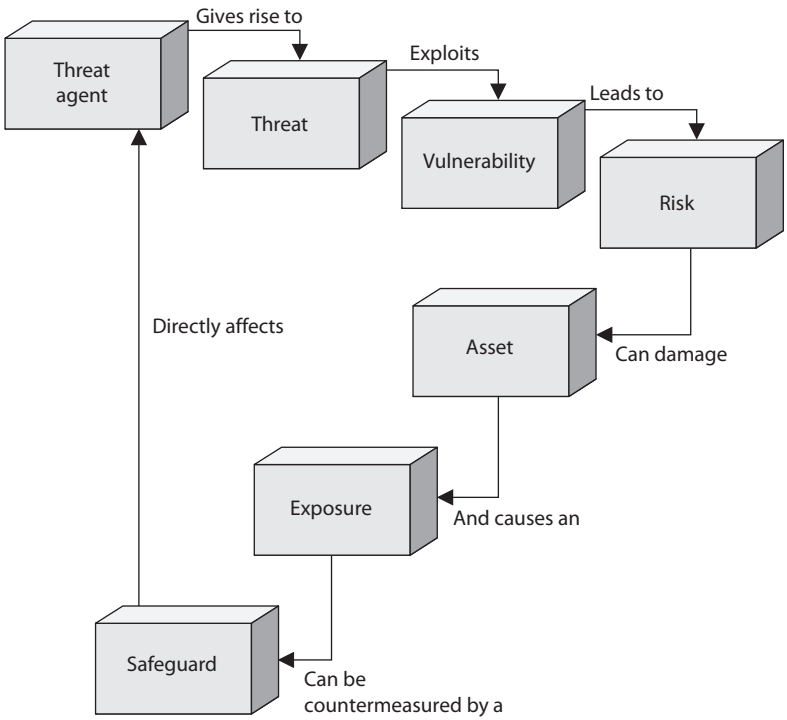


Figure 1-1 The relationships among the different security concepts

Security Governance Principles

Now that we have established a shared vocabulary for the fundamental cybersecurity concepts and understand how they relate to each other, let's turn our attention to how we can prioritize, assess, and continuously improve the security of our organizations. This is where security governance comes into play. *Security governance* is a framework that supports the security goals of an organization being set and expressed by senior management, communicated throughout the different levels of the organization, and consistently applied and assessed. Security governance grants power to the entities who need to implement and enforce security and provides a way to verify the performance of these necessary security activities. Senior management not only needs to set the direction of security but also needs a way to be able to view and understand how their directives are being met or not being met.

If a board of directors and CEO demand that security be integrated properly at all levels of the organization, how do they know it is really happening? Oversight mechanisms must be developed and integrated so that the people who are ultimately responsible for an organization are constantly and consistently updated on the overall health and security posture of the organization. This happens through properly defined communication channels, standardized reporting methods, and performance-based metrics.

Let's compare two companies. Company A has an effective security governance program in place and Company B does not. Now, to the untrained eye it would seem

as though Companies A and B are equal in their security practices because they both have security policies, procedures, and standards in place, the same security technology controls (firewalls, endpoint detection, identity management, and so on), defined security roles, and security awareness training. You may think, "These two companies are on the ball and quite evolved in their security programs." But if you look closer, you will see some critical differences (listed in Table 1-1).

Does the organization you work for look like Company A or Company B? Most organizations today have many of the pieces and parts to a security program (policies, standards, firewalls, security team, IDS, and so on), but management may not be

Company A	Company B
Board members understand that information security is critical to the company and demand to be updated quarterly on security performance and breaches.	Board members do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.
The chief executive officer (CEO), chief financial officer (CFO), chief information officer (CIO), chief information security officer (CISO), and business unit managers participate in a risk management committee that meets each month, and information security is always one topic on the agenda to review.	The CEO, CFO, and business unit managers feel as though information security is the responsibility of the CIO, CISO, and IT department and do not get involved.
Executive management sets an acceptable risk level that is the basis for the company's security policies and all security activities.	The CISO copied some boilerplate security policies, inserted his company's name, and had the CEO sign them.
Executive management holds business unit managers responsible for carrying out risk management activities for their specific business units.	All security activity takes place within the security department; thus, security works within a silo and is not integrated throughout the organization.
Critical business processes are documented along with the risks that are inherent at the different steps within the business processes.	Business processes are not documented and not analyzed for potential risks that can affect operations, productivity, and profitability.
Employees are held accountable for any security breaches they participate in, either maliciously or accidentally.	Policies and standards are developed, but no enforcement or accountability practices have been envisioned or deployed.
Security products, managed services, and consulting services are purchased and deployed in an informed manner. They are also constantly reviewed to ensure they are cost-effective.	Security products, managed services, and consulting services are purchased and deployed without any real research or performance metrics to determine the return on investment or effectiveness.
The organization is continuing to review its processes, including security, with the goal of continued improvement.	The organization does not analyze its performance for improvement, but continually marches forward and makes similar mistakes over and over again.

Table 1-1 Security Governance Program: A Comparison of Two Companies

truly involved, and security has not permeated throughout the organization. Some organizations rely just on technology and isolate all security responsibilities within the IT group. If security were just a technology issue, then this security team could properly install, configure, and maintain the products, and the company would get a gold star and pass the audit with flying colors. But that is not how information security works. It is much more than just technological solutions. Security must be driven throughout the organization, and having several points of responsibility and accountability is critical.

At this point, you may be asking, "So, what does security governance actually look like in the real world?" Security governance is typically implemented as a formal cybersecurity program or an information security management system (ISMS). Whichever of these names you call it, it is a collection of policies, procedures, baselines, and standards that an organization puts in place to make sure that its security efforts are aligned with business needs, streamlined, and effective, and that no security controls are missing. Figure 1-2 illustrates many of the elements that go into a complete security program.

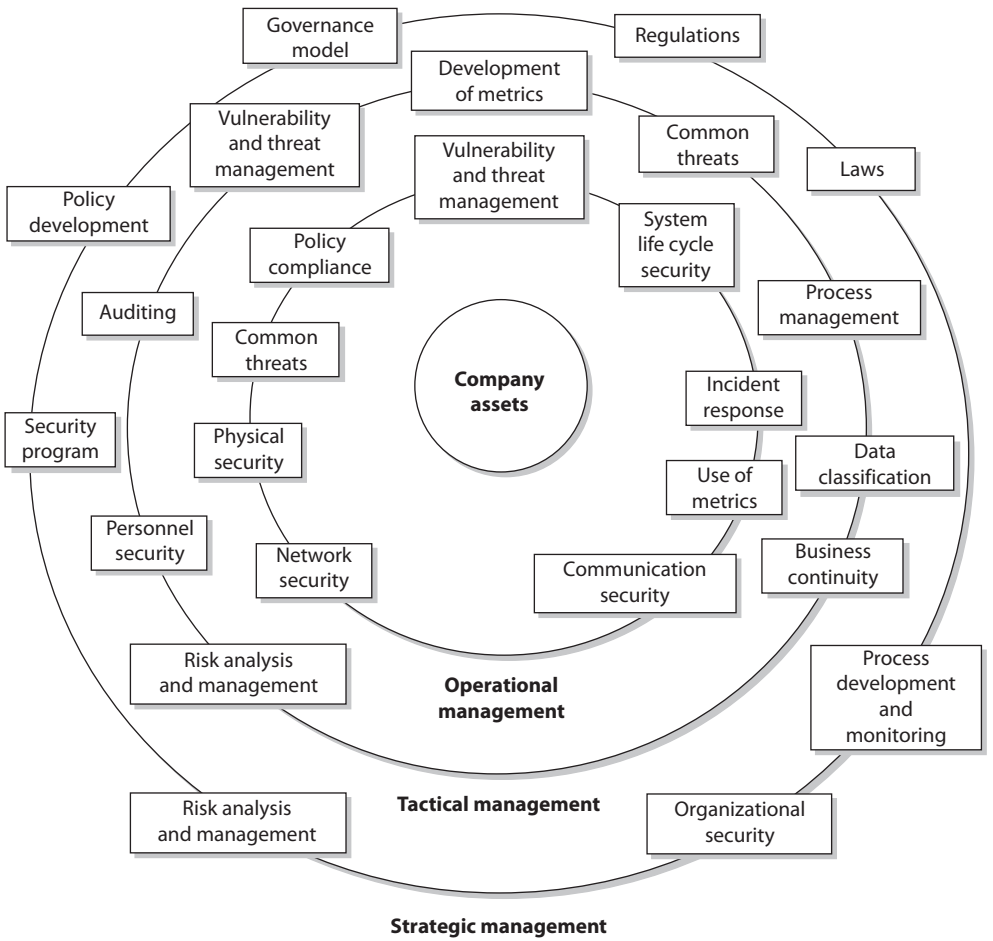


Figure 1-2 A complete security program contains many items.

Aligning Security to Business Strategy

An *enterprise security architecture* is a subset of an enterprise architecture (discussed in depth in Chapter 4) and implements an information security strategy. It consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally. It is a comprehensive and rigorous method for describing the structure and behavior of all the components that make up a holistic ISMS. The main reason to develop an enterprise security architecture is to ensure that security efforts align with business practices in a standardized and cost-effective manner. The architecture works at an abstraction level and provides a frame of reference. Besides security, this type of architecture allows organizations to better achieve interoperability, integration, ease of use, standardization, and governance.

How do you know if an organization does not have an enterprise security architecture in place? If the answer is "yes" to most of the following questions, this type of architecture is not in place:

- Does security take place in silos throughout the organization?
- Is there a continual disconnect between senior management and the security staff?
- Are redundant products purchased for different departments for overlapping security needs?
- Is the security program made up of mainly policies without actual implementation and enforcement?
- When a user's access requirements increase because of business needs, does the network administrator just modify the access controls without the user manager's documented approval?
- When a new product is being rolled out, do unexpected interoperability issues pop up that require more time and money to fix?
- Do many "one-off" efforts take place instead of following standardized procedures when security issues arise?
- Are the business unit managers unaware of their security responsibilities and how their responsibilities map to legal and regulatory requirements?
- Is "sensitive data" defined in a policy, but the necessary controls are not fully implemented and monitored?
- Are stovepipe (point) solutions implemented instead of enterprise-wide solutions?
- Are the same expensive mistakes continuing to take place?
- Is security governance currently unavailable because the enterprise is not viewed or monitored in a standardized and holistic manner?
- Are business decisions being made without taking security into account?
- Are security personnel usually putting out fires with no real time to look at and develop strategic approaches?
- Are some business units engaged in security efforts that other business units know nothing about?

If many of these answers are "yes," no useful architecture is in place. Now, the following is something very interesting the authors have seen over several years. Most organizations have multiple problems in the preceding list and yet they focus on each item as if it is unconnected to the other problems. What the CSO, CISO, and/or security administrator does not always understand is that these are just *symptoms* of a treatable disease. The "treatment" is to put one person in charge of a team that develops a phased-approach enterprise security architecture rollout plan. The goals are to integrate technology-oriented and business-centric security processes; link administrative, technical, and physical controls to properly manage risk; and integrate these processes into the IT infrastructure, business processes, and the organization's culture.

A helpful tool for aligning an organization's security architecture with its business strategy is the *Sherwood Applied Business Security Architecture (SABSA)*, which is shown in Table 1-2. It is a layered framework, with its first layer describing the business context within which the security architecture must exist. Each layer of the framework decreases in abstraction and increases in detail, so it builds upon the others and moves from policy to practical implementation of technology and solutions. The idea is to provide a chain of traceability through the contextual, conceptual, logical, physical, component, and operational levels.

	Assets (What)	**Motivation (Why)**	**Process (How)**	**People (Who)**	**Location (Where)**	**Time (When)**
Contextual	The business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetimes and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices, and procedures	Security mechanisms	Users, applications, and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions, and ACLs	Processes, nodes, addresses, and protocols	Security step timing and sequencing
Operational	Assurance of operation continuity	Operation risk management	Security service management and support	Application and user management and support	Security of sites, networks, and platforms	Security operations schedule

Table 1-2 SABSA Architecture Framework

The following outlines the questions that are to be asked and answered at each level of the framework:

- ***What* are you trying to do at this layer?** The assets to be protected by your security architecture.
- ***Why* are you doing it?** The motivation for wanting to apply security, expressed in the terms of this layer.
- ***How* are you trying to do it?** The functions needed to achieve security at this layer.
- ***Who* is involved?** The people and organizational aspects of security at this layer.
- ***Where* are you doing it?** The locations where you apply your security, relevant to this layer.
- ***When* are you doing it?** The time-related aspects of security relevant to this layer.

SABSA is a framework and methodology for enterprise security architecture and service management. Since it is a *framework*, this means it provides a structure for individual architectures to be built from. Since it is a *methodology* also, this means it provides the processes to follow to build and maintain this architecture. SABSA provides a life-cycle model so that the architecture can be constantly monitored and improved upon over time.

EXAM TIP You do not need to memorize the SABSA framework, but you do need to understand how security programs align with business strategies.

For an enterprise security architecture to be successful in its development and implementation, the following items must be understood and followed: strategic alignment, business enablement, process enhancement, and security effectiveness. We'll cover the first three of these in the following sections but will cover security effectiveness in Chapter 18 when we discuss security assessments.

Strategic Alignment

Strategic alignment means the business drivers and the regulatory and legal requirements are being met by the enterprise security architecture. Security efforts must provide and support an environment that allows an organization to not only survive, but thrive. The security industry has grown up from the technical and engineering world, not the business world. In many organizations, while the IT security personnel and business personnel might be located physically close to each other, they are commonly worlds apart in how they see the same organization they work in. Technology is only a tool that supports a business; it is not the business itself. The IT environment is analogous to the circulatory system within a human body; it is there to support the body—the body does not exist to support the circulatory system. And security is analogous to the immune system of the body—it is there to protect the overall environment. If these critical systems (business, IT, security)

do not work together in a concerted effort, there will be deficiencies and imbalances. While deficiencies and imbalances lead to disease in the body, deficiencies and imbalances within an organization can lead to risk and security compromises.

Business Enablement

When looking at the *business enablement* requirement of the enterprise security architecture, we need to remind ourselves that each organization exists for one or more specific business purposes. Publicly traded companies are in the business of increasing shareholder value. Nonprofit organizations are in the business of furthering a specific set of causes. Government organizations are in the business of providing services to their citizens. Companies and organizations do not exist for the sole purpose of being secure. Security cannot stand in the way of business processes, but should be implemented to better enable them.

Business enablement means the core business processes are integrated into the security operating model—they are standards based and follow a risk tolerance criteria. What does this mean in the real world? Let's say a company's accountants have figured out that if they allow the customer service and support staff to work from home, the company would save a lot of money on office rent, utilities, and overhead—plus, the company's insurance would be cheaper. The company could move into this new model with the use of virtual private networks (VPNs), firewalls, content filtering, and so on. Security enables the company to move to this different working model by providing the necessary protection mechanisms. If a financial institution wants to enable its customers to view bank account information and carry out money transfers online, it can offer this service if the correct security mechanisms are put in place (access control, authentication, secure connections, etc.). Security should help the organization thrive by providing the mechanisms to do new things safely.

Process Enhancement

Process enhancement can be quite beneficial to an organization if it takes advantage of this capability when it is presented to it. An organization that is serious about securing its environment will have to take a close look at many of the business processes that take place on an ongoing basis. Many times, these processes are viewed through the eyeglasses of security, because that's the reason for the activity, but this is a perfect chance to enhance and improve upon the same processes to increase productivity. When you look at many business processes taking place in all types of organizations, you commonly find a duplication of efforts, manual steps that can be easily automated, or ways to streamline and reduce time and effort that are involved in certain tasks. This is commonly referred to as *process reengineering*.

When an organization is developing its security enterprise components, those components must be integrated into the business processes to be effective. This can allow for process management to be refined and calibrated. This, in turn, allows for security to be integrated in system life cycles and day-to-day operations. So, while business enablement means "we can do new stuff," process enhancement means "we can do stuff better."

Organizational Processes

The processes we just covered are regular day-to-day ones. There are other processes that happen less frequently but may have a much more significant impact on the security posture of the organization. Let's dig a bit deeper into some of these key organizational processes and how our security efforts align with, enable, and enhance them.

Mergers and Acquisitions

As companies grow, they often acquire new capabilities (e.g., markets, products, and intellectual property) by merging with another company or outright acquiring it. *Mergers and acquisitions (M&A)* always take place for business reasons, but they almost always have significant cybersecurity implications. Think of it this way: your company didn't acquire only the business assets of that other company it just purchased; it also acquired its security program and all the baggage that may come with it. Suppose that during the M&A process you discover that the company that your company is acquiring has a significant but previously unknown data breach. This is exactly what happened in 2017 when Verizon acquired Yahoo! and discovered that the latter had experienced two massive security breaches. The acquisition went forward, but at a price that was $350 million lower than originally agreed.

One of the ways in which companies protect themselves during a merger or acquisition is by conducting extensive audits of the company they are about to merge with or acquire. There are many service providers who now offer *compromise assessments*, which are in-depth technical examinations of a company's information systems to determine whether an undocumented compromise is ongoing or has happened in the past. It's sort of like exploratory surgery; let's open up the patient and see what we find. Another approach is to conduct an audit of the ISMS, which is more focused on policies, procedures, and controls.

Divestitures

A *divestiture*, on the other hand, is when your company sells off (or otherwise gets rid of) a part of itself. There are many reasons why a company may want to divest itself of a business asset, such as having a business unit that is not profitable or no longer well aligned with the overarching strategy. If the divestiture involves a sale or transfer of an asset to another company, that company is going to audit that asset. In other words, for us cybersecurity professionals, a divestiture is when we have to answer tough questions from the buyer, and an M&A is when we are the ones asking the tough questions of someone else. They are two sides to the same coin.

If your company is divesting assets for whose security you are responsible, you will probably work closely with the business and legal teams to identify any problem areas that might reduce the value of the assets being sold. For example, if there are any significant vulnerabilities in those assets, you may want to apply controls to mitigate the related risks. If you discover a compromise, you want to eradicate it and recover from it aggressively.

A less obvious cybersecurity implication of divestiture is the need to segment the part or parts of the ISMS that involve the asset(s) in question. If your company is selling a

business unit, it undoubtedly has security policies, procedures, and controls that apply to it but may also apply to other business areas. Whoever is acquiring the assets will want to know what those are, and maybe even test them at a technical level. You need to be prepared to be audited without revealing any proprietary or confidential information in the process. Be sure to keep your legal team close to ensure you are responsive to what is required of you, but nothing else.

Governance Committees

The organizational processes we've described so far (M&A and divestitures) are triggered by a business decision to either acquire or get rid of some set of assets. There is another key process that is ongoing in many organizations with mature cybersecurity practices. A *governance committee* is a standing body whose purpose is to review the structures and practices of the organization and report its findings to the board of directors. While it may sound a bit scary to have such a committee watching over everything you do, they can actually be your allies by shining a light on the tough issues that you cannot solve by yourself without help from the board. It is important for you to know who is who in your organization and who can help get what you need to ensure a secure environment.

Organizational Roles and Responsibilities

Senior management and other levels of management understand the vision of the organization, the business goals, and the objectives. The next layer down is the functional management, whose members understand how their individual departments work, what roles individuals play within the organization, and how security affects their department directly. The next layers are operational managers and staff. These layers are closer to the actual operations of the organization. They know detailed information about the technical and procedural requirements, the systems, and how the systems are used. The employees at these layers understand how security mechanisms integrate into systems, how to configure them, and how they affect daily productivity. Every layer offers different insight into what type of role security plays within an organization, and each should have input into the best security practices, procedures, and chosen controls to ensure the agreed-upon security level provides the necessary amount of protection without negatively affecting the company's productivity.

EXAM TIP Senior management always carries the ultimate responsibility for the organization.

Although each layer is important to the overall security of an organization, some specific roles must be clearly defined. Individuals who work in smaller environments (where everyone must wear several hats) may get overwhelmed with the number of roles presented next. Many commercial businesses do not have this level of structure in their security teams, but many large companies, government agencies, and military units do. What you need to understand are the responsibilities that must be assigned and whether

they are assigned to just a few people or to a large security team. These roles include the executive management, security officer, data owner, data custodian, system owner, security administrator, supervisor (user manager), change control analyst, data analyst, user, auditor, and the guy who gets everyone coffee.

Executive Management

The individuals designated as executive management typically are those whose titles start with "chief," and collectively they are often referred to as the "C-suite." Executive leaders are ultimately responsible for everything that happens in their organizations, and as such are considered the ultimate business and function owners. This has been evidenced time and again (as we will see shortly) in high-profile cases wherein executives have been fired, sued, or even prosecuted for organizational failures or fraud that occurred under their leadership. Let's start at the top of a corporate entity, the CEO.

Chief Executive Officer The *chief executive officer (CEO)* has the day-to-day management responsibilities of an organization. This person is often the chairperson of the board of directors and is the highest-ranking officer in the company. This role is for the person who oversees the company's finances, strategic planning, and operations from a high level. The CEO is usually seen as the visionary for the company and is responsible for developing and modifying the company's business plan. The CEO sets budgets; forms partnerships; and decides on what markets to enter, what product lines to develop, how the company will differentiate itself, and so on. This role's overall responsibility is to ensure that the company grows and thrives.

NOTE The CEO can delegate tasks, but not necessarily responsibility. More and more regulations dealing with information security are holding the CEO accountable for ensuring the organization practices due care and due diligence with respect to information security, which is why security departments across the land are receiving more funding. Personal liability for the decision makers and purse-string holders has loosened those purse strings, and companies are now able to spend more money on security than before. (Due care and due diligence are described in detail in Chapter 3.)

Chief Financial Officer The *chief financial officer (CFO)* is responsible for the corporation's accounting and financial activities and the overall financial structure of the organization. This person is responsible for determining what the company's financial needs will be and how to finance those needs. The CFO must create and maintain the company's capital structure, which is the proper mix of equity, credit, cash, and debt financing. This person oversees forecasting and budgeting and the processes of submitting financial statements to the regulators and stakeholders.

Chief Information Officer The *chief information officer (CIO)* may report to either the CEO or CFO, depending upon the corporate structure, and is responsible for the strategic use and management of information systems and technology within the organization. Over time, this position has become more strategic and less operational in

Executives and Incarcerations and Fines, Oh My!

The CFO and CEO are responsible for informing stakeholders (creditors, analysts, employees, management, investors) of the firm's financial condition and health. After the corporate debacles at Enron and WorldCom uncovered in 2001–2002, the U.S. government enacted the Sarbanes-Oxley Act (SOX), which prescribes to the CEO and CFO financial reporting responsibilities and includes penalties and potential *personal* liability for failure to comply. SOX gave the Securities Exchange Commission (SEC) more authority to create regulations that ensure these officers cannot simply pass along fines to the corporation for personal financial misconduct. Under SOX, they can personally be fined millions of dollars and/or go to jail. The following list provides a sampling of some of the cases in the past decade in which C-suite executives have been held accountable for cybersecurity issues under various laws:

- **August 2020** Joseph Sullivan, former chief information security officer at Uber, was charged with obstruction of justice and misprision of a felony in connection with the attempted cover-up of the 2016 hack of Uber.
- **July 2019** Facebook agreed to pay $100M in fines for making misleading disclosures concerning the risks to user data after becoming aware that Cambridge Analytica had improperly collected and misused PII on nearly 30M Facebook users in 2014 and 2015. The company neither admitted nor denied the SEC allegations as part of this agreement.
- **March 2019** Jun Ying, a former chief information officer for Equifax, pled guilty and was subsequently convicted to four months in prison on charges of insider trading for allegedly selling his stock in the company after discovering a massive data breach. He suspected (correctly) that the stock would lose value once the breach became known.
- **March 2018** Martin Shkreli, a notorious pharmaceutical executive, was sentenced to seven years in prison after being convicted of securities fraud stemming from his alleged use of funds from new companies to pay down debts previously incurred by financially troubled companies.
- **December 2017** KIT Digital's former CEO Kaleil Isaza Tuzman was found guilty of market manipulation and fraud charges. His former CFO, Robin Smyth, had previously pled guilty and turned government witness against Tuzman. As of this writing, Tuzman is still awaiting sentencing.
- **June 2015** Joe White, the former CFO of Shelby Regional Medical Center, was sentenced to 23 months in federal prison after making false claims to receive payments under the Medicare Electronic Health Record Incentive Program.

These are only some of the big cases that made it into the headlines. Other executives have also received punishments for "creative accounting" and fraudulent activities.

many organizations. CIOs oversee and are responsible for the day-in, day-out technology operations of a company, but because organizations are so dependent upon technology, CIOs are being asked to sit at the corporate table more and more.

CIO responsibilities have extended to working with the CEO (and other management) on business-process management, revenue generation, and how business strategy can be accomplished with the company's underlying technology. This person usually should have one foot in techno-land and one foot in business-land to be effective because she is bridging two very different worlds.

The CIO sets the stage for the protection of company assets and is ultimately responsible for the success of the company's security program. Direction should be coming down from the CEO, and there should be clear lines of communication between the board of directors, the C-level staff, and mid-management.

Chief Privacy Officer The *chief privacy officer (CPO)* is a newer position, created mainly because of the increasing demands on organizations to protect a long laundry list of different types of data. This role is responsible for ensuring that customer, company, and employee data is kept safe, which keeps the company out of criminal and civil courts and hopefully out of the headlines. This person is often an attorney with privacy law experience and is directly involved with setting policies on how data is collected, protected, and given out to third parties. The CPO often reports to the chief security officer.

It is important that the CPO understand the privacy, legal, and regulatory requirements the organization must comply with. With this knowledge, the CPO can then develop the organization's policies, standards, procedures, controls, and contract agreements to ensure that privacy requirements are being properly met. Remember also that organizations are responsible for knowing how their suppliers, partners, and other third parties are protecting this sensitive information. The CPO may be responsible for reviewing the data security and privacy practices of these other parties.

Some companies have carried out risk assessments without considering the penalties and ramifications they would be forced to deal with if they do not properly protect the information they are responsible for. Without considering these liabilities, risk cannot be properly assessed.

Privacy

Privacy is different from security. *Privacy* indicates the amount of control an individual should be able to have and expect to have as it relates to the release of their own sensitive information. *Security* refers to the mechanisms that can be put into place to provide this level of control.

It is becoming more critical (and more difficult) to protect personally identifiable information (PII) because of the increase of identity theft and financial fraud threats. PII is a combination of identification elements (name, address, phone number, account number, etc.). Organizations must have privacy policies and controls in place to protect their employee and customer PII. Chapter 3 discusses PII in depth.

CSO vs. CISO

The CSO and CISO may have similar or very different responsibilities, depending on the individual organization. In fact, an organization may choose to have both, either, or neither of these roles. It is up to an organization that has either or both of these roles to define their responsibilities. By and large, the CSO role usually has a further-reaching list of responsibilities compared to the CISO role. The CISO is usually focused more on technology and has an IT background. The CSO usually is required to understand a wider range of business risks, including physical security, not just technological risks.

The CSO is usually more of a businessperson and typically is present in larger organizations. If a company has both roles, the CISO reports directly to the CSO.

The CSO is commonly responsible for ensuring *convergence*, which is the formal cooperation between previously disjointed security functions. This mainly pertains to physical and IT security working in a more concerted manner instead of working in silos within the organization. Issues such as loss prevention, fraud prevention, business continuity planning, legal/regulatory compliance, and insurance all have physical security and IT security aspects and requirements. So one individual (CSO) overseeing and intertwining these different security disciplines allows for a more holistic and comprehensive security program.

The organization should document how privacy data is collected, used, disclosed, archived, and destroyed. Employees should be held accountable for not following the organization's standards on how to handle this type of information.

Chief Security Officer The *chief security officer (CSO)* is responsible for understanding the risks that the company faces and for mitigating these risks to an acceptable level. This role is responsible for understanding the organization's business drivers and for creating and maintaining a security program that facilitates these drivers, along with providing security, compliance with a long list of regulations and laws, and any customer expectations or contractual obligations.

The creation of this role is a mark in the "win" column for the security industry because it means security is finally being seen as a business issue. Previously, security was relegated to the IT department and was viewed solely as a technology issue. As organizations began to recognize the need to integrate security requirements and business needs, creating a position for security in the executive management team became more of a necessity. The CSO's job is to ensure that business is not disrupted in any way due to security issues. This extends beyond IT and reaches into business processes, legal issues, operational issues, revenue generation, and reputation protection.

Data Owner

The *data owner* (information owner) is usually a member of management who is in charge of a specific business unit and who is ultimately responsible for the protection

and use of a specific subset of information. The data owner has due-care responsibilities and thus will be held responsible for any negligent act that results in the corruption or disclosure of the data. The data owner decides upon the classification of the data she is responsible for and alters that classification if the business need arises. This person is also responsible for ensuring that the necessary security controls are in place, defining security requirements per classification and backup requirements, approving any disclosure activities, ensuring that proper access rights are being used, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And the data owner will deal with security violations pertaining to the data she is responsible for protecting. The data owner, who obviously has enough on her plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian.

NOTE Data ownership takes on a different meaning when outsourcing data storage requirements. You may want to ensure that the service contract includes a clause to the effect that all data is and shall remain the sole and exclusive property of your organization.

Data Custodian

The *data custodian* (information custodian) is responsible for maintaining and protecting the data. This role is usually filled by the IT or security department, and the duties include implementing and maintaining security controls; performing regular backups of the data; periodically validating the integrity of the data; restoring data from backup media; retaining records of activity; and fulfilling the requirements specified in the company's security policy, standards, and guidelines that pertain to information security and data protection.

System Owner

The *system owner* is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role must ensure that the systems are

Data Owner Issues

Each business unit should have a data owner who protects the unit's most critical information. The company's policies must give the data owners the necessary authority to carry out their tasks.

This is not a technical role, but rather a business role that must understand the relationship between the unit's success and the protection of this critical asset. Not all businesspeople understand this role, so they should be given the necessary training.

properly assessed for vulnerabilities and must report any that are discovered to the incident response team and data owner.

Security Administrator

The *security administrator* is responsible for implementing and maintaining specific security network devices and software in the enterprise. These controls commonly include firewalls, an intrusion detection system (IDS), intrusion prevention system (IPS), antimalware, security proxies, data loss prevention, etc. It is common for a delineation to exist between the security administrator's responsibilities and the network administrator's responsibilities. The security administrator has the main focus of keeping the network secure, and the network administrator has the focus of keeping things up and running.

A security administrator's tasks commonly also include creating new system user accounts, implementing new security software, testing security patches and components, and issuing new passwords. The security administrator must make sure access rights given to users support the policies and data owner directives.

Supervisor

The *supervisor* role, also called *user manager*, is ultimately responsible for all user activity and any assets created and owned by these users. For example, suppose Kathy is the supervisor of ten employees. Her responsibilities would include ensuring that these employees understand their responsibilities with respect to security; making sure the employees' account information is up to date; and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

Change Control Analyst

Since the only thing that is constant is change, someone must make sure changes happen securely. The *change control analyst* is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that the change will not introduce any vulnerabilities, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity.

Data Analyst

Having proper data structures, definitions, and organization is very important to a company. The *data analyst* is responsible for ensuring that data is stored in a way that makes the most sense to the company and the individuals who need to access and work with it. For example, payroll information should not be mixed with inventory information; the purchasing department needs to have a lot of its values in monetary terms; and the inventory system must follow a standardized naming scheme. The data analyst may be responsible for architecting a new system that will hold company information or advising in the purchase of a product that will do so. The data analyst works with the data owners to help ensure that the structures set up coincide with and support the company's business objectives.

User

The *user* is any individual who routinely uses the data for work-related tasks. The user must have the necessary level of access to the data to perform the duties within their position and is responsible for following operational security procedures to ensure the data's confidentiality, integrity, and availability to others.

Auditor

The function of the *auditor* is to periodically check that everyone is doing what they are supposed to be doing and to ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations. Organizations can have internal auditors and/or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met.

While many security professionals fear and dread auditors, they can be valuable tools in ensuring the overall security of the organization. Their goal is to find the things you have missed and help you understand how to fix the problems.

Why So Many Roles?

Most organizations will not have all the roles previously listed, but what is important is to build an organizational structure that contains the necessary roles and map the correct security responsibilities to them. This structure includes clear definitions of responsibilities, lines of authority and communication, and enforcement capabilities. A clear-cut structure takes the mystery out of who does what and how things are handled in different situations.

Security Policies, Standards, Procedures, and Guidelines

Computers and the information processed on them usually have a direct relationship with a company's critical missions and objectives. Because of this level of importance, senior management should make protecting these items a high priority and provide the necessary support, funds, time, and resources to ensure that systems, networks, and information are protected in the most logical and cost-effective manner possible. A comprehensive management approach must be developed to accomplish these goals successfully. This is because everyone within an organization may have a different set of personal values and experiences they bring to the environment with regard to security. It is important to make sure everyone is consistent regarding security at a level that meets the needs of the organization.

For a company's security plan to be successful, it must start at the top level and be useful and functional at every single level within the organization. Senior management needs to define the scope of security and identify and decide what must be protected and to what extent. Management must understand the business needs and compliance requirements (regulations, laws, and liability issues) for which it is responsible regarding security and ensure that the company as a whole fulfills its obligations. Senior management also must determine what is expected from employees and what the consequences of

noncompliance will be. These decisions should be made by the individuals who will be held ultimately responsible if something goes wrong. But it is a common practice to bring in the expertise of the security officers to collaborate in ensuring that sufficient policies and controls are being implemented to achieve the goals being set and determined by senior management.

A security program contains all the pieces necessary to provide overall protection to an organization and lays out a long-term security strategy. A security program's documentation should be made up of security policies, procedures, standards, guidelines, and baselines. The human resources and legal departments must be involved in the development and enforcement of rules and requirements laid out in these documents.

ISMS vs. Enterprise Security Architecture

What is the difference between an ISMS and an enterprise security architecture? An ISMS outlines the controls that need to be put into place (risk management, vulnerability management, business continuity planning, data protection, auditing, configuration management, physical security, etc.) and provides direction on how those controls should be managed throughout their life cycle. The ISMS specifies the pieces and parts that need to be put into place to provide a holistic security program for the organization overall and how to properly take care of those pieces and parts. The enterprise security architecture illustrates how these components are to be integrated into the different layers of the current business environment. The security components of the ISMS have to be interwoven throughout the business environment and not siloed within individual company departments.

For example, the ISMS will dictate that risk management needs to be put in place, and the enterprise security architecture will chop up the risk management components and illustrate how risk management needs to take place at the strategic, tactical, and operational levels. As another example, the ISMS could dictate that data protection needs to be put into place. The security architecture can show how this happens at the infrastructure, application, component, and business level. At the infrastructure level we can implement data loss protection technology to detect how sensitive data is traversing the network. Applications that maintain sensitive data must have the necessary access controls and cryptographic functionality. The components within the applications can implement the specific cryptographic functions. And protecting sensitive company information can be tied to business drivers, which is illustrated at the business level of the architecture.

The ISO/IEC 27000 series (which outlines the ISMS and is covered in detail in Chapter 4) is very policy oriented and outlines the necessary components of a security program. This means that the ISO standards are general in nature, which is not a defect—they were created that way so that they could be applied to various types of businesses, companies, and organizations. But since these standards are general, it can be difficult to know how to implement them and map them to your company's infrastructure and business needs. This is where the enterprise security architecture comes into play. The architecture is a tool used to ensure that what is outlined in the security standards is implemented throughout the different layers of an organization.

The language, level of detail, formality of the documents, and supporting mechanisms should be examined by the policy developers. Security policies, standards, guidelines, procedures, and baselines must be developed with a realistic view to be most effective. Highly structured organizations usually follow documentation in a more uniform way. Less structured organizations may need more explanation and emphasis to promote compliance. The more detailed the rules are, the easier it is to know when one has been violated. However, overly detailed documentation and rules can prove to be more burdensome than helpful. The business type, its culture, and its goals must be evaluated to make sure the proper language is used when writing security documentation.

There are a lot of legal liability issues surrounding security documentation. If your organization has a policy outlining how it is supposed to be protecting sensitive information and it is found out that your organization is not practicing what it is preaching, criminal charges and civil suits could be filed and successfully executed. It is important that an organization's security does not just look good on paper, but in action also.

Security Policy

A *security policy* is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization. A security policy can be an organizational policy, an issue-specific policy, or a system-specific policy. In an *organizational security policy*, management establishes how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out. This policy must address applicable laws, regulations, and liability issues and how they are to be satisfied. The organizational security policy provides scope and direction for all future security activities within the organization. It also describes the amount of risk senior management is willing to accept.

The organizational security policy has several important characteristics that must be understood and implemented:

- Business objectives should drive the policy's creation, implementation, and enforcement. The policy should not dictate business objectives.
- It should be an easily understood document that is used as a reference point for all employees and management.
- It should be developed and used to integrate security into all business functions and processes.
- It should be derived from and support all legislation and regulations applicable to the company.
- It should be reviewed and modified as a company changes, such as through adoption of a new business model, a merger with another company, or change of ownership.
- Each iteration of the policy should be dated and under version control.
- The units and individuals who are governed by the policy must have easy access to it. Policies are commonly posted on portals on an intranet.

- It should be created with the intention of having the policies in place for several years at a time. This will help ensure policies are forward-thinking enough to deal with potential changes that may arise.
- The level of professionalism in the presentation of the policies reinforces their importance, as well as the need to adhere to them.
- It should not contain language that isn't readily understood by everyone. Use clear and declarative statements that are easy to understand and adopt.
- It should be reviewed on a regular basis and adapted to correct incidents that have occurred since the last review and revision of the policies.

A process for dealing with those who choose not to comply with the security policies must be developed and enforced so there is a structured method of response to noncompliance. This establishes a process that others can understand and thus recognize not only what is expected of them but also what they can expect as a response to their noncompliance.

Organizational security policies are also referred to as master security policies. An organization will have many policies, and they should be set up in a hierarchical manner. The organizational (master) security policy is at the highest level, with policies underneath it that address security issues specifically. These are referred to as issue-specific policies.

An *issue-specific policy*, also called a *functional policy*, addresses specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply with these security issues. For example, an organization may choose to have an e-mail security policy that outlines what management can and cannot do with employees' e-mail messages for monitoring purposes, that specifies which e-mail functionality employees can or cannot use, and that addresses specific privacy issues.

As a more specific example, an e-mail policy might state that management can read any employee's e-mail messages that reside on the mail server, but not when they reside on the user's workstation. The e-mail policy might also state that employees cannot use e-mail to share confidential information or pass inappropriate material and that they may be subject to monitoring of these actions. Before they use their e-mail clients, employees should be asked to confirm that they have read and understand the e-mail policy, either by signing a confirmation document or clicking Yes in a confirmation dialog box. The policy provides direction and structure for the staff by indicating what they can and cannot do. It informs the users of the expectations of their actions, and it provides liability protection in case an employee cries "foul" for any reason dealing with e-mail use.

EXAM TIP A policy needs to be technology and solution independent. It must outline the goals and missions, but not tie the organization to specific ways of accomplishing them.

A common hierarchy of security policies is outlined here, which illustrates the relationship between the master policy and the issue-specific policies that support it:

Organizational policy:

- Acceptable use policy
- Risk management policy
- Vulnerability management policy
- Data protection policy
- Access control policy
- Business continuity policy
- Log aggregation and auditing policy
- Personnel security policy
- Physical security policy
- Secure application development policy
- Change control policy
- E-mail policy
- Incident response policy

A *system-specific policy* presents the management's decisions that are specific to the actual computers, networks, and applications. An organization may have a system-specific policy outlining how a database containing sensitive information should be protected, who can have access, and how auditing should take place. It may also have a system-specific policy outlining how laptops should be locked down and managed. This policy type is directed to one or a group of similar systems and outlines how they should be protected.

Policies are written in broad terms to cover many subjects in a general fashion. Much more granularity is needed to actually support the policy, and this happens with the use of procedures, standards, guidelines, and baselines. The policy provides the foundation. The procedures, standards, guidelines, and baselines provide the security framework. And the necessary security controls (administrative, technical, and physical) are used to fill in the framework to provide a full security program.

Standards

Standards refer to mandatory activities, actions, or rules. Standards describe specific requirements that allow us to meet our policy goals. They are unambiguous, detailed, and measurable. There should be no question as to whether a specific asset or action complies with a given standard.

Organizational security standards may specify how hardware and software products are to be used. They can also be used to indicate expected user behavior. They provide a

Types of Policies

Policies generally fall into one of the following categories:

- **Regulatory** This type of policy ensures that the organization is following standards set by specific industry regulations (HIPAA, GLBA, SOX, PCI DSS, etc.; see Chapter 3). It is very detailed and specific to a type of industry. It is used in financial institutions, healthcare facilities, public utilities, and other government-regulated industries.
- **Advisory** This type of policy strongly advises employees as to which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical or financial information.
- **Informative** This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one that teaches individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations.

means to ensure that specific technologies, applications, parameters, and procedures are implemented in a uniform (standardized) manner across the organization. Organizational standards may require that all employees use a specific smart card as their access control token, that its certificate expire after 12 months, and that it be locked after three unsuccessful attempts to enter a personal identification number (PIN). These rules are compulsory within a company, and if they are going to be effective, they must be enforced.

An organization may have an issue-specific data classification policy that states "All confidential data must be properly protected." It would need a supporting data protection standard outlining how this protection should be implemented and followed, as in "Confidential information must be protected with AES256 at rest and in transit."

Tactical and strategic goals are different. A strategic goal can be viewed as the ultimate endpoint, while tactical goals are the steps necessary to achieve it. As shown in Figure 1-3, standards, guidelines, and procedures are the tactical tools used to achieve and support the directives in the security policy, which is considered the strategic goal.

EXAM TIP The term *standard* has more than one meaning in our industry. Internal documentation that lays out rules that must be followed is a standard. But sometimes, best practices, as in the ISO/IEC 27000 series, are referred to as standards because they were developed by a standards body. And as we will see later, we have specific technologic standards, as in IEEE 802.11. You need to understand the context of how this term is used. The CISSP exam will not try and trick you on this word; just know that the industry uses it in several different ways.

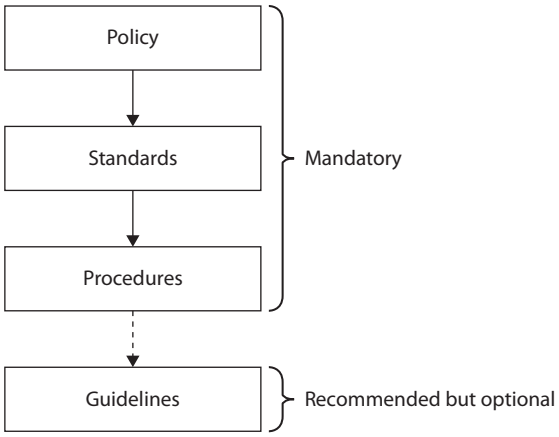


Figure 1-3 Policies are implemented through standards, procedures, and guidelines.

Baselines

The term *baseline* refers to a point in time that is used as a comparison for future changes. Once risks have been mitigated and security put in place, a baseline is formally reviewed and agreed upon, after which all further comparisons and development are measured against it. A baseline results in a consistent reference point.

Let's say that your doctor has told you that you're overweight due to your diet of donuts, pizza, and soda. (This is very frustrating to you because the supplement company's TV commercial said you could eat whatever you wanted and just take their very expensive pills every day and lose weight.) The doctor tells you that you need to exercise each day and elevate your heart rate to double its normal rate for 30 minutes twice a day. How do you know when you are at double your heart rate? You find out your baseline (regular heart rate) by using a heart rate monitor or going old school and manually taking your pulse with a stopwatch. So you start at your baseline and continue to exercise until you have doubled your heart rate or die, whichever comes first.

Baselines are also used to define the minimum level of protection required. In security, specific baselines can be defined per system type, which indicates the necessary settings and the level of protection being provided. For example, a company may stipulate that all accounting systems must meet an Evaluation Assurance Level (EAL) 4 baseline. This means that only systems that have gone through the Common Criteria process and achieved this rating can be used in this department. Once the systems are properly configured, this is the necessary baseline. When new software is installed, when patches or upgrades are applied to existing software, or when other changes to the system take place, there is a good chance the system may no longer be providing its necessary minimum level of protection (its baseline). Security personnel must assess the systems as changes take place and ensure that the baseline level of security is always being met. If a technician installs a patch on a system and does not ensure the baseline is still being met, there could be new vulnerabilities introduced into the system that will allow attackers easy access to the network.

NOTE Baselines that are not technology oriented should be created and enforced within organizations as well. For example, a company can mandate that while in the facility all employees must have a badge with a picture ID in view at all times. It can also state that visitors must sign in at a front desk and be escorted while in the facility. If these rules are followed, then this creates a baseline of protection.

Guidelines

Guidelines are recommended actions and operational guides to users, IT staff, operations staff, and others when a specific standard does not apply. They can also be used as a recommended way to achieve specific standards when those do apply. Guidelines can deal with the methodologies of technology, personnel, or physical security. Life is full of gray areas, and guidelines can be used as a reference during those times. Whereas standards are specific mandatory rules, guidelines are general approaches that provide the necessary flexibility for unforeseen circumstances.

A policy might state that access to confidential data must be audited. A supporting guideline could further explain that audits should contain sufficient information to allow for reconciliation with prior reviews. Supporting procedures would outline the necessary steps to configure, implement, and maintain this type of auditing.

Procedures

Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal. The steps can apply to users, IT staff, operations staff, security members, and others who may need to carry out specific tasks. Many organizations have written procedures on how to install operating systems, configure security mechanisms, implement access control lists, set up new user accounts, assign computer privileges, audit activities, destroy material, report incidents, and much more.

Procedures are considered the lowest level in the documentation chain because they are closest to the computers and users (compared to policies) and provide detailed steps for configuration and installation issues.

Procedures spell out how the policy, standards, and guidelines will actually be implemented in an operating environment. If a policy states that all individuals who access confidential information must be properly authenticated, the supporting procedures will explain the steps for this to happen by defining the access criteria for authorization, how access control mechanisms are implemented and configured, and how access activities are audited. If a policy states that backups should be performed, then the procedures will define the detailed steps necessary to perform the backup, the timelines of backups, the storage of backup media, and so on. Procedures should be detailed enough to be both understandable and useful to a diverse group of individuals.

Implementation

To tie these items together, let's walk through an implementation example. A corporation's security *policy* indicates that confidential information should be properly protected.

It states the issue in very broad and general terms. A supporting *standard* mandates that all customer information held in databases must be encrypted with the Advanced Encryption Standard (AES) algorithm while it is stored and that it cannot be transmitted over the Internet unless IPSec encryption technology is used. The standard indicates what type of protection is required and provides another level of granularity and explanation. The supporting *procedures* explain exactly how to implement the AES and IPSec technologies, and the *guidelines* cover how to handle cases when data is accidentally corrupted or compromised during transmission. Once the software and devices are configured as outlined in the procedures, this is considered the *baseline* that must always be maintained. All of these work together to provide a company with a security structure.

Unfortunately, security policies, standards, procedures, baselines, and guidelines often are written because an auditor instructed a company to document these items, but then they are placed on a file server and are not shared, explained, or used. To be useful, they must be put into action. Employees aren't going to follow the rules if they don't know the rules exist. Security policies and the items that support them not only must be developed but must also be implemented and enforced.

To be effective, employees need to know about security issues within these documents; therefore, the policies and their supporting counterparts need visibility. Awareness training, manuals, presentations, newsletters, and screen banners can achieve this visibility. It must be clear that the directives came from senior management and that the full management staff supports these policies. Employees must understand what is expected of them in their actions, behaviors, accountability, and performance.

Implementing security policies and the items that support them shows due care by the company and its management staff. Informing employees of what is expected of them and the consequences of noncompliance can come down to a liability issue. For example, if a company fires an employee because he was downloading pornographic material to the company's computer, the employee may take the company to court and win if the employee can prove he was not properly informed of what was considered acceptable and unacceptable use of company property and what the consequences were. Security awareness training is covered later in this chapter, but personnel security is much broader than that.

Personnel Security

Although society has evolved to be extremely dependent upon technology in the workplace, people are still the key ingredient to a successful company. But in security circles, people are often the weakest link. Either accidentally through mistakes or lack of training, or intentionally through fraud and malicious intent, personnel cause more serious and hard-to-detect security issues than hacker attacks, outside espionage, or equipment failure. Although the future actions of individuals cannot be predicted, it is possible to minimize the risks by implementing preventive measures. These include hiring the most qualified individuals, performing background checks, using detailed job descriptions, providing necessary training, enforcing strict access controls, and terminating individuals in a way that protects all parties involved.

Several items can be put into place to reduce the possibilities of fraud, sabotage, misuse of information, theft, and other security compromises. *Separation of duties (SoD)* makes sure that one individual cannot complete a critical task by herself. In the movies, when a submarine captain needs to launch a nuclear missile to blow up the enemy and save (or end) civilization as we know it, the launch usually requires two codes to be entered into the launching mechanism by two different senior crewmembers. This is an example of separation of duties, and it ensures that the captain cannot complete such an important and terrifying task all by himself.

Separation of duties is a security control that can reduce the potential for fraud. For example, an employee cannot complete a critical financial transaction by herself. She will need to have her supervisor's approval before the transaction can be completed. There is usually a third person involved who verifies that this procedure was followed.

In an organization that practices separation of duties, collusion must take place for fraud to be committed. *Collusion* means that at least two people are working together to cause some type of destruction or fraud. In our example, the employee and her supervisor must be participating in the fraudulent activity to make it happen. Even if this were to happen, the third person who reviewed the transaction would provide a way to detect this collusion early enough (hopefully) to stop the transaction.

Two variations of separation of duties are *split knowledge* and *dual control*. In both cases, two or more individuals are authorized and required to perform a duty or task. In the case of split knowledge, no one person knows or has all the details to perform a task. For example, two managers might be required to open a bank vault, with each only knowing part of the combination. In the case of dual control, two individuals are again authorized to perform a task, but both must be available and active in their participation to complete the task or mission. For example, two officers must perform an identical key-turn in a nuclear missile submarine, each out of reach of the other, to launch a missile. The control here is that no one person has the capability of launching a missile, because they cannot reach to turn both keys at the same time.

These are examples of what is generally known as an *m of n control*, which is a control that requires a certain number of agents (*m*) out of a pool of authorized agents (*n*) to complete an operation. This type of control can also be called *quorum authentication*, because it requires the collaboration of a certain number of individuals (the quorum). In the bank vault example, if there were five managers authorized to open the vault and two were required to actually open it, this would be a 2 of 5 control, since $m = 2$ and $n = 5$. You don't want to make *n* too big because that increases the odds that two individuals could secretly conspire to do something harmful. On the other hand, you would not want *m* and *n* to have the same value, since the loss of any one individual would render the vault unopenable!

Job rotation (rotation of assignments) is an administrative detective control that can be put into place to uncover fraudulent activities. No one person should stay in one position for a long time because they may end up having too much control over a segment of the business. Such total control could result in fraud or the misuse of resources. Employees should be moved into different roles with the idea that they may be able to detect suspicious activity carried out by the previous employee filling that position. This type of control is commonly implemented in financial institutions.

Employees in sensitive areas should be forced to take their vacations, which is known as a *mandatory vacation*. While they are on vacation, other individuals fill their positions and thus can usually detect any fraudulent errors or activities. Two of the many ways to detect fraud or inappropriate activities would be the discovery of activity on someone's user account while they're supposed to be away on vacation, or if a specific problem stopped while someone was away and not active on the network. These anomalies are worthy of investigation. Employees who carry out fraudulent activities commonly do not take vacations because they do not want anyone to figure out what they are doing behind the scenes. This is why they must periodically be required to be away from the organization for a period of time, usually two weeks. Placing someone on administrative leave during an investigation is also a form of mandatory vacation.

Candidate Screening and Hiring

The issues, policies, and procedures discussed in the previous section are important to consider in the daily operations of your organization's staff, but let's not get too far ahead of ourselves. Personnel security starts way before a staff member shows up for work. Hiring the right candidate for a position can have a significant impact on the organization's security.

Depending on the position to be filled, human resources should perform a level of candidate screening to ensure that the company hires the right individual for the right job. Each candidate's skills should be tested and evaluated, and the caliber and character of the individual should be examined. Joe might be the best programmer in the state, but if someone looks into his past and finds out he served prison time because he hacked into a bank, the hiring manager might not be so eager to bring Joe into the organization.

Human resources should contact candidates' references, review their military records, if applicable, verify their educational background, obtain their credit report, check out their publicly viewable social media presence, and, if necessary, require proof of a recently administered negative drug test. Many times, candidates are able to conceal important personal behaviors, which is why hiring practices now include scenario questions, personality tests, and observations of the individual, instead of just looking at a person's work history. When a person is hired, he is bringing his skills and whatever other baggage he carries. A company can reduce its heartache pertaining to personnel by first conducting useful and careful hiring practices.

The goal is to hire the "right person" and not just hire a person for "right now." Employees represent an investment on the part of the organization, and by taking the time and hiring the right people for the jobs, the organization will be able to maximize its investment and achieve a better return. Many organizations place a lot of value on determining whether a candidate is a good "cultural" fit. This means that the person will blend well into the culture that already exists in the company. People who fit in are more likely to follow the existing norms, policies, and procedures.

A detailed background check can reveal some interesting information. Things like unexplained gaps in employment history, the validity and actual status of professional certifications, criminal records, driving records, job titles that have been misrepresented, credit histories, unfriendly terminations, appearances on suspected terrorist watch lists, and even real reasons for having left previous jobs can all be determined through the use

of background checks. This has real benefit to the employer and the organization because it serves as the first line of defense for the organization against being attacked from within. Any negative information found in these areas could be indicators of potential problems that the candidate could create for the company at a later date if hired. Take the credit report, for instance. On the surface, the candidate's credit standing may seem to be personal information that the organization doesn't need to know about, but if the report indicates the potential employee has a poor credit standing and a history of financial problems, your organization certainly won't want to place that person in charge of its accounting, or even the petty cash.

Ultimately, the goal of performing background checks is to achieve several different things for the organization at the same time:

- Mitigate risk
- Lower hiring and training costs and the turnover rate for employees
- Protect customers and employees from someone who could potentially conduct malicious and dishonest actions that could harm the organization, its employees, and its customers as well as the general public

In many cases, it is also harder to go back and conduct background checks after the individual has been hired and is working, because there will need to be a specific cause or reason for conducting this kind of investigation. If any employee moves to a position of greater security sensitivity or potential risk, a follow-up investigation should be considered.

Possible background check criteria could include

- National identification number trace
- Criminal check
- Sexual offender registry check
- Employment verification
- Education verification
- Professional reference verification
- Immigration check
- Professional license/certification verification
- Credit report
- Drug screening

Employment Agreements and Policies

Congratulations! Your organization found the right candidate who passed its screening with flying colors and accepted the offer of employment. Now what? Depending on the jurisdiction in which your organization is located, it may be legally required as an employer to enter into a contract or other agreement with the candidate in order for the

hiring action to be official. Whether or not this is a requirement for your organization, it is almost always a good idea to put this employment agreement in writing and ensure that it is signed by both parties. If you are a hiring manager, you should always follow the guidance provided by your human resources and legal teams, but it is useful to be aware of how this all works.

One of the key elements of an employment agreement is a reference to the policies that are applicable to employees in their new roles. Again, depending on where you are in the world, some policies (typically those dealing with safety and welfare) may be required to be included or referenced in the agreement. At a minimum, the employment agreement should include language pointing to the employee manual or other repository of policies for your organization. The point is that every new hire should sign an agreement stating that they are aware of the policies with which they must comply as a condition of employment. This becomes particularly helpful if there are any allegations of misconduct later on. For example, absent a signed employment agreement, if an employee deliberately (or even maliciously) accesses a computer or files that she shouldn't, she could claim she was never told it was wrong and get off the hook. According to the Federal Bureau of Investigation (FBI) manual on prosecuting computer crimes, "it is relatively easy to prove that a defendant had only limited authority to access a computer in cases where the defendant's access was limited by restrictions that were memorialized in writing, such as terms of service, a computer access policy, a website notice, or an employment agreement or similar contract."

Another important element of an employment agreement is the establishment of a probationary period. This is a period of time during which it is relatively easy to fire the new employee for misconduct or just failing to live up to expectations. Depending on the laws in your jurisdiction, it could be difficult to get rid of an employee even if it's obvious they are not working out. A probationary period could be helpful should you decide that your new hire is not as good as you thought.

Onboarding, Transfers, and Termination Processes

Onboarding is the process of turning a candidate into a trusted employee who is able to perform all assigned duties. Having a structured and well-documented onboarding process not only will make the new employee feel valued and welcome but will also ensure that your organization doesn't forget any security tasks. Though the specific steps will vary by organization, the following are some that are pretty universal:

- The new employee attends all required security awareness training.
- The new employee must read all security policies, be given an opportunity to have any questions about the policies answered, and sign a statement indicating they understand and will comply with the policies.
- The new employee is issued all appropriate identification badges, keys, and access tokens pursuant to their assigned roles.
- The IT department creates all necessary accounts for the new employee, who signs into the systems and sets their passwords (or changes any temporary passwords).

Organizations should develop *nondisclosure agreements (NDAs)* and require them to be signed by new employees to protect the organization and its sensitive information. NDAs typically specify what is considered sensitive information, how it should be protected, when it can be shared with others, and how long these obligations last after the employee (or the agreement) is terminated.

One of the most overlooked issues in personnel security is what happens when an employee's role within the organization changes. This could be a promotion (or demotion), assumption of new additional roles, loss of old roles, transfer to another business unit, or perhaps the result of a total restructuring of a business unit. Typically, what happens is that whatever old authorizations the employee had are never taken away, but new ones are added. Over time, employees who've been transferred or reassigned could accumulate a very extensive set of authorizations on information systems that they no longer need to access. IT and security staff need to be involved in transfers and role changes so that they can determine what policies apply and which permissions should be added, left in place, or removed. The goal is to ensure that every staff member has the permissions they need to do their jobs, and not a single one more.

Unfortunately, sometimes organizations have to terminate employees. Because terminations can happen for a variety of reasons, and terminated people have different reactions, companies should have a specific set of procedures to follow with every termination to ensure that their security posture isn't undermined in the process. For example:

- The employee must leave the facility immediately under the supervision of a manager or security guard.
- The employee must surrender any identification badges or keys, be asked to complete an exit interview, and return company supplies.
- That user's accounts and passwords must be disabled or changed immediately.

These actions may seem harsh when they actually take place, but too many companies have been hurt by vengeful employees who have retaliated against the companies after their positions were revoked for one reason or another. If an employee is disgruntled in any way or the termination is unfriendly, that employee's accounts must be disabled right away, and all passwords on all systems must be changed.

Practical Tips on Terminations

Without previous arrangement, an employee cannot be compelled to complete an exit interview, despite the huge value to the company of conducting such interviews. Neither can an employee be compelled to return company property, as a practical matter, if he or she simply chooses not to. The best way to motivate departing employees to comply is to ensure that any severance package they may be eligible for is contingent upon completion of these tasks, and that means having them agree to such conditions up-front, as part of their employment agreement.

Vendors, Consultants, and Contractors

Many companies today could not perform their business functions without the services of an assortment of vendors, consultants, and contractors who have different levels of access to the companies' facilities and information systems. From the janitorial staff who have physical access to virtually any area of a facility to the outsourced software developers in a different country who could introduce (willingly or otherwise) vulnerabilities (or even backdoors) to the companies' most sensitive systems, the risks associated with vendors, consultants, and contractors can be significant if left unmitigated.

There are a number of approaches to dealing with third parties in your environment from an information security standpoint. One approach is to enter into service agreements that require contractors to use security controls that are at least as stringent as your organization's security controls, *and* to prove it. The service agreement could include specific requirements for security controls or leverage existing standards such as the International Organization for Standardization (ISO) 27001 certification (which we discuss in Chapter 4). Either way, the agreement must specify a way to verify compliance with the contractual obligations and clearly state the penalties for failing to meet those obligations.

Another approach to dealing with third parties is to assume that vendors, consultants, and contractors are untrusted and place strict controls around every aspect of their performance. For example, you could require that janitors be escorted by designated employees and that outsourced developers work on virtual desktop infrastructure under the control of your organization. You could also require that highly sensitive assets (e.g., proprietary algorithms, trade secrets, and customer data) be off limits to these third parties. This approach will likely reduce certain risks but may not be ideal for building partnerships or engendering mutual trust.

There is no single best way to deal with the security issues inherent in working with third parties. As with every aspect of personnel security, you should work in close coordination with your business units, human resources staff, and legal counsel. Coordinating with legal counsel is particularly critical, because your organization's liability may (and often does) extend to the actions and inactions of your vendors, consultants, and contractors. For example, if your organization's network is breached because one of your contractors violated policies and that breach resulted in customers' PII being stolen and causing them financial losses, your company could be liable for their damages. This is known as *downstream liability*.

Compliance Policies

There are many forms of liability that may pertain to your organization. Your organization may be subject to external regulations that require special attention and compliance from a security standpoint. Examples are healthcare providers in the United States, who fall under the Healthcare Insurance Portability and Accountability Act (HIPAA); companies that handle payment card information, which must follow the Payment Card Industry Data Security Standard (PCI DSS); and organizations that handle personal information of citizens of the European Union, which fall under the General Data Protection Regulation (GDPR). Many more examples exist, but the point is that if your organization is regulated,

then your personnel security practices must comply with these regulations. As a security leader, you should know which regulations apply to your organization and how security policies, including personnel security ones, work to ensure regulatory compliance.

Privacy Policies

Even if your organization doesn't fall under GDPR or any of the myriad of similar privacy regulations and laws, there are good reasons for you to ensure that your organization has a privacy policy and that your information security practices are aligned with it. For example, suppose you have a policy that allows employees to privately check personal webmail during their breaks, and you also have a policy of decrypting and inspecting all web traffic on your networks to ensure no adversaries are using encryption to sneak around your security controls. These two policies could be in conflict with each other. Worse yet, an employee could sue for violation of privacy if his e-mail messages are intercepted and read by your security team.

Security Awareness, Education, and Training Programs

Even if you develop security policies that protect organizational assets and are aligned with all relevant laws and regulations, it is all for naught if nobody knows what they are expected to do. For an organization to achieve the desired results of its security program, it must communicate the what, how, and why of security to its employees. Security awareness training should be comprehensive, tailored for specific groups, and organization-wide. It should repeat the most important messages in different formats; be kept up to date; be entertaining, positive, and humorous; be simple to understand; and—most important—be supported by senior management. Management must allocate the resources for this activity and enforce its attendance within the organization.

The goal is for each employee to understand the importance of security to the company as a whole and to each individual. Expected responsibilities and acceptable behaviors must be clarified, and noncompliance repercussions, which could range from a warning to dismissal, must be explained before being invoked. Security awareness training can modify employees' behavior and attitude toward security. This can best be achieved through a formalized process of security awareness training.

Degree or Certification?

Some roles within the organization need hands-on experience and skill, meaning that the hiring manager should be looking for specific industry certifications. Some positions require more of a holistic and foundational understanding of concepts or a business background, and in those cases a degree may be required. Table 1-3 provides more information on the differences between awareness, training, and education.

	Awareness	Training	Education
Attribute	"What"	"How"	"Why"
Level	Information	Knowledge	Insight
Learning objective	Recognition and retention	Skill	Understanding
Example teaching method	**Media:** Videos Newsletters Posters CBT Social engineering testing	**Practical Instruction:** Lecture and/or demo Case study Hands-on practice	**Theoretical Instruction:** Seminar and discussion Reading and study Research
Test measure	True/False, multiple choice (identify learning)	Problem solving—i.e., recognition and resolution (apply learning)	Essay (interpret learning)
Impact timeframe	Short-term	Intermediate	Long-term

Table 1-3 Aspects of Awareness, Training, and Education

Methods and Techniques to Present Awareness and Training

Because security is a topic that can span many different aspects of an organization, it can be difficult to communicate the correct information to the right individuals. By using a formalized process for security awareness training, you can establish a method that will provide you with the best results for making sure security requirements are presented to the right people in an organization. This way you can make sure everyone understands what is outlined in the organization's security program, why it is important, and how it fits into the individual's role in the organization. The higher levels of training typically are more general and deal with broader concepts and goals, and as the training moves down to specific jobs and tasks, it becomes more situation specific as it directly applies to certain positions within the company.

A security awareness program is typically created for at least three types of audiences: management, staff, and technical employees. Each type of awareness training must be geared toward the individual audience to ensure each group understands its particular responsibilities, liabilities, and expectations. If technical security training were given to senior management, their eyes would glaze over as soon as protocols and firewalls were mentioned. On the flip side, if legal ramifications, company liability issues pertaining to protecting data, and shareholders' expectations were discussed with the IT group, they would quickly turn to their smartphone and start tweeting, browsing the Internet, or texting their friends.

Members of senior management would benefit the most from a short, focused security awareness orientation that discusses corporate assets and financial gains and losses pertaining to security. They need to know how stock prices can be negatively affected by compromises, understand possible threats and their outcomes, and know why security

must be integrated into the environment the same way as other business processes. Because members of management must lead the rest of the company in support of security, they must gain the right mindset about its importance.

Middle management would benefit from a more detailed explanation of the policies, procedures, standards, and guidelines and how they map to the individual departments for which each middle manager is responsible. Middle managers should be taught why their support for their specific departments is critical and what their level of responsibility is for ensuring that employees practice safe computing activities. They should also be shown how the consequences of noncompliance by individuals who report to them can affect the company as a whole and how they, as managers, may have to answer for such indiscretions.

Staff training, which typically involves the largest portion of an organization, should provide plenty of examples of specific behaviors that are expected, recommended, and forbidden. This is an opportunity to show how alert users can be sensors providing early warning of attacks, which can dramatically improve the security posture of any organization. This can be accomplished by training the staff to recognize and report the sorts of attacks they are likely to face. Conversely, it is important to also show the consequences, organizational and personal, of being careless or violating policies and procedures.

The technical departments must receive a different presentation that aligns more to their daily tasks. They should receive a more in-depth training to discuss technical configurations, incident handling, and how to recognize different types of security compromises.

Perhaps no other topic is more important or better illustrates the need to communicate security issues differently to each of these three audiences than the topic of social engineering. *Social engineering* is the deliberate manipulation of a person or group of persons to persuade them to do something they otherwise wouldn't or shouldn't. In a security context, this typically means getting a member of the organization to violate a security policy or procedure or to help an attacker compromise a system. The most common form of social engineering is *phishing*, which is the use of e-mail messages to perform social engineering. While all employees should know that they should not click on links or open attachments in e-mail messages if they don't recognize the sender, executives, managers, and end users should be presented the problem in a different light.

Regardless of how the training is presented, it is usually best to have each employee sign a document indicating they have heard and understand all the security topics discussed and that they also understand the ramifications of noncompliance. This reinforces the policies' importance to the employee and also provides evidence down the road if the employee claims they were never told of these expectations. Awareness training should happen during the hiring process and at least annually after that. Attendance of training should also be integrated into employment performance reports.

Various methods should be employed to reinforce the concepts of security awareness. Things like screen banners, employee handbooks, and even posters can be used as ways to remind employees about their duties and the necessities of good security practices. But there are other ways to drive employee engagement. For example, *gamification* is the application of elements of game play to other activities such as security awareness training. By some accounts, gamification can improve employees' skill retention by 40 percent. Another approach is to leverage employees who are not formally part of the

security program and yet have the skills and aptitudes that make them security advocates within their own business units. These individuals can be identified and deliberately nurtured to act as conduits between business units and the security program. They can become *security champions*, which are members of an organization that, though their job descriptions do not include security, inform and encourage the adoption of security practices within their own teams.

Periodic Content Reviews

The only constant in life is change, so it should come as no surprise that after we develop the curricula and materials for security awareness training, we have to keep them up to date by conducting periodic content reviews. It is essential that this be a deliberate process and not done in an ad hoc manner. One way to do this is to schedule refreshes at specific intervals like semi-annually or yearly and assign the task to an individual owner. This person would work with a team to review and update the plan and materials but is ultimately responsible for keeping the training up to date.

Another approach is to have content reviews be triggered by other events. For example, reviews can be required whenever any of the following occur:

- A security policy is added, changed, or discontinued
- A major incident (or pattern of smaller incidents) occurs that could've been avoided or mitigated through better security awareness
- A major new threat is discovered
- A major change is made to the information systems or security architecture
- An assessment of the training program shows deficiencies

Program Effectiveness Evaluation

Many organizations treat security awareness training as a "check in the box" activity that is done simply to satisfy a requirement. The reality, however, is that effective training has both objectives (why we do it) and outcomes (what people can do after participating in it). The objectives are usually derived from senior-level policies or directives and drive the development of outcomes, which in turn drive the content and methods of delivery. For example, if the objective is reducing the incidence of successful phishing attacks, then it would be appropriate to pursue an outcome of having end users be able to detect a phishing e-mail. Both the objective and the outcome are measurable, which makes it easier to answer the question "is this working?"

We can evaluate whether the security training program is effective in improving an organization's security posture by simply measuring things before the training and then after it. Continuing the earlier example, we could keep track of the number of successful phishing attacks and see what happens to that number after the training has been conducted. This would be an assessment of the objective. We could also take trained and untrained users and test their ability to detect phishing e-mails. We would expect the trained users to fare better at this task, which would test the outcome. If we see that the number of phishing

attacks remains unchanged (or worse, grows) or that the users are no better at detecting phishing e-mails after the training, then maybe the program is not effective.

When assessing the effectiveness of a training program, it is very important to analyze the data and not jump to conclusions. In the phishing example, there are many possible explanations for the lack of improvement. Maybe the adversaries are sending more-sophisticated messages that are harder to detect. Similarly, the results could simply show that the users just don't care and will continue to click links and open attachments until the consequences become negative enough for them. The point is to consider the root causes of the measurements when assessing the training.

Professional Ethics

Security awareness and training, of course, build on the notion that there are right ways and wrong ways in which to behave. This is the crux of ethics, which can be based on many different issues and foundations. Ethics can be relative to different situations and interpreted differently from individual to individual. Therefore, they are often a topic of debate. However, some ethics are less controversial than others, and these types of ethics are easier to expect of all people.

An interesting relationship exists between law and ethics. Most often, laws are based on ethics and are put in place to ensure that others act in an ethical way. However, laws do not apply to everything—that is when ethics should kick in. Some things may not be illegal, but that does not necessarily mean they are ethical.

Certain common ethical fallacies are used by many in the computing world to justify unethical acts. They exist because people look at issues differently and interpret (or misinterpret) rules and laws that have been put into place. The following are examples of these ethical fallacies:

- Hackers only want to learn and improve their skills. Many of them are not making a profit off of their deeds; therefore, their activities should not be seen as illegal or unethical.
- The First Amendment protects and provides the right for U.S. citizens to write viruses.
- Information should be shared freely and openly; therefore, sharing confidential information and trade secrets should be legal and ethical.
- Hacking does not actually hurt anyone.

(ISC)² Code of Professional Ethics

(ISC)² requires all certified system security professionals to commit to fully supporting its Code of Ethics. If a CISSP intentionally or knowingly violates this Code of Ethics, he or she may be subject to a peer review panel, which will decide whether the certification should be revoked.

The (ISC)² Code of Ethics for the CISSP is listed on the (ISC)² site at https://www.isc2.org/Ethics. The following list is an overview, but each CISSP candidate should read

the full version and understand the Code of Ethics before attempting this exam. The code's preamble makes it clear that "[t]he safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior." It goes on to provide four canons for CISSPs:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

Organizational Code of Ethics

More regulations are requiring organizations to have an ethical statement and potentially an ethical program in place. The ethical program is to serve as the "tone at the top," which means that the executives need to ensure not only that their employees are acting ethically but also that they themselves are following their own rules. The main goal is to ensure that the motto "succeed by any means necessary" is not the spoken or unspoken culture of a work environment. Certain structures can be put into place that provide a breeding ground for unethical behavior. If the CEO gets more in salary based on stock prices, then she may find ways to artificially inflate stock prices, which can directly hurt the investors and shareholders of the company. If managers can only be promoted based on the amount of sales they bring in, these numbers may be fudged and not represent reality. If an employee can only get a bonus if a low budget is maintained, he might be willing to take shortcuts that could hurt company customer service or product development. Although ethics seem like things that float around in the ether and make us feel good to talk about, they have to be actually implemented in the real corporate world through proper business processes and management styles.

The Computer Ethics Institute

The *Computer Ethics Institute* is a nonprofit organization that works to help advance technology by ethical means.

The Computer Ethics Institute has developed its own Ten Commandments of Computer Ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.

7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Chapter Review

This chapter laid out some of the fundamental principles of cybersecurity: the meaning of security, how it is governed, and the means by which it is implemented in an enterprise. It then focused on the most important aspect of security: people. They are the most important asset to any organization and can also be the greatest champions, or underminers, of cybersecurity. The difference lies in who we hire, what roles we assign to them, and how we train them. Bring the right people into the right seats and train them well and you'll have a robust security posture. Do otherwise at your own peril.

Our collective goal in information systems security boils down to ensuring the availability, integrity, and confidentiality of our information in an environment rich in influencers. These include organizational goals, assets, laws, regulations, privacy, threats, and, of course, people. Each of these was discussed in some detail in this chapter. Along the way, we also covered tangible ways in which we can link security to each of the influencers. As CISSPs we must be skilled in creating these linkages, as we are trusted to be able to apply the right solution to any security problem.

Quick Review

- The objectives of security are to provide confidentiality, integrity, availability, authenticity, and nonrepudiation.
- Confidentiality means keeping unauthorized entities (be they people or processes) from gaining access to information assets.
- Integrity means that that an asset is free from unauthorized alterations.
- Availability protection ensures reliability and timely access to data and resources to authorized individuals.
- Authenticity protections ensure we can trust that something comes from its claimed source.
- Nonrepudiation, which is closely related to authenticity, means that someone cannot disavow being the source of a given action.
- A vulnerability is a weakness in a system that allows a threat source to compromise its security.

- A threat is any potential danger that is associated with the exploitation of a vulnerability.
- A threat source (or threat agent, or threat actor) is any entity that can exploit a vulnerability.
- A risk is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact.
- A control, or countermeasure, is put into place to mitigate (reduce) the potential risk.
- Security governance is a framework that provides oversight, accountability, and compliance.
- An information security management system (ISMS) is a collection of policies, procedures, baselines, and standards that an organization puts in place to make sure that its security efforts are aligned with business needs, streamlined, and effective and that no security controls are missing.
- An enterprise security architecture implements an information security strategy and consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally.
- An enterprise security architecture should tie in strategic alignment, business enablement, process enhancement, and security effectiveness.
- Security governance is a framework that supports the security goals of an organization being set and expressed by senior management, communicated throughout the different levels of the organization, and consistently applied and assessed.
- Senior management always carries the ultimate responsibility for the organization.
- A security policy is a statement by management dictating the role security plays in the organization.
- Standards are documents that describe specific requirements that are compulsory in nature and support the organization's security policies.
- A baseline is a minimum level of security.
- Guidelines are recommendations and general approaches that provide advice and flexibility.
- Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal.
- Job rotation and mandatory vacations are administrative security controls that can help detect fraud.
- Separation of duties ensures no single person has total control over a critical activity or task.
- Split knowledge and dual control are two variations of separation of duties.

- Social engineering is an attack carried out to manipulate a person into providing sensitive data to an unauthorized individual.
- Security awareness training should be comprehensive, tailored for specific groups, and organization-wide.
- Gamification is the application of elements of game play to other activities such as security awareness training.
- Security champions, which are members of an organization that, though their job descriptions do not include security, inform and encourage the adoption of security practices within their own teams.
- Professional ethics codify the right ways for a group of people to behave.

Questions

Please remember that these questions are formatted and asked in a certain way for a reason. Keep in mind that the CISSP exam is asking questions at a conceptual level. Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. Instead, the candidate should look for the best answer in the list.

1. Which factor is the most important item when it comes to ensuring security is successful in an organization?
   - **A.** Senior management support
   - **B.** Effective controls and implementation methods
   - **C.** Updated and relevant security policies and procedures
   - **D.** Security awareness by all employees

Use the following scenario to answer Questions 2–4. Todd is a new security manager and has the responsibility of implementing personnel security controls within the financial institution where he works. Todd knows that many employees do not fully understand how their actions can put the institution at risk; thus, he needs to develop a security awareness program. He has determined that the bank tellers need to get a supervisory override when customers have checks over $3,500 that need to be cashed. He has also uncovered that some employees have stayed in their specific positions within the company for over three years. Todd would like to be able to investigate some of the activities of bank personnel to see if any fraudulent activities have taken place. Todd is already ensuring that two people must use separate keys at the same time to open the bank vault.

2. Todd documents several fraud opportunities that the employees have at the financial institution so that management understands these risks and allocates the funds and resources for his suggested solutions. Which of the following best describes the control Todd should put into place to be able to carry out fraudulent investigation activity?

A. Separation of duties

B. Job rotation

C. Mandatory vacations

D. Split knowledge

3. If the financial institution wants to ensure that fraud cannot happen successfully unless collusion occurs, what should Todd put into place?

A. Separation of duties

B. Job rotation

C. Social engineering

D. Split knowledge

4. Todd wants to be able to prevent fraud from taking place, but he knows that some people may get around the types of controls he puts into place. In those situations he wants to be able to identify when an employee is doing something suspicious. Which of the following incorrectly describes what Todd is implementing in this scenario and what those specific controls provide?

A. Separation of duties, by ensuring that a supervisor must approve the cashing of a check over $3,500. This is an administrative control that provides preventive protection for Todd's organization.

B. Job rotation, by ensuring that one employee only stays in one position for up to three months at a time. This is an administrative control that provides detective capabilities.

C. Security awareness training, which can also emphasize enforcement.

D. Dual control, which is an administrative detective control that can ensure that two employees must carry out a task simultaneously.

5. Which term denotes a potential cause of an unwanted incident, which may result in harm to a system or organization?

A. Vulnerability

B. Exploit

C. Threat

D. Attacker

6. A CISSP candidate signs an ethics statement prior to taking the CISSP examination. Which of the following would be a violation of the (ISC)^2 Code of Ethics that could cause the candidate to lose his or her certification?
   - **A.** E-mailing information or comments about the exam to other CISSP candidates
   - **B.** Submitting comments on the questions of the exam to (ISC)^2
   - **C.** Submitting comments to the board of directors regarding the test and content of the class
   - **D.** Conducting a presentation about the CISSP certification and what the certification means
7. You want to ensure that your organization's finance department, and only the finance department, has access to the organization's bank statements. Which of the security properties would be most important?
   - **A.** Confidentiality
   - **B.** Integrity
   - **C.** Availability
   - **D.** Both A and C
8. You want to make use of the OpenOffice productivity software suite mandatory across your organization. In what type of document would you codify this?
   - **A.** Policy
   - **B.** Standard
   - **C.** Guideline
   - **D.** Procedure
9. For an enterprise security architecture to be successful in its development and implementation, which of the following items is not essential?
   - **A.** Strategic alignment
   - **B.** Security guidelines
   - **C.** Business enablement
   - **D.** Process enhancement
10. Which of the following practices is likeliest to mitigate risks when considering a candidate for hiring?
   - **A.** Security awareness training
   - **B.** Nondisclosure agreement (NDA)
   - **C.** Background checks
   - **D.** Organizational ethics

Answers

1. **A.** Without senior management's support, a security program will not receive the necessary attention, funds, resources, and enforcement capabilities.
2. **C.** Mandatory vacation is an administrative detective control that allows for an organization to investigate an employee's daily business activities to uncover any potential fraud that may be taking place. The employee should be forced to be away from the organization for a two-week period, and another person should be put into that role. The idea is that the person who was rotated into that position may be able to detect suspicious activities.
3. **A.** Separation of duties is an administrative control that is put into place to ensure that one person cannot carry out a critical task by himself. If a person were able to carry out a critical task alone, this could put the organization at risk. Collusion is when two or more people come together to carry out fraud. So if a task was split between two people, they would have to carry out collusion (working together) to complete that one task and carry out fraud.
4. **D.** Dual control is an administrative preventive control. It ensures that two people must carry out a task at the same time, as in two people having separate keys when opening the vault. It is not a detective control. Notice that the question asks what Todd is *not* doing. Remember that on the exam you need to choose the *best* answer. In many situations you will not like the question or the corresponding answers on the CISSP exam, so prepare yourself. The questions can be tricky, which is one reason why the exam itself is so difficult.
5. **C.** The question provides the definition of a threat. The term attacker (option D) could be used to describe a threat agent that is, in turn, a threat, but use of this term is much more restrictive. The best answer is a threat.
6. **A.** A CISSP candidate and a CISSP holder should never discuss with others what was on the exam. This degrades the usefulness of the exam to be used as a tool to test someone's true security knowledge. If this type of activity is uncovered, the person could be stripped of their CISSP certification because this would violate the terms of the NDA into which the candidate enters prior to taking the test. Violating an NDA is a violation of the ethics canon that requires CISSPs to act honorably, honestly, justly, responsibly, and legally.
7. **D.** Confidentiality is ensuring that unauthorized parties (i.e., anyone other than finance department employees) cannot access protected assets. Availability is ensuring that authorized entities (i.e., finance) maintain access to assets. In this case, both confidentiality and availability are important to satisfy the requirements as stated.
8. **B.** Standards describe mandatory activities, actions, or rules. A policy is intended to be strategic, so it would not be the right document. A procedure describes the manner in which something must be done, which is much broader than is needed to make using a particular software suite mandatory across your organization. Finally, guidelines are recommended but optional practices.

9. **B.** Security guidelines are optional recommendations on issues that are not covered by mandatory policies, standards, or procedures. A successful enterprise security architecture is aligned with the organization's strategy, enables its business, and enhances (rather than hinders) its business processes.
10. **C.** The best way to reduce risk is to conduct background checks before you offer employment to a candidate. This ensures you are hiring someone whose past has been examined for any obviously disqualifying (or problematic) issues. The next step would be to sign an employment agreement that would include an NDA, followed by onboarding, which would include security awareness training and indoctrination into the organizational code of ethics.

CHAPTER 2

Risk Management

This chapter presents the following:

- Risk management (assessing risks, responding to risks, monitoring risks)
- Supply chain risk management
- Business continuity

A ship in harbor is safe, but that is not what ships are built for.

—William G.T. Shedd

We next turn our attention to the concept that should underlie every decision made when defending our information systems: risk. Risk is so important to understand as a cybersecurity professional that we not only cover it in detail in this chapter (one of the longest in the book) but also return to it time and again in the rest of the book. We start off narrowly by focusing on the vulnerabilities in our organizations and the threats that would exploit them to cause us harm. That sets the stage for an in-depth discussion of the main components of risk management: framing, assessing, responding to, and monitoring risks. We pay particular attention to supply chain risks, since these represent a big problem to which many organizations pay little or no attention. Finally, we'll talk about business continuity because it is so closely linked to risk management. We'll talk about disaster recovery, a closely related concept, in later chapters.

Risk Management Concepts

Risk in the context of security is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact. *Risk management (RM)* is the process of identifying and assessing risk, reducing it to an acceptable level, and ensuring it remains at that level. There is no such thing as a 100-percent-secure environment. Every environment has vulnerabilities and threats. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Risks to an organization come in different forms, and they are not all computer related. As we saw in Chapter 1, when a company acquires another company, it takes on a lot of risk in the hope that this move will increase its market base, productivity,

and profitability. If a company increases its product line, this can add overhead, increase the need for personnel and storage facilities, require more funding for different materials, and maybe increase insurance premiums and the expense of marketing campaigns. The risk is that this added overhead might not be matched in sales; thus, profitability will be reduced or not accomplished.

When we look at information security, note that an organization needs to be aware of several types of risk and address them properly. The following items touch on the major categories:

- **Physical damage** Fire, water, vandalism, power loss, and natural disasters
- **Human interaction** Accidental or intentional action or inaction that can disrupt productivity
- **Equipment malfunction** Failure of systems and peripheral devices
- **Inside and outside attacks** Hacking, cracking, and attacking
- **Misuse of data** Sharing trade secrets, fraud, espionage, and theft
- **Loss of data** Intentional or unintentional loss of information to unauthorized parties
- **Application error** Computation errors, input errors, and software defects

Threats must be identified, classified by category, and evaluated to calculate their damage potential to the organization. Real risk is hard to measure, but prioritizing the potential risks in the order of which ones must be addressed first is obtainable.

Holistic Risk Management

Who really understands risk management? Unfortunately, the answer to this question is that not enough people inside or outside of the security profession really get it. Even though information security is big business today, the focus all too often is on applications, devices, viruses, and hacking. Although these items all must be considered and weighed in risk management processes, they should be considered pieces of the overall security puzzle, not the main focus of risk management.

Security is a business issue, but businesses operate to make money, not just to be secure. A business is concerned with security only if potential risks threaten its bottom line, which they can in many ways, such as through the loss of reputation and customer base after a database of credit card numbers is compromised; through the loss of thousands of dollars in operational expenses from a new computer worm; through the loss of proprietary information as a result of successful company espionage attempts; through the loss of confidential information from a successful social engineering attack; and so on. It is critical that security professionals understand these individual threats, but it is more important that they understand how to calculate the risk of these threats and map them to business drivers.

To properly manage risk within an organization, you have to look at it holistically. Risk, after all, exists within a context. The U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk*, defines three tiers to risk management:

- **Organization view (Tier 1)** Concerned with risk to the organization as a whole, which means it frames the rest of the conversation and sets important parameters such as the risk tolerance level.
- **Mission/business process view (Tier 2)** Deals with the risk to the major functions of the organization, such as defining the criticality of the information flows between the organization and its partners or customers.
- **Information systems view (Tier 3)** Addresses risk from an information systems perspective. Though this is where we will focus our discussion, it is important to understand that it exists within the context of (and must be consistent with) other, more encompassing risk management efforts.

These tiers are dependent on each other, as shown in Figure 2-1. Risk management starts with decisions made at the organization tier, which flow down to the other two tiers. Feedback on the effects of these decisions flows back up the hierarchy to inform the next set of decisions to be made. Carrying out risk management properly means that you have a holistic understanding of your organization, the threats it faces, the countermeasures that can be put into place to deal with those threats, and continuous monitoring to ensure the acceptable risk level is being met on an ongoing basis.

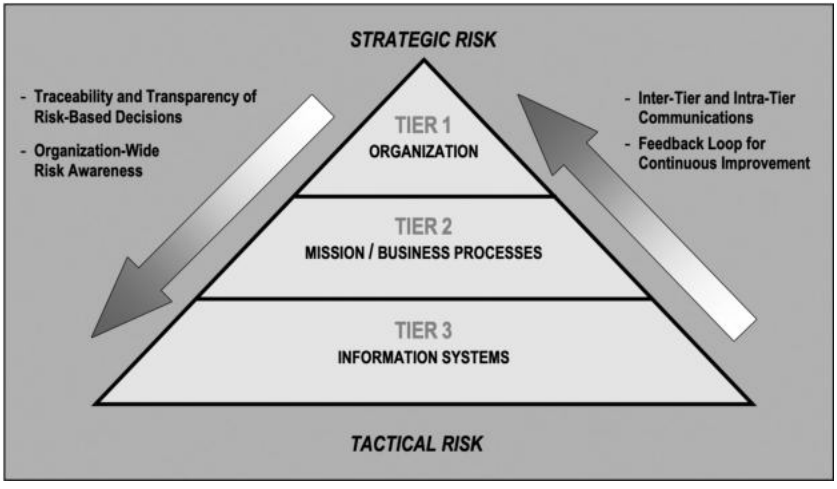


Figure 2-1 The three tiers of risk management (Source: NIST SP 800-39)

Information Systems Risk Management Policy

Proper risk management requires a strong commitment from senior leaders, a documented process that supports the organization's mission, an information systems risk management (ISRM) policy, and a delegated ISRM team. The ISRM policy should be a subset of the organization's overall risk management policy (*risks to an organization include more than just information security issues*) and should be mapped to the organizational security policies. The ISRM policy should address the following items:

- The objectives of the ISRM team
- The level of risk the organization will accept and what is considered an acceptable level of risk
- Formal processes of risk identification
- The connection between the ISRM policy and the organization's strategic planning processes
- Responsibilities that fall under ISRM and the roles to fulfill them
- The mapping of risk to internal controls
- The approach toward changing staff behaviors and resource allocation in response to risk analysis
- The mapping of risks to performance targets and budgets
- Key metrics and performance indicators to monitor the effectiveness of controls

The ISRM policy provides the foundation and direction for the organization's security risk management processes and procedures and should address all issues of information security. It should provide direction on how the ISRM team communicates information on the organization's risks to senior management and how to properly execute management's decisions on risk mitigation tasks.

The Risk Management Team

Each organization is different in its size, security posture, threat profile, and security budget. One organization may have one individual responsible for ISRM or a team that works in a coordinated manner. The overall goal of the team is to ensure that the organization is protected in the most cost-effective manner. This goal can be accomplished only if the following components are in place:

- An established risk acceptance level provided by senior management
- Documented risk assessment processes and procedures
- Procedures for identifying and mitigating risks
- Appropriate resource and fund allocation from senior management
- Security awareness training for all staff members associated with information assets
- The ability to establish improvement (or risk mitigation) teams in specific areas when necessary

- The mapping of legal and regulation compliancy requirements to control and implement requirements
- The development of metrics and performance indicators so as to measure and manage various types of risks
- The ability to identify and assess new risks as the environment and organization change
- The integration of ISRM and the organization's change control process to ensure that changes do not introduce new vulnerabilities

Obviously, this list is a lot more than just buying a new shiny firewall and calling the organization safe.

The ISRM team, in most cases, is not made up of employees with the dedicated task of risk management. It consists of people who already have a full-time job in the organization and are now tasked with something else. Thus, senior management support is necessary so proper resource allocation can take place.

Of course, all teams need a leader, and ISRM is no different. One individual should be singled out to run this rodeo and, in larger organizations, this person should be spending 50 to 70 percent of their time in this role. Management must dedicate funds to making sure this person receives the necessary training and risk analysis tools to ensure it is a successful endeavor.

The Risk Management Process

By now you should believe that risk management is critical to the long-term security (and even success) of your organization. But how do you get this done? NIST SP 800-39 describes four interrelated components that comprise the risk management process. These are shown in Figure 2-2. Let's consider each of these components briefly now, since they will nicely frame the remainder of our discussion of risk management.

- **Frame risk** Risk framing defines the context within which all other risk activities take place. What are our assumptions and constraints? What are the organizational priorities? What is the risk tolerance of senior management?
- **Assess risk** Before we can take any action to mitigate risk, we have to assess it. This is perhaps the most critical aspect of the process, and one that we will discuss at length. If your risk assessment is spot-on, then the rest of the process becomes pretty straightforward.
- **Respond to risk** By now, we've done our homework. We know what we should, must, and can't do (from the framing component), and we know what we're up against in terms of threats, vulnerabilities, and attacks (from the assess component). Responding to the risk becomes a matter of matching our limited resources with our prioritized set of controls. Not only are we mitigating significant risk, but, more importantly, we can tell our bosses what risk we can't do anything about because we're out of resources.

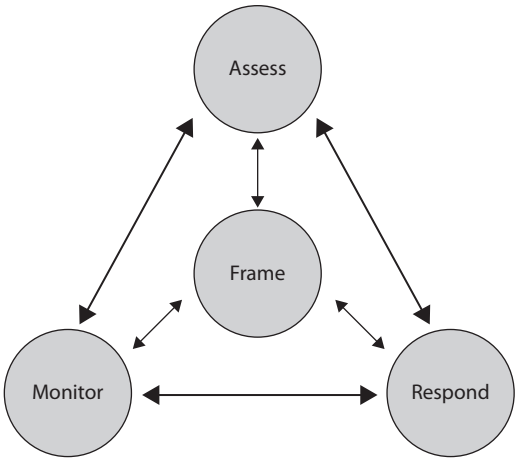


Figure 2-2 The components of the risk management process

- **Monitor risk** No matter how diligent we've been so far, we probably missed something. If not, then the environment likely changed (perhaps a new threat source emerged or a new system brought new vulnerabilities). In order to stay one step ahead of the bad guys, we need to continuously monitor the effectiveness of our controls against the risks for which we designed them.

You will notice that our discussion of risk so far has dealt heavily with the whole framing process. In the preceding sections, we've talked about the organization (top to bottom), the policies, and the team. The next step is to assess the risk, and what better way to start than by understanding threats and the vulnerabilities they might exploit.

Overview of Vulnerabilities and Threats

To focus our efforts on the likely (and push aside the less likely) risks to our organizations, we need to consider what it is that we have that someone (or something) else may be able to take, degrade, disrupt, or destroy. As we will see later (in the section "Assessing Risks"), inventorying and categorizing our information systems is a critical early step in the process. For the purpose of modeling the threat, we are particularly interested in the vulnerabilities inherent in our systems that could lead to the compromise of their confidentiality, integrity, or availability. We then ask the question, "Who would want to exploit this vulnerability, and why?" This leads us to a deliberate study of our potential adversaries, their motivations, and their capabilities. Finally, we determine whether a given threat source has the means to exploit one or more vulnerabilities in order to attack our assets.

NOTE We will discuss threat modeling in detail in Chapter 9.