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, fixedform (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

↟Why Become a CISSP?

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)

↟Why Become a CISSP?

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
Chapter 1
Chapter 2
Chapter 3
Chapter 4

Cybersecurity Governance
Risk Management
Compliance
Frameworks

🡅This page intentionally left blank

🡅1

CHAPTER

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.

Availability

Security objectives

Integrity

Confidentiality

↟Chapter 1: Cybersecurity Governance

5

Confidentiality

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

PART I

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.

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,

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

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 ▪▪▪▪▪, 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.

• 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.

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.

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.

Figure 1-1 The relationships among the different security concepts

agent

Leads to
Threat
Vulnerability
Risk

Directly affects
Asset

Exposure

Safeguard

Can damage

And causes an

Can be
countermeasured by a

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

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

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

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.

Governance model

Vulnerability and threat management

Policy development

Regulations

Development of metrics

Common threats

Vulnerability and threat management

System life cycle security

Policy compliance

Process

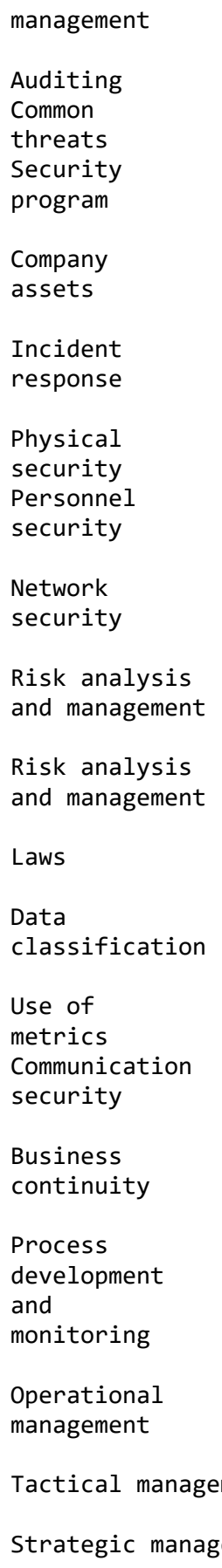

Figure 1-2 A complete security program contains many items.

Organizational
security

Aligning Security to Business Strategy

• 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?

PART I

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:

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 technologyoriented 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

Securityrelated
lifetimes and
deadlines

Logical

Business
information
model

Security
policies

Security
services

Entity schema Security
and privilege domain
profiles
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

• 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)

PART I

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

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

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

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.

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

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

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.

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.

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.

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.

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

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.

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.

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

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

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.

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.

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.

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.

• 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.

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 systemspecific 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

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:

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.

Standards

Mandatory

Procedures

Guidelines

Recommended but optional

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