Senior management has an obligation to protect the organization from a long list of activities that can negatively affect it, including protection from malicious code, natural disasters, privacy violations, infractions of the law, and more. The costs and benefits of this protection should be evaluated in monetary and nonmonetary terms to ensure that the cost of security does not outweigh the expected benefits. Security should be proportional to potential loss estimates pertaining to the severity, likelihood, and extent of potential damage.

As Figure 3-5 shows, there are many costs to consider when it comes to security breaches: loss of business, response activities, customer and partner notification, and detection and escalation measures. These types of costs need to be understood so that the organization can practice proper due care by implementing the necessary controls to reduce the risks and these costs. Security mechanisms should be employed to reduce the frequency and severity of security-related losses. A sound security program is a smart business practice.

Senior management needs to decide upon the amount of risk it is willing to take pertaining to computer and information security, and implement security in an economical and responsible manner. These risks do not always stop at the boundaries of the organization. Many organizations work with third parties, with whom they must share sensitive data. The main organization is still liable for the protection of this sensitive data that it owns, even if the data is on another organization's network. This is why more and more regulations are requiring organizations to evaluate their third-party security measures.

If one of the organizations does not provide the necessary level of protection and its negligence affects a partner it is working with, the affected organization can sue the upstream organization. For example, let's say Company A and Company B have constructed an extranet. Company A does not put in controls to detect and deal with viruses. Company A

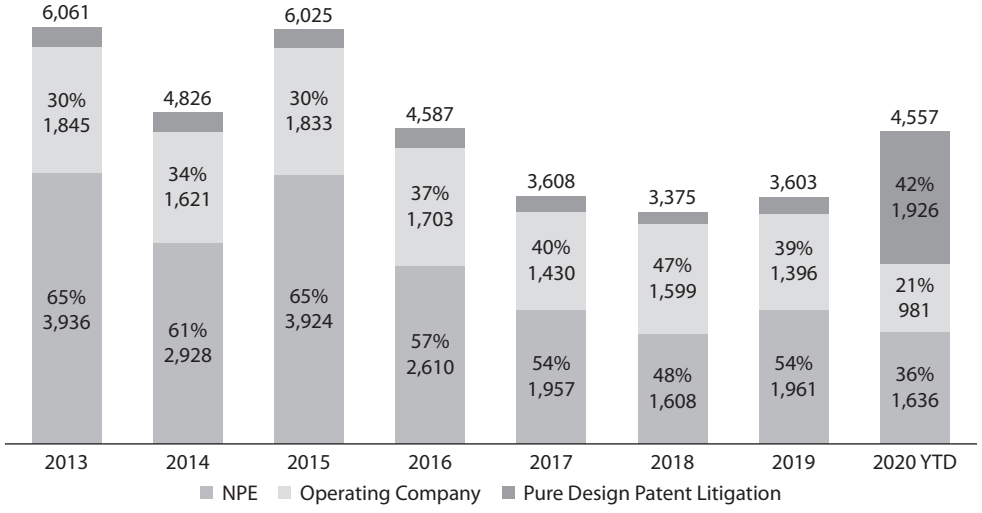

Figure 3-5 Data breach costs (Source: Ponemon Institute and IBM Security)

gets infected with a destructive virus and it is spread to Company B through the extranet. The virus corrupts critical data and causes a massive disruption to Company B's production. Therefore, Company B can sue Company A for being negligent. Both companies need to make sure they are doing their part to ensure that their activities, or the lack of them, will not negatively affect another company, which is referred to as *downstream liability*.

EXAM TIP *Responsibility* generally refers to the obligations and expected actions and behaviors of a particular party. An obligation may have a defined set of specific actions that are required, or a more general and open approach, which enables the party to decide how it will fulfill the particular obligation. *Accountability* refers to the ability to hold a party responsible for certain actions or inaction.

Each company has different requirements when it comes to its list of due care responsibilities. If these steps are not taken, the company may be charged with negligence if damage arises out of its failure to follow these steps. To prove negligence in court, the plaintiff must establish that the defendant had a *legally recognized obligation*, or duty, to protect the plaintiff from unreasonable risks and that the defendant's failure to protect the plaintiff from an unreasonable risk (breach of duty) was the *proximate cause* of the plaintiff's damages. Penalties for negligence can be either civil or criminal, ranging from actions resulting in compensation for the plaintiff to jail time for violation of the law.

EXAM TIP *Proximate cause* is an act or omission that naturally and directly produces a consequence. It is the superficial or obvious cause for an occurrence. It refers to a cause that leads directly, or in an unbroken sequence, to a particular result. It can be seen as an element of negligence in a court of law.

Requirements for Investigations

Investigations are launched for a multitude of specific reasons. Maybe you suspect an employee is using your servers to mine bitcoin after hours, which in most places would be a violation of acceptable use policies. Maybe you think civil litigation is reasonably foreseeable or you uncover evidence of crime on your systems. Sometimes, we are the targets of investigation and not the investigators, such as when a government regulator suspects we are not in compliance. Though the investigative process is similar regardless of the reason, it is important to differentiate the types of investigations you are likely to come across.

Administrative

An *administrative investigation* is one that is focused on policy violations. These represent the least impactful (to the organization) type of investigation and will likely result in administrative action if the investigation supports the allegations. For instance, violations of voluntary industry standards (such as PCI DSS) could result in

an administrative investigation, particularly if the violation resulted in some loss or bad press for the organization. In the worst case, someone can get fired. Typically, however, someone is counseled not to do something again and that is that. Either way, you want to keep your human resources (HR) staff involved as you proceed.

Criminal

A seemingly administrative affair, however, can quickly get stickier. Suppose you start investigating someone for a possible policy violation and along the way discover that person was involved in what is likely criminal activity. A *criminal investigation* is one that is aimed at determining whether there is cause to believe beyond a reasonable doubt that someone committed a crime. The most important thing to consider is that we, as information systems security professionals, are not qualified to determine whether or not someone broke the law; that is the job of law enforcement agencies (LEAs). Our job, once we have reason to believe that a crime may have taken place, is to preserve evidence, ensure the designated people in our organizations contact the appropriate LEA, and assist them in any way that is appropriate.

Civil

Not all statutes are criminal, however, so it is possible to have an alleged violation of a law result in something other than a criminal investigation. The two likeliest ways to encounter this is regarding possible violations of civil law or government regulations. A *civil investigation* is typically triggered when a lawsuit is imminent or ongoing. It is similar to a criminal investigation, except that instead of working with an LEA you will probably be working with attorneys from both sides (the plaintiff is the party suing and the defendant is the one being sued). Another key difference in civil (versus criminal) investigations is that the standard of proof is much lower; instead of proving beyond a reasonable doubt, the plaintiff just has to show that the preponderance of the evidence supports the allegation.

Regulatory

Somewhere between the previous three (administrative, criminal, and civil investigations) lies the fourth kind you should know. A *regulatory investigation* is initiated by a government regulator when there is reason to believe that the organization is not in compliance. These vary significantly in scope and could look like any of the other three types of investigation depending on the severity of the allegations. As with criminal investigations, the key thing to remember is that your job is to preserve evidence and assist the regulator's investigators as appropriate.

Chapter Review

The fact that the Internet is a global medium does not negate the power of governments to establish and enforce laws that govern what can be done by whom on networks within each country. This can create challenges for cybersecurity professionals whose organizations

have clients, partners, or activities in multiple jurisdictions. The most important thing you can do as a CISSP is develop a good relationship with your legal team and use that to ensure you are aware of all the legal and regulatory requirements that may pertain to cybersecurity. Then, after you implement the necessary controls, check with your lawyer friends again to ensure you've exercised due diligence. Keep checking, because laws and regulations do change over time, particularly if you are operating in multiple countries.

Quick Review

- Law is a system of rules (written or otherwise), created by a government, that apply equally to everyone in the country.
- Regulations are written rules issued by an executive body, covering specific issues, and apply only to the specific entities that fall under the authority of the agency that issues them.
- Civil law system:
  - Uses prewritten rules and is not based on precedent.
  - Is different from civil (tort) laws, which work under a common law system.
- Common law system:
  - Made up of criminal, civil, and administrative laws.
- Customary law system:
  - Addresses mainly personal conduct and uses regional traditions and customs as the foundations of the laws.
  - Is usually mixed with another type of listed legal system rather than being the sole legal system used in a region.
- Religious law system:
  - Laws are derived from religious beliefs and address an individual's religious responsibilities; commonly used in Muslim countries or regions.
- Mixed law system:
  - Uses two or more legal systems.
- Criminal law deals with an individual's conduct that violates government laws developed to protect the public.
- Civil law deals with wrongs committed against individuals or organizations that result in injury or damages. Civil law does not use prison time as a punishment, but usually requires financial restitution.
- Administrative, or regulatory, law covers standards of performance or conduct expected by government agencies from companies, industries, and certain officials.
- Many attacks cross international borders, which make them harder to prosecute because doing so requires deconflicting the laws of the various countries involved; attackers use this to their advantage.

- Island-hopping attacks are those in which an attacker compromises an easier target that has a trusted connection to the ultimate target.
- An advanced persistent threat (APT) is a sophisticated threat actor that has the means and the will to devote extraordinary resources to compromising a specific target and remaining undetected for extended periods of time.
- A data breach is a security event that results in the actual or potential compromise of the confidentiality or integrity of protected information by unauthorized actors.
- Personally identifiable information (PII) is data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
- Each country has specific rules that control what can be legally imported and exported. This applies particularly to some cryptographic tools and techniques.
- A transborder data flow (TDF) is the movement of machine-readable data across a political boundary such as a country's border.
- Data localization laws require that certain types of data be stored and processed in that country, sometimes exclusively.
- Intellectual property (IP) is a type of property created by human intellect that consists of ideas, inventions, and expressions that are uniquely created by a person and can be protected from unauthorized use by others.
- A license is an agreement between an intellectual property (IP) owner (the licensor) and somebody else (the licensee), granting that party the right to use the IP in very specific ways.
- Trade secrets are deemed proprietary to a company and often include information that provides a competitive edge. The information is protected as long as the owner takes the necessary protective actions.
- Copyright protects the expression of ideas rather than the ideas themselves.
- Trademarks protect words, names, product shapes, symbols, colors, or a combination of these used to identify products or a company. These items are used to distinguish products from the competitors' products.
- A patent grants ownership and enables that owner to legally enforce his rights to exclude others from using the invention covered by the patent.
- Due diligence can be defined as doing everything within one's power to prevent a bad thing from happening. It is normally associated with leaders, laws, and regulations.
- Due care means taking the precautions that a reasonable and competent person would take in the same situation. It is normally applicable to everyone, and its absence could be used to show negligence.
- Administrative investigations are focused on policy violations.

- Criminal investigations are aimed at determining whether there is cause to believe that someone committed a crime.
- A civil investigation is typically triggered when a lawsuit is imminent or ongoing, and is similar to a criminal investigation, except that instead of working with law enforcement agencies you will probably be working with attorneys from both sides.
- A regulatory investigation is initiated by a government regulator when there is reason to believe that the organization is not in compliance.

Questions

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

1. When can executives be charged with negligence?

A. If they follow the transborder laws

B. If they do not properly report and prosecute attackers

C. If they properly inform users that they may be monitored

D. If they do not practice due care when protecting resources

2. To better deal with computer crime, several legislative bodies have taken what steps in their strategy?

A. Expanded several privacy laws

B. Broadened the definition of property to include data

C. Required corporations to have computer crime insurance

D. Redefined transborder issues

3. Which of the following is true about data breaches?

A. They are exceptionally rare.

B. They always involve personally identifiable information (PII).

C. They may trigger legal or regulatory requirements.

D. The United States has no laws pertaining to data breaches.

Use the following scenario to answer Questions 4–6. Business is good and your company is expanding operations into Europe. Because your company will be dealing with personal information of European Union (EU) citizens, you know that it will be subject to the EU's General Data Protection Regulation (GDPR). You have a mature security program that is certified by the International Organization for Standardization (ISO), so you are confident you can meet any new requirements.

4. Upon learning of your company's plans to expand into Europe, what should be one of the first things you do?
   - **A.** Consult your legal team
   - **B.** Appoint a Data Protection Officer (DPO)
   - **C.** Label data belonging to EU persons
   - **D.** Nothing, because your ISO certification should cover all new requirements
5. You have determined all the new GDPR requirements and estimate that you will need an additional $250,000 to meet them. How can you best justify this investment to your senior business leaders?
   - **A.** It is the right thing to do.
   - **B.** You are legally required to provide that money.
   - **C.** You'll make way more profits than that in the new market.
   - **D.** The cost of noncompliance could easily exceed the additional budget request.
6. Your Security Operations Center (SOC) chief notifies you of a data breach in which your organization's entire customer list may have been compromised. As the data controller, what are your notification requirements?
   - **A.** No later than 72 hours after you contain the breach
   - **B.** Within 30 days of the breach
   - **C.** As soon as possible, but within 60 days of becoming aware of the breach
   - **D.** No later than 72 hours after becoming aware of the breach

Use the following scenario to answer Questions 7–9. Faced with a lawsuit alleging patent infringement, your CEO stands up a working group to look at licensing and intellectual property (IP) issues across the company. The intent is to ensure that the company is doing everything within its power to enforce IP rights, both its own rights and others' rights. The CEO asks you to lead an effort to look internally and externally for any indication that your company is violating the IP rights of others or that your own IP is being used by unauthorized parties.

7. Which term best describes what the CEO is practicing?
   - **A.** Due care
   - **B.** Due diligence
   - **C.** Compliance
   - **D.** Downstream liability

8. You discover that another organization is publishing some of your company's copyrighted blogs on its website as if they were its own. What is your best course of action?

A. Do nothing; the blogs are not particularly valuable, and you have bigger problems

B. Contact the webmasters directly and ask them to take the blogs down

C. Have the legal team send a cease-and-desist order to the offending organization

D. Report your findings to the CEO

9. You discover dozens of workstations running unlicensed productivity software in a virtual network that is isolated from the Internet. Why is this a problem?

A. Users should not be able to install their own applications.

B. It is not a problem as long as the virtual machines are not connected to the Internet.

C. Software piracy can have significant financial and even criminal repercussions.

D. There is no way to register the licenses if the devices cannot access the Internet.

10. Which of the following would you use to control the public distribution, reproduction, display, and adaptation of an original white paper written by your staff?

A. Copyright

B. Trademark

C. Patent

D. Trade secret

11. Many privacy laws dictate which of the following rules?

A. Individuals have a right to remove any data they do not want others to know.

B. Agencies do not need to ensure that the data is accurate.

C. Agencies need to allow all government agencies access to the data.

D. Agencies cannot use collected data for a purpose different from what they collected it for.

12. Which of the following has an incorrect definition mapping?

i. Civil (code) law: Based on previous interpretations of laws

ii. Common law: Rule-based law, not precedent-based

iii. Customary law: Deals mainly with personal conduct and patterns of behavior

iv. Religious law: Based on religious beliefs of the region

A. i, iii

B. i, ii, iii

C. i, ii

D. iv

Answers

1. **D.** Executives are held to a certain standard and are expected to act responsibly when running and protecting an organization. These standards and expectations equate to the due care concept under the law. Due care means to carry out activities that a reasonable person would be expected to carry out in the same situation. If an executive acts irresponsibly in any way, she can be seen as not practicing due care and be held negligent.
2. **B.** Many times, what is corrupted, compromised, or taken from a computer is data, so current laws have been updated to include the protection of intangible assets, as in data. Over the years, data and information have become many organizations' most valuable asset, which must be protected by the laws.
3. **C.** Organizations experiencing a data breach may be required by laws or regulations to take certain actions. For instance, many countries have disclosure requirements that require notification to affected parties and/or regulatory bodies within a specific timeframe.
4. **A.** Your best bet when facing a new legal or regulatory environment or issue is to consult with your legal team. It is their job to tell you what you're required to do, and your job to get it done. Your will almost certainly need to appoint a Data Protection Officer (DPO), and you will probably need to label or otherwise categorize data belonging to EU persons, but you still need to check with your attorneys first.
5. **D.** Fines for noncompliance with the GDPR can range from up to €20 million (approximately $22.5 million) to 4 percent of a company's annual global revenue—whichever is greater. While it is true that this is the right thing to do, that answer is not as compelling to business leaders whose job is to create value for their shareholders.
6. **D.** The GDPR has the strictest breach notification requirements of any data protection law in the world. Your organization is required to notify the supervisory authority of the EU member state involved within 72 hours of becoming aware of the breach. Examples of supervisory authorities are the Data Protection Commission in Ireland, the Hellenic Data Protection Authority in Greece, and the Agencia Española de Protección de Datos in Spain.
7. **B.** Due diligence is doing everything within one's power to prevent a bad thing from happening and is normally associated with an organization's leaders. Given the CEO's intent, this is the best answer. Compliance could be an answer but is not the best one since the scope of the effort appears to be very broad and there is no mention of specific laws or regulations with which the CEO wants to comply.
8. **C.** A company must protect resources that it claims to be intellectual property such as copyrighted material and must show that it exercised due care (reasonable acts of protection) in its efforts to protect those resources. If you

ignore this apparent violation, it may be much more difficult to enforce your rights later when more valuable IP is involved. You should never attempt to do this on your own. That's why you have a legal team!

9. **C.** Whether or not the computers on which unlicensed software runs can reach the Internet is irrelevant. The fact is that your company is using a software product that it is not authorized to use, which is considered software piracy.
10. **A.** A copyright fits the situation precisely. A patent could be used to protect a novel invention described in the paper, but the question did not imply that this was the case. A trade secret cannot be publicly disseminated, so it does not apply. Finally, a trademark protects only a word, symbol, sound, shape, color, or combination of these.
11. **D.** The Federal Privacy Act of 1974 and the General Data Protection Regulation (GDPR) were created to protect personal data. These acts have many stipulations, including that the information can only be used for the reason for which it was collected.
12. **C.** The following has the proper definition mappings:
    - **i.** Civil (code) law: Rule-based law, not precedent-based
    - **ii.** Common law: Based on previous interpretations of laws
    - **iii.** Customary law: Deals mainly with personal conduct and patterns of behavior
    - **iv.** Religious law: Based on religious beliefs of the region

This page intentionally left blank

CHAPTER 4

Frameworks

This chapter presents the following:

- Overview of frameworks
- Risk frameworks
- Information security frameworks
- Enterprise architecture frameworks
- Other frameworks

You can't build a great building on a weak foundation.

—Gordon B. Hinckley

The previous chapters have covered a lot of material dealing with governance, risk, and compliance. By now, you may be asking yourself, "How does this all fit together into an actionable process?" This is where frameworks come to the rescue. You can think of a framework as a strong foundation on which to build whatever it is you're trying to build, whether it's a risk management program or security controls. A framework gives you just enough rigidity to keep your effort from collapsing under its own weight, but still gives you a lot of leeway so that you can customize the framework to your particular situation. While it is possible (though very difficult) to build successful programs all by yourself, why reinvent the wheel when you can leverage the hard-earned lessons of other experts in the field?

In this chapter, we will discuss a variety of frameworks that you are likely to encounter both in your job and when taking the CISSP exam. We divide them into three groups: risk frameworks, information security frameworks, and enterprise architecture frameworks. Risk management enables any successful information security program, so we'll tackle those two groups in that order, followed by enterprise architecture frameworks. We'll then round out our discussion with the other frameworks and concepts that you should know.

Overview of Frameworks

A *framework* is a basic structure underlying a system, concept, or text. So the purpose of frameworks in IT and cybersecurity is to provide structure to the ways in which we manage risks, develop enterprise architectures, and secure all our assets. Think of frameworks as the consensus of many great minds on how we should approach these issues.

As you will see in the following sections, various for-profit and nonprofit organizations have developed their own frameworks for risk management, security programs, security controls, process management, and enterprise development. We will examine their similarities and differences and illustrate where each is used within the industry. The following is a basic breakdown.

Risk:

- **NIST RMF** The Risk Management Framework, developed by the National Institute of Standards and Technology, is composed of three interrelated NIST Special Publications (SPs): 800-39, 800-37, and 800-30.
- **ISO/IEC 27005** Focused on risk treatment, this joint International Organization for Standardization/International Electrotechnical Commission framework is best used in conjunction with ISO/IEC 27000 series standards.
- **OCTAVE** The Operationally Critical Threat, Asset, and Vulnerability Evaluation framework, developed at Carnegie Mellon University, is focused on risk assessment.
- **FAIR** The FAIR Institute's Factor Analysis of Information Risk framework focuses on more precisely measuring the probabilities of incidents and their impacts.

Security Program:

- **ISO/IEC 27000 series** This is a series of international standards on how to develop and maintain an information security management system (ISMS), developed by ISO and IEC.
- **NIST Cybersecurity Framework** Driven by the need to secure government systems, NIST developed this widely used and comprehensive framework for risk-driven information security.

Security Controls:

- **NIST SP 800-53** This NIST publication provides a catalog of controls and a process for selecting them in order to protect U.S. federal systems.
- **CIS Controls** The Center for Internet Security (CIS) Controls framework is one of the simplest approaches for companies of all sizes to select and implement the right controls.
- **COBIT 2019** This is a business framework to allow for IT enterprise management and governance that was developed by ISACA.

Enterprise Architecture:

- **Zachman Framework** This is a model for the development of enterprise architectures, developed by John Zachman.
- **TOGAF** The Open Group Architecture Framework is a model and methodology for the development of enterprise architectures.

- **DoDAF** The U.S. Department of Defense Architecture Framework was developed to ensure interoperability of systems to meet military mission goals.
- **SABSA** The Sherwood Applied Business Security Architecture model and methodology for the development of information security enterprise architectures was developed by the SABSA Institute.

NOTE Chapter 1 already discussed the SABSA model.

Risk Frameworks

By combining the definition of a framework in the previous section with our definition of risk management in Chapter 2, we can define a *risk management framework (RMF)* as a structured process that allows an organization to identify and assess risk, reduce it to an acceptable level, and ensure that it remains at that level. In essence, an RMF is a structured approach to risk management.

As you might imagine, there is no shortage of RMFs out there. What is important to you as a security professional is to ensure your organization has an RMF that works for you. That being said, there are some frameworks that have enjoyed widespread success and acceptance. You should at least be aware of these, and ideally adopt (and perhaps modify) one of them to fit your organization's particular needs. We'll cover the NIST RMF in more detail, mostly to familiarize you with the components of this framework, but also because it is the one you are most likely to encounter in your career.

NIST RMF

The NIST Risk Management Framework (RMF) is described in three core interrelated Special Publications (there are other key publications specific to individual steps of the RMF):

- SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*
- SP 800-39, *Managing Information Security Risk*
- SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*

This framework incorporates the key elements of risk management that you should know as a security professional. It is important to keep in mind, however, that it is geared toward federal government entities and may have to be modified to fit your own needs.

The NIST RMF outlines the seven-step process shown in Figure 4-1, each of which will be addressed in turn in the following sections. It is important to note that this is a never-ending cycle because our information systems are constantly changing. Each change needs to be analyzed to determine whether it should trigger another trip around the loop.

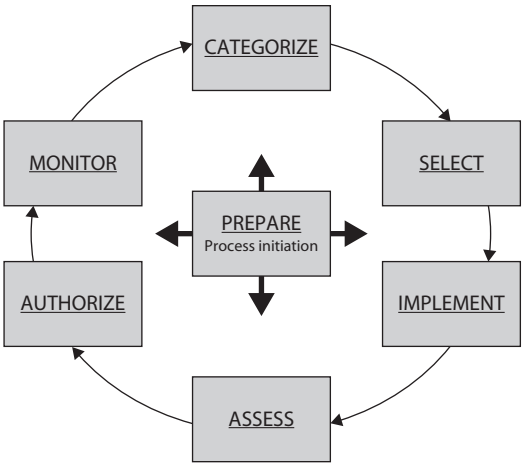

Figure 4-1 The NIST Risk Management Framework process

Prepare

The first step is to ensure that the top executives and the senior leaders (at both the strategic and operational levels) are in sync across the organization. This includes agreeing on roles, priorities, constraints, and risk tolerance. Another key activity during the prepare step is to conduct an organizational risk assessment that provides a common point of reference for the entire team to communicate about strategic risks. One of the outcomes of this assessment is the identification of high-value assets, on which the entire effort will be focused.

Categorize

The next step is to categorize your information systems based on criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. The idea is to create categories for your systems based on how important they are so that you can prioritize your defensive resources. All U.S. government agencies are required to use the following NIST SP 800-60 documents for this purpose: *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* and *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*.

NIST SP 800-60 applies sensitivity and criticality to each security objective (confidentiality, integrity, and availability) to determine a system's criticality. For example, suppose you have a customer relationship management (CRM) system. If its confidentiality were to be compromised, this would cause significant harm to your company, particularly if the information fell into the hands of your competitors. The system's integrity and availability, on the other hand, would probably not be as critical to your business, so they would be classified as relatively low. The format for describing the security category (SC) of this CRM would be as follows:

$$SC_{CRM} = \{(\textbf{confidentiality}, \textit{high}),(\textbf{integrity}, \textit{low}),(\textbf{availability}, \textit{low})\}$$

SP 800-60 uses three SCs: low impact, moderate impact, and high impact. A low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is one in which at least one of the security

objectives is moderate and no security objective is greater than moderate. Finally, a high-impact system is an information system in which at least one security objective is high. This method of categorization is referred to as the "high water mark" because it uses the highest security objective category to determine the overall category of the system. In our example, the SC of the CRM system would be high because at least one objective (confidentiality) is rated high.

Select

Once you have categorized your systems, it is time to select, and quite possibly tailor, the controls you will use to protect them. The NIST RMF defines three types of security controls: common, system-specific, and hybrid. A *common control* is one that applies to multiple systems and exists outside of their individual boundaries. Following our CRM example, if you placed a web application firewall (WAF) in front of the CRM (and in front of all your other web applications), that would be an example of a common control. The WAF is outside the system boundary of the CRM and protects it and other systems.

System-specific controls, on the other hand, are implemented within the system boundary and, obviously, protect only that specific system. The system owner, and not the broader organization, is responsible for these. An example would be a login page on the CRM that forces the use of Transport Layer Security (TLS) to encrypt the user credentials. If the authentication subsystem was an integral part of the CRM, then this would be an example of an application-specific control.

Wouldn't it be wonderful if everything was black or white, true or false? Alas, the real world is much messier than that. Oftentimes, controls blur the line between common and system-specific and become something else. A *hybrid control*, according to the NIST RMF, is one that is partly common and partly system-specific. Continuing our CRM example, a hybrid control could be security awareness training. There would be a common aspect to the training (e.g., don't share your password) but also some system-specific content (e.g., don't save your customers' information and e-mail it to your personal account so that you can reach out to them while you're on vacation).

The specific controls required to mitigate risks to acceptable levels are documented in the NIST control catalog, NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. We'll discuss this publication later in this chapter, but for now it is worth noting that it provides a mapping between the impact categories we assigned to information systems in the categorize step of this RMF and specific controls that mitigate risks to those systems.

Implement

There are two key tasks in this step: implementation and documentation. The first part is very straightforward. For example, if you determined in the previous step that you need to add a rule to your WAF to filter out attacks like Structured Query Language (SQL) injection, you implement that rule. Simple. The part with which many of us struggle is the documentation of this change.

The documentation is important for two obvious reasons. First, it allows everyone to understand what controls exist, where, and why. Have you ever inherited a system that is configured in a seemingly nonsensical way? You try to understand why certain parameters

or rules exist but hesitate to change them because the system might fail. Likely, this was the result of either improper documentation or (even worse) a successful attack. The second reason why documentation is important is that it allows us to fully integrate the controls into the overall assessment and monitoring plan. Failing to do this invites having controls that quietly become obsolete and ineffective over time and result in undocumented risks.

Assess

The security controls we implement are useful to our overall risk management effort only insofar as we can assess them. It is absolutely essential to our organizations to have a comprehensive plan that assesses all security controls (common, hybrid, and system-specific) with regard to the risks they are meant to address. This plan must be reviewed and approved by the appropriate official(s), and it must be exercised.

To execute an assessment plan, you will, ideally, identify an assessor who is both competent and independent from the team that implemented the controls. This person must act as an honest broker that not only assesses the effectiveness of the controls but also ensures the documentation is appropriate for the task. For this reason, it is important to include all necessary assessment materials in the plan.

The assessment determines whether or not the controls are effective. If they are, then the results are documented in the report so that they are available as references for the next assessment. If the controls are not effective, then the report documents the results, the remediation actions that were taken to address the shortcomings, and the outcome of the reassessment. Finally, the appropriate security plans are updated to include the findings and recommendations of the assessment.

NOTE An assessment of security controls is also called an audit. We discuss audits in detail in Chapter 18.

Authorize

As we already discussed, no system is ever 100 percent risk-free. At this stage in the RMF, we present the results of both our risk and controls assessments to the appropriate decision-maker in order to get approval to connect our information system into our broader architecture and operate it. This person (or group) is legally responsible and accountable for the system while it is operating, and therefore must make a true risk-based decision to allow the system to operate. This person determines whether the risk exposure is acceptable to the organization. This normally requires a review of a plan of action that addresses how and when the organization will deal with the remaining weaknesses and deficiencies in the information system. In many organizations this authorization is given for a set period of time, which is usually specified in a plan of action and milestones (POAM or POA&M).

Monitor

These milestones we just mentioned are a key component of the monitoring or continuous improvement stage of the RMF. At a minimum, we must periodically look at all our controls and determine whether they are still effective. Has the threat changed its tactics, techniques, and procedures (TTPs)? Have new vulnerabilities been discovered? Has an

undocumented or unapproved change to our configuration altered our risk equations? These are only some of the issues that we address through ongoing monitoring and continuous improvement.

ISO/IEC 27005

ISO/IEC 27005, updated in 2018, is another widely used information security risk management framework. Similar to the NIST RMF we just discussed, ISO/IEC 27005 provides guidelines for information security risk management in an organization but does not dictate a specific approach for implementing it. In other words, the framework tells us what sorts of things we ought to do, but not how to do them. Similarly to how the NIST RMF can be paired with the security controls in NIST SP 800-53, ISO/IEC 27005 is best used in conjunction with ISO/IEC 27001, which, as we'll see shortly, provides a lot more structure to information security program development.

The risk management process defined by ISO/IEC 27005 is illustrated in Figure 4-2. It all starts with establishing the context in which the risks exist. This is similar to the

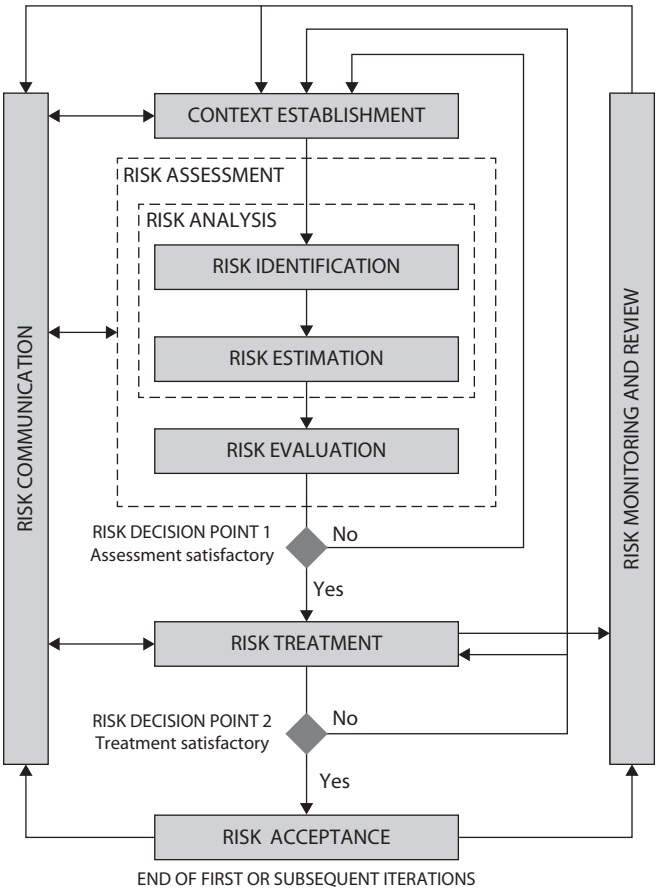

Figure 4-2 ISO/IEC 27005 risk management process

business impact analysis (BIA) we discussed in Chapter 2, but it adds new elements, such as evaluation criteria for risks as well as the organizational risk appetite. The risk assessment box in the middle of the figure should look familiar, since we also discussed this process (albeit with slightly different terms) in Chapter 2.

The risk treatment step is similar to the NIST RMF steps of selecting and implementing controls but is broader in scope. Rather than focusing on controls to mitigate the risks, ISO/IEC 27005 outlines four ways in which the risk can be treated:

- **Mitigate** the risk by implementing controls that bring it to acceptable levels.
- **Accept** the risk and hope it doesn't realize, which assumes that the impact of this risk is less than the cost of treating it.
- **Transfer** the risk to another entity such as an insurance company or a business partner.
- **Avoid** the risk by not implementing the information system that brings it, or by changing business practices so the risk is no longer present or is reduced to acceptable levels.

NOTE The NIST RMF also briefly touches on these treatments in the authorize step of its process.

Risk acceptance in ISO/IEC 27005 is very similar to the authorize step in the NIST RMF, and the risk monitoring steps in both are very similar. A notable difference between these two RMFs, on the other hand, is that ISO/IEC 27005 explicitly identifies risk communication as an important process. This is an essential component of any risk management methodology, since we cannot enlist the help of senior executives, partners, or other stakeholders if we cannot effectively convey our message to a variety of audiences. Just because this communication is not explicitly called out in the NIST RMF or any other RMF, however, doesn't decrease its importance.

As you can see, this framework doesn't really introduce anything new to the risk conversation we've been having over the last two chapters; it just rearranges things a bit. Of course, despite these high-level similarities, the two risk-based frameworks we've discussed differ in how they are implemented. For best results, you should combine ISO/IEC 27005 risk management with an ISO/IEC 27001 security program.

OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is not really a framework per se. Rather, it is a methodology for risk assessments developed at Carnegie Mellon University. So, while it falls short of a framework, it is fairly commonly used in the private sector. As a cybersecurity professional, you really should be aware of it and know when it might come in handy.

OCTAVE is self-directed, meaning that it uses a small team of representatives of IT and the business sides of the organization to conduct the analysis. This promotes

collaboration on identifying risks and facilitates communication with business leaders on those risks. It also follows the approach of focusing on the most critical assets in risk analysis to prioritize areas of attention. OCTAVE follows the 80/20 Pareto principle, which states that 80 percent of the consequences come from 20 percent of the causes. This highlights one of the key benefits of this methodology, which is its focus on speed based on the fact that, for most businesses, time is money.

This risk assessment methodology is divided into three phases. The first is an organizational view, in which the analysis team defines threat profiles based on assets that are critical to the business. The second phase then looks at the organization's technology infrastructure to identify vulnerabilities that might be exploited by those threats. Finally, in the third phase, the team analyses and classifies individual risks as high, medium, or low and then develops mitigation strategies for each. This classification scheme belies one of the advantages or drawbacks (depending on your perspective) of OCTAVE: it is fundamentally a qualitative approach to assessing risks.

FAIR

If you want to apply a more rigorous, quantitative approach to managing risk, you may want to read up on the Factor Analysis of Information Risk (FAIR), which is a proprietary framework for understanding, analyzing, and measuring information risk. In fact, if you want a quantitative approach, this is pretty much the only international standard framework you can use. Recall that a quantitative approach is one in which risks are reduced to numbers (typically monetary quantities), while a qualitative approach uses categories of risks such as low, medium, and high.

The main premise of FAIR is that we should focus not on possible threats but on probable threats. Thus, its quantitative nature makes a lot of sense. In this framework, risk is defined as the "probable frequency and probable magnitude of future loss," where loss can be quantified as lost productivity, costs of replacement or response, fines, or competitive advantage. Note that each of these can be reduced (perhaps with a bit of work) to monetary quantities. If this approach appeals to you, consider it in conjunction with the discussion of quantitative risk assessment in Chapter 2.

Information Security Frameworks

Armed with the knowledge gained from the risk management frameworks, we are now ready to properly secure our information systems. After all, our main goal is to develop cost-effective defenses that enable our organizations to thrive despite the risks they face. For this reason, most information security frameworks have an explicit tie-in to risk management.

Broadly speaking, information security frameworks can be divided into two categories: those that look holistically at the entire security program, and those that are focused on controls. These are not mutually exclusive, by the way. As we will see, the NIST Cybersecurity Framework is compatible with the NIST SP 800-53 controls. Nor do information security frameworks have to be implemented in a wholesale manner. This is, after all, the beauty of frameworks: we get to pick and choose the parts that make the most sense to us and then tailor those to our specific organizational needs.

Security Program Frameworks

Let's start at the top. A security program is made up of many components: logical, administrative, and physical protection mechanisms (i.e., controls); procedures; business processes; and people. These components all work together to provide a protection level for an environment. Each has an important place in the framework, and if one is missing or incomplete, the whole framework may be affected. The program should work in layers: each layer provides support for the layer above it and protection for the layer below it. Because a security program is a framework, organizations are free to plug in different types of technologies, methods, and procedures to accomplish the necessary protection level for their environment.

A security program based upon a flexible framework sounds great, but how do we build one? Before a fortress is built, the structure is laid out in blueprints by an architect. We need a detailed plan to follow to properly build our security program. Thank goodness industry standards have been developed just for this purpose. Let's take a closer look at two of the most popular information security program frameworks: the ISO/IEC 27000 series and the NIST Cybersecurity Framework.

ISO/IEC 27000 Series

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27000 series serves as industry best practices for the management of security controls in a holistic manner within organizations around the world. The list of standards that makes up this series grows each year. Collectively, these standards describe an information security management system (ISMS), but each standard has a specific focus (such as metrics, governance, auditing, and so on). The currently published ISO/IEC 27000 series of standards (with a bunch of them omitted) include the following:

- **ISO/IEC 27000** Overview and vocabulary
- **ISO/IEC 27001** ISMS requirements
- **ISO/IEC 27002** Code of practice for information security controls
- **ISO/IEC 27003** ISMS implementation guidance
- **ISO/IEC 27004** ISMS monitoring, measurement, analysis, and evaluation
- **ISO/IEC 27005** Information security risk management
- **ISO/IEC 27007** ISMS auditing guidelines
- **ISO/IEC 27014** Information security governance
- **ISO/IEC 27017** Security controls for cloud services
- **ISO/IEC 27019** Security for process control in the energy industry
- **ISO/IEC 27031** Business continuity
- **ISO/IEC 27033** Network security
- **ISO/IEC 27034** Application security
- **ISO/IEC 27035** Incident management

- **ISO/IEC 27037** Digital evidence collection and preservation
- **ISO/IEC 27050** Electronic discovery
- **ISO/IEC 27799** Health organizations

It is common for organizations to seek an ISO/IEC 27001 certification by an accredited third party. The third party assesses the organization against the ISMS requirements laid out in ISO/IEC 27001 and attests to the organization's compliance level. Just as $(ISC)^2$ attests to information security professionals' knowledge once they pass the CISSP exam, the third party attests to the security practices within the boundaries of the organization it evaluates.

It is useful to understand the differences between the ISO/IEC 27000 series of standards and how they relate to each other. Figure 4-3 illustrates the differences between general requirements, general guidelines, and sector-specific guidelines.

EXAM TIP You don't have to memorize the entire ISO/IEC 27000 series of standards. You just need to be aware of them.

As you probably realize, ISO 27001 is the most important of these standards for most organizations. It is not enough to simply purchase the document and implement it in your environment; you actually need an external party (called a Certification Body) to audit you and certify that you are in compliance with the standard. This ISO 27001 certification is useful to demonstrate to your customers and partners that you are not a security risk to them, which in some cases can be a contractual obligation. Additionally,

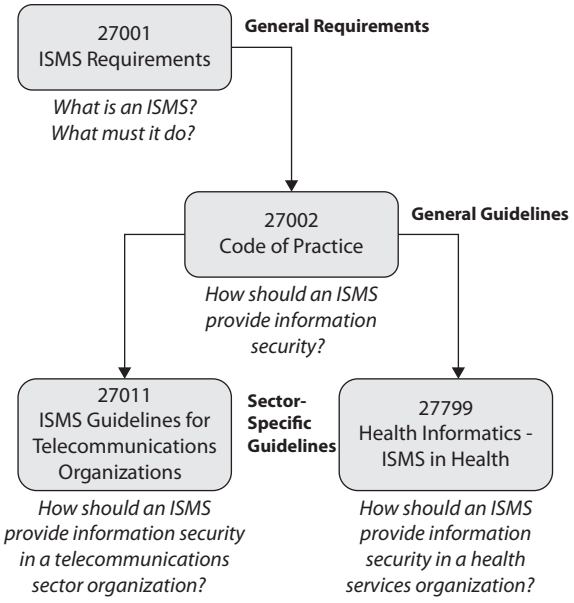

Figure 4-3 How ISO/IEC 27000 standards relate to each other

this certification can help avoid regulatory fines by proving that the organization practices due diligence in protecting its information systems. The certification process can take a year or longer (depending on how mature your security program is), but for many medium and large business, it is worth the investment.

NIST Cybersecurity Framework

On February 12, 2013, U.S. President Barack Obama signed Executive Order 13636, calling for the development of a voluntary cybersecurity framework for organizations that are part of the critical infrastructure. The goal of this construct was for it to be flexible, repeatable, and cost-effective so that it could be prioritized for better alignment with business processes and goals. A year to the day later, NIST published the "Framework for Improving Critical Infrastructure Cybersecurity," commonly called the Cybersecurity Framework, which was the result of a collaborative process with members of the government, industry, and academia. The Cybersecurity Framework is divided into three main components:

- **Framework Core** Consists of the various activities, outcomes, and references common to all organizations. These are broken down into five functions, 22 categories, and 98 subcategories.
- **Implementation Tiers** Categorize the degree of rigor and sophistication of cybersecurity practices, which can be Partial (tier 1), Risk Informed (tier 2), Repeatable (tier 3), or Adaptive (tier 4). The goal is not to force an organization to move to a higher tier, but rather to inform its decisions so that it can do so if it makes business sense.
- **Framework Profile** Describes the state of an organization with regard to the Cybersecurity Framework categories and subcategories. A Framework Profile enables decision-makers to compare the "as-is" situation to one or more "to-be" possibilities, so that they can align cybersecurity and business priorities and processes in ways that make sense to that particular organization. An organization's Framework Profile is tailorable based on the requirements of the industry segment within which it operates and the organization's needs.

The Framework Core practices organize cybersecurity activities into five higher-level functions with which you should be familiar. Everything we do can be aligned with one of these:

- **Identify** Understand your organization's business context, resources, and risks.
- **Protect** Develop appropriate controls to mitigate risk in ways that make sense.
- **Detect** Discover in a timely manner anything that threatens your security.
- **Respond** Quickly contain the effects of anything that threatens your security.
- **Recover** Return to a secure state that enables business activities after an incident.

EXAM TIP For the exam, you should remember the five functions of the NIST Cybersecurity Framework and the fact that it is voluntary.

Security Control Frameworks

Up to now we have reviewed the ISO/IEC 27000 series and the NIST CSF, both of which outline the necessary components of an organizational security program. Now we are going to get more focused and look at the objectives of the controls we are going to put into place to accomplish the goals outlined in our security program and enterprise architecture. This is where security control frameworks come in handy. This section presents three popular frameworks: NIST SP 800-53, CIS Controls, and COBIT.

NIST SP 800-53

One of the standards that NIST has been responsible for developing is SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, currently in its fifth revision (Rev. 5). It outlines controls that agencies need to put into place to be compliant with the Federal Information Processing Standards (FIPS). It is worth noting that, although this publication is aimed at federal government organizations, many other organizations have voluntarily adopted it to help them better secure their systems.

Basically, SP 800-53 provides specific guidance on how to select security controls. It prescribes a four-step process for applying controls:

1. Select the appropriate security control baselines.
2. Tailor the baselines.
3. Document the security control selection process.
4. Apply the controls.

The first step assumes that you have already determined the security categories (SCs) of your information systems based on criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. SP 800-53 uses three SCs: low impact, moderate impact, and high impact. If this sounds familiar, that's because we discussed this categorization earlier in this chapter when we covered the NIST RMF and SP 800-60.

This exercise in categorizing your information systems is important because it enables you to prioritize your work. It also determines which of the more than 1,000 controls listed in SP 800-53 you need to apply to it. These controls are broken down into 20 families. Table 4-1 outlines the control categories that are addressed in SP 800-53, Rev. 5.

Let's circle back to the example of the customer relationship management system we used when discussing the NIST RMF. Recall that we determined that the CRM's SC was high because the impact of a loss of confidentiality was high. We can go through the entire catalog of controls and see which of them apply to this hypothetical CRM. In the

ID	Family	ID	Family
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Table 4-1 NIST SP 800-53 Control Categories

interest of brevity, we will only look at the first three controls (IR-1, IR-2, and IR-3) in the Incident Response, or IR family. You can see in Table 4-2 how these controls apply to the different SCs. Since the CRM is SC high, all three controls are required for it. You can also see that IR-2 and IR-3 have control enhancements listed.

Let's dive into the first control and see how we would use it. Chapter 3 of SP 800-53 is a catalog that describes in detail what each security control is. If we go to the description

Control No.	Control Name *CONTROL ENHANCEMENT NAME*	Control Baselines Low	 Mod.	 High
IR-1	Policy and Procedures	X	X	X
IR-2	Incident Response Training	X	X	X
IR-2(1)	*Simulated Events*			X
IR-2(2)	*Automated Training Environments*			X
IR-2(3)	*Breach*			
IR-3	Incident Response Testing		X	X
IR-3(1)	*Automated Testing*			
IR-3(2)	*Coordination with Related Plans*		X	X

Table 4-2 Sample Mapping of Security Controls to the Three Security Categories in SP 800-53

of the baseline IR-1 (Incident Response Policy and Procedures) control, we see that it requires that the organization do the following:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] incident response policy that:

(a.) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b.) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Notice that there are assignments in square brackets in five of these requirements. These are parameters that enable an organization to tailor the baseline controls to its own unique conditions and needs. For example, in the first assignment (IR-1.a), we could specify who receives the policies and procedures; in the second (IR-1.a.1), we could specify the level(s) at which the incident response policy applies; in the third (IR-1.b), we could identify the individual (by role, not name) responsible for the policy; and in the last two assignments (IR-1.c.1 and IR-1.c.2), we could provide the frequency and triggering events for policy and procedure reviews. This is all a "fill in the blanks" approach to tailoring the controls to meet your organization's unique conditions.

EXAM TIP You do not need to memorize the controls, control enhancements, or assignments of NIST SP 800-53. We provide them here to illustrate how a framework provides structure while still allowing you room to customize it.

CIS Controls

The Center for Internet Security (CIS) is a nonprofit organization that, among other things, maintains a list of 20 critical security controls designed to mitigate the threat of the majority of common cyberattacks. It is another example (together with NIST SP 800-53) of a controls framework. The CIS Controls, currently in Version 7.1, are shown in Figure 4-4.

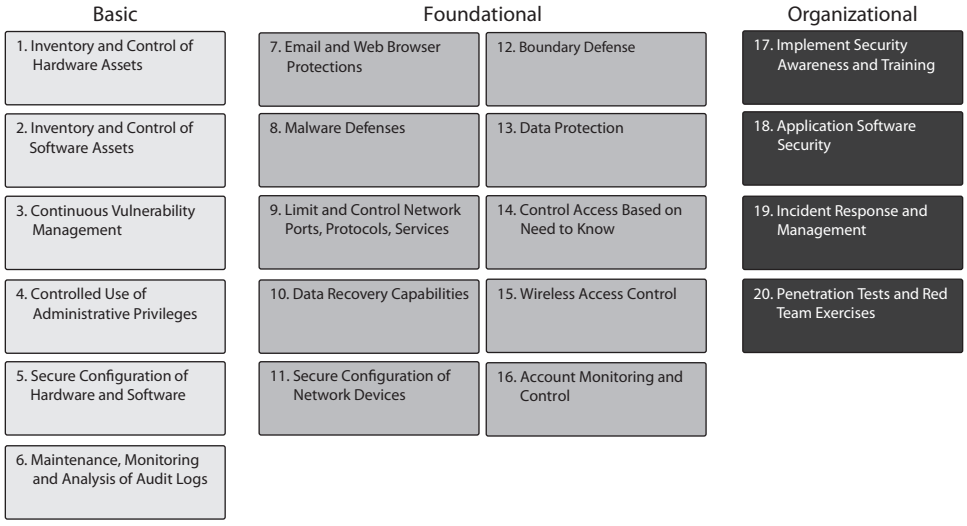

Figure 4-4 CIS Controls

Despite CIS's use of the word "controls," you should really think of these like the 20 families of controls in SP 800-53. Under these 20 controls, there are a total of 171 subcontrols that have similar granularity as those established by the NIST. For example, if we look into control 13 (Data Protection), we can see the nine subcontrols listed in Table 4-3.

Subcontrol	Title	IG1	IG2	IG3
13.1	Maintain an Inventory of Sensitive Information	X	X	X
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	X	X	X
13.3	Monitor and Block Unauthorized Network Traffic			X
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers		X	X
13.5	Monitor and Detect Any Unauthorized Use of Encryption			X
13.6	Encrypt Mobile Device Data	X	X	X
13.7	Manage USB Devices		X	X
13.8	Manage System's External Removable Media's Read/Write Configurations			X
13.9	Encrypt Data on USB Storage Devices			X

Table 4-3 Data Protection Subcontrols Mapped to Implementation Groups

The CIS recognizes that not every organization will have the resources (or face the risks) necessary to implement all controls. For this reason, they are grouped into three categories, listed next. While every organization should strive for full implementation, this approach provides a way to address the most urgent requirements first and then build on them over time.

- **Basic** These key controls should be implemented by every organization to achieve minimum essential security.
- **Foundational** These controls embody technical best practices to improve an organization's security.
- **Organizational** These controls focus on people and processes to maintain and improve cybersecurity.

A useful tool to help organizations match their implementation of controls to their resource levels are implementation groups (IGs). Version 7.1 of the CIS controls describes the following three IGs:

- **Implementation Group 1** Small to medium-sized organizations with limited IT and cybersecurity expertise whose principal concern is to keep the business operational. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.
- **Implementation Group 2** Larger organizations with multiple departments, including one responsible for managing and protecting IT infrastructure. Small organizational units. These organizations often store and process sensitive client or company information and may have regulatory compliance burdens. A major concern is loss of public confidence if a breach occurs.
- **Implementation Group 3** Large organizations that employ security experts with different specialty areas. Their systems and data contain sensitive information or functions that are subject to regulatory and compliance oversight. Successful attacks against these organizations can cause significant harm to the public welfare.

You can see in Table 4-3 how subcontrols can be mapped to these implementation groups. This helps ensure that limited resources are focused on the most critical requirements.

COBIT 2019

COBIT 2019 (the name used to be an acronym for Control Objectives for Information Technologies) is a framework for governance and management developed by ISACA (which formerly stood for the Information Systems Audit and Control Association) and the IT Governance Institute (ITGI). It helps organizations optimize the value of their IT by balancing resource utilization, risk levels, and realization of benefits. This is all done by explicitly tying stakeholder drivers to stakeholder needs to organizational goals (to meet those needs) to IT goals (to meet or support the organizational goals). It is a holistic approach based on six key principles of governance systems:

1. Provide stakeholder value
2. Holistic approach

3. Dynamic governance system
4. Governance distinct from management
5. Tailored to enterprise needs
6. End-to-end governance system

Everything in COBIT is ultimately linked to the stakeholders through a series of transforms called cascading goals. The concept is pretty simple. At any point in our IT governance or management processes, we should be able to ask the question "why are we doing this?" and be led to an IT goal that is tied to an enterprise goal, which is in turn tied to a stakeholder need. COBIT specifies 13 enterprise and 13 alignment goals that take the guesswork out of ensuring we consider all dimensions in our decision-making processes.

These two sets of 13 goals are different but related. They ensure that we are aligned with the sixth principle of covering the enterprise end to end by explicitly tying enterprise and IT goals in both the governance and management dimensions, which is the fourth principle. These goals were identified by looking for commonalities (or perhaps universal features) of a large set of organizations. The purpose of this analysis is to enable a holistic approach, which is the second key principle in COBIT.

The COBIT framework includes, but differentiates, enterprise governance and management. The difference between these two is that governance is a set of higher-level processes aimed at balancing the stakeholder value proposition, while management is the set of activities that achieve enterprise objectives. As a simplifying approximation, you can think of governance as the things that the C-suite leaders do and management as the things that the other organizational leaders do. Figure 4-5 illustrates how the

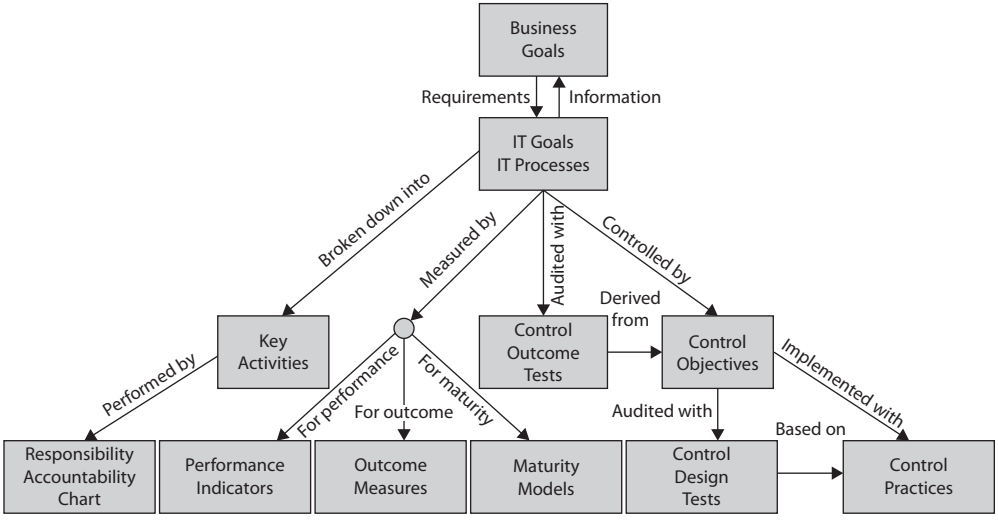

Figure 4-5 COBIT framework

five governance and 35 management objectives defined by COBIT are organized into five domains. Governance objectives all fall within the Evaluate, Direct and Monitor (EDM) domain. Management objectives, on the other hand, fall into four domains: Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Monitor, Evaluate and Assess (MEA).

A majority of the security compliance auditing practices used today in the industry are based off of COBIT. So if you want to make your auditors happy and pass your compliance evaluations, you should learn, practice, and implement the control objectives outlined in COBIT, which are considered industry best practices.

TIP Many people in the security industry mistakenly assume that COBIT is purely security focused, when in reality it deals with all aspects of information technology, security being only one component. COBIT is a set of practices that can be followed to carry out IT governance, which requires proper security practices.

Enterprise Architecture Frameworks

Organizations have a choice when attempting to secure their environment as a whole. They can just toss in products here and there, which are referred to as point solutions or stovepipe solutions, and hope the ad hoc approach magically works in a manner that secures the environment evenly and covers all of the organization's vulnerabilities. Most organizations, particularly small and medium businesses, don't start with a secure architecture. Instead, they focus on their core business, get just enough security to survive, and adjust things as they grow. This organic growth model lends itself to short-term measures that result in a "constantly putting out fires" approach. It is usually easier and cheaper for senior management to approve money for a new security tool than to approve the time, money, and business disruption needed to re-architect an information system to properly secure it.

The second approach to securing an organization's environment would be to define an enterprise security architecture, allow it to be the guide when implementing solutions to ensure business needs are met, provide standard protection across the environment, and reduce the number of security surprises the organization will run into. The catch is that if a company has been following the first ad hoc approach for a while, it can be very challenging (and expensive) to rebuild its infrastructure without causing pain to a lot of people. Although implementing an enterprise security architecture does not necessarily promise pure utopia, it does tame the chaos and gets the security staff and organization into a more proactive and mature mindset when dealing with security as a whole.

Developing an architecture from scratch is not an easy task. Sure, it is easy to draw a big box with smaller boxes inside of it, but what do the boxes represent? What are the relationships between the boxes? How does information flow between the boxes? Who needs to view these boxes, and what aspects of the boxes do they need for decision making? An architecture is a conceptual construct. It is a tool to help individuals understand a complex item (such as an enterprise) in digestible chunks. An example of an architecture

is the Open Systems Interconnection (OSI) networking model, an abstract model used to illustrate the architecture of a networking stack. A networking stack within a computer is very complex because it has so many protocols, interfaces, services, and hardware specifications. But when we think about it in a modular framework (the OSI seven layers), we can better understand the network stack as a whole and the relationships between the individual components that make it up.

NOTE The OSI network stack will be covered extensively in Chapter 11.

An *enterprise architecture* encompasses the essential and unifying components of an organization. It expresses the enterprise structure (form) and behavior (function). It embodies the enterprise's components, their relationships to each other, and their relationships to the environment.

This section covers several different enterprise architecture frameworks. Each framework has its own specific focus, but they all provide guidance on how to build individual architectures so that they are useful tools to a diverse set of individuals. Notice the difference between an architecture *framework* and an actual architecture. You use the framework as a guideline on how to build an architecture that best fits your company's needs. Each company's architecture will be different because companies have different business drivers, security and regulatory requirements, cultures, and organizational structures—but if each starts with the same architecture *framework*, then their architectures will have similar structures and goals. It is similar to three people starting with a ranch-style house blueprint. One person chooses to have four bedrooms built because they have three children, one person chooses to have a larger living room and three bedrooms, and the other person chooses two bedrooms and two living rooms. Each person started with the same blueprint (framework) and modified it to meet their needs (architecture).

When developing an architecture, first the *stakeholders* need to be identified, the people who will be looking at and using the architecture. Next, the *views* need to be developed, which is how the information that is most important to the different stakeholders will be illustrated in the most useful manner. The NIST developed a framework, illustrated in Figure 4-6, that shows that companies have several different viewpoints. Executives need to understand the company from a business point of view, business process developers need to understand what type of information needs to be collected to support business activities, application developers need to understand system requirements that maintain and process the information, data modelers need to know how to structure data elements, and the technology group needs to understand the network components required to support the layers above it. They are all looking at an architecture of the same company; it is just being presented in views that they understand and that directly relate to their responsibilities within the organization.

An enterprise architecture enables you to not only understand the company from several different views, but also understand how a change that takes place at one level will affect items at other levels. For example, if there is a new business requirement, how is it going to be supported at each level of the enterprise? What type of new information must

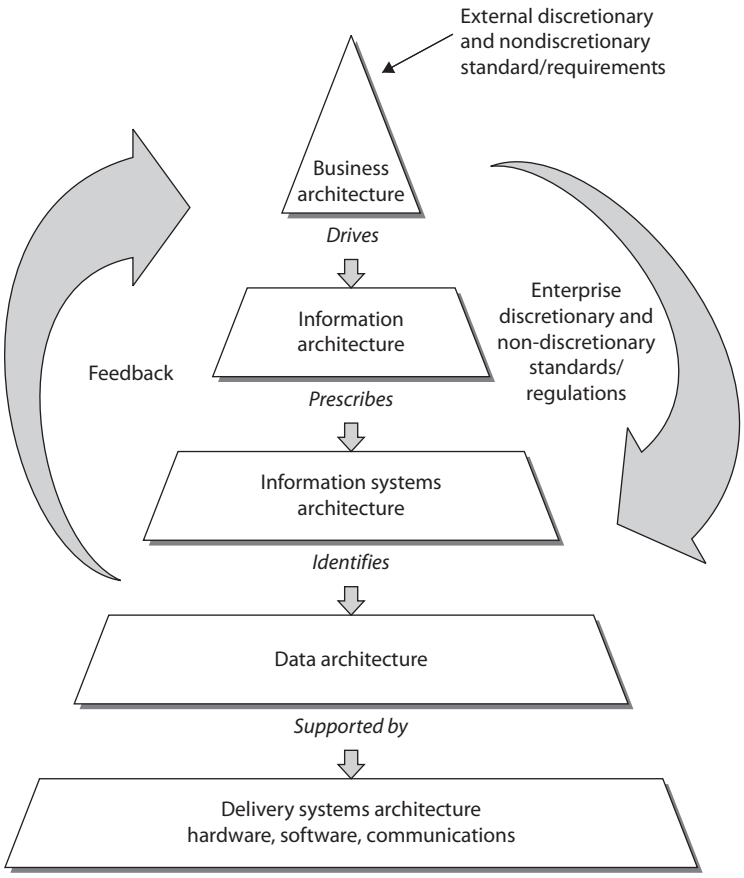

Figure 4-6
NIST enterprise architecture framework

be collected and processed? Do new applications need to be purchased or current ones modified? Are new data elements required? Will new networking devices be required? An architecture enables you to understand all the things that will need to change just to support one new business function.

The architecture can be used in the opposite direction also. If a company is looking to do a technology refresh, will the new systems still support all of the necessary functions in the layers above the technology level? An architecture enables you to understand an organization as one complete organism and identify how changes to one internal component can directly affect another one.

Why Do We Need Enterprise Architecture Frameworks?

As you have probably experienced, business people and technology people sometimes seem like totally different species. Business people use terms like "net profits," "risk universes," "portfolio strategy," "hedging," "commodities," and so on. Technology people use terms like "deep packet inspection," "layer three devices," "cross-site scripting," "load balancing," and so forth. Think about the acronyms techies like us throw around—TCP, APT, ICMP, RAID, UDP, L2TP, PPTP, IPSec, and AES. We can have complete

conversations between ourselves without using any real words. And even though business people and technology people use some of the same words, they have totally different meanings to the individual groups. To business people, a protocol is a set of approved processes that must be followed to accomplish a task. To technical people, a protocol is a standardized manner of communication between computers or applications. Business and technical people use the term "risk," but each group is focusing on very different risks a company can face—market share versus security breaches. And even though each group uses the term "data" the same, business people look at data only from a functional point of view and security people look at data from a risk point of view.

This divide between business perspectives and technology perspectives not only can cause confusion and frustration—it commonly costs money. If the business side of the house wants to offer customers a new service, as in paying bills online, there may have to be extensive changes to the current network infrastructure, applications, web servers, software logic, cryptographic functions, authentication methods, database structures, and so on. What seems to be a small change in a business offering can cost a lot of money when it comes to adding up the new technology that needs to be purchased and implemented, programming that needs to be carried out, re-architecting of networks, and the like. It is common for business people to feel as though the IT department is more of an impediment when it comes to business evolution and growth, and in turn the IT department feels as though the business people are constantly coming up with outlandish and unrealistic demands with no supporting budgets.

This type of confusion between business and technology people has caused organizations around the world to implement incorrect solutions because they did not understand the business functionality to technical specifications requirements. This results in having to repurchase new solutions, carry out rework, and waste an amazing amount of time. Not only does this cost the organization more money than it should have in the first place, business opportunities may be lost, which can reduce market share. So we need a tool that both business people and technology people can use to reduce confusion, optimize business functionality, and not waste time and money. This is where business enterprise architectures come into play. They allow both groups (business and technology) to view the same organization in ways that make sense to them.

When you go to the doctor's office, there is a poster of a skeleton system on one wall, a poster of a circulatory system on the other wall, and another poster of the organs that make up a human body. These are all different views of the same thing, the human body. This is the same functionality that enterprise architecture frameworks provide: different views of the same thing. In the medical field we have specialists (podiatrists, brain surgeons, dermatologists, oncologists, ophthalmologists, etc.). Each organization is also made up of its own specialists (HR, marketing, accounting, IT, R&D, management, etc.). But there also has to be an understanding of the entity (whether it is a human body or company) holistically, which is what an enterprise architecture attempts to accomplish.

Zachman Framework

One of the first enterprise architecture frameworks that was created is the *Zachman Framework*, created by John Zachman. This model is generic, and is well suited to frame the work we do in information systems security. A sample (though fairly simplified) representation is depicted in Table 4-4.

		Interrogatives					
		What	**How**	**Where**	**Who**	**When**	**Why**
Perspective (Audience)	Contextual (Executives)	Assets and Liabilities	Business Lines	Business Locales	Partners, Clients, and Employees	Milestones and Major Events	Business Strategy
	Conceptual (Business Mgrs.)	Products	Business Processes	Logistics and Communications	Workflows	Master Calendar	Business Plan
	Architectural (System Architects)	Data Models	Systems Architectures	Distributed Systems Architectures	Use Cases	Project Schedules	Business Rule Models
	Technological (Engineers)	Data Management	Systems Designs	System Interfaces	Human Interfaces	Process Controls	Process Outputs
	Implementation (Technicians)	Data Stores	Programs	Network Nodes and Links	Access Controls	Network/ Security Operations	Performance Metrics
	Enterprise	Information	Functions	Networks	Organizations	Schedules	Strategies

Table 4-4 Zachman Framework for Enterprise Architecture

The Zachman Framework is a two-dimensional model that uses six basic communication interrogatives (What, How, Where, Who, When, and Why) intersecting with different perspectives (Executives, Business Managers, System Architects, Engineers, Technicians, and Enterprise-wide) to give a holistic understanding of the enterprise. This framework was developed in the 1980s and is based on the principles of classical business architecture that contain rules that govern an ordered set of relationships. One of these rules is that each row should describe the enterprise completely from that row's perspective. For example, IT personnel's jobs require them to see the organization in terms of data stores, programs, networks, access controls, operations, and metrics. Though they are (or at least should be) aware of other perspectives and items, the performance of their duties in the example organization is focused on these items.

The goal of this framework is to be able to look at the same organization from different viewpoints. Different groups within a company need the same information, but presented in ways that directly relate to their responsibilities. A CEO needs financial statements, scorecards, and balance sheets. A network administrator needs network schematics, a systems engineer needs interface requirements, and the operations department needs configuration requirements. If you have ever carried out a network-based vulnerability test, you know that you cannot tell the CEO that some systems are vulnerable to time-of-check to time-of-use (TOC/TOU) attacks or that the company software allows for client-side browser injections. The CEO needs to know this information, but in a language she can understand. People at each level of the organization need information in a language and format that are most useful to them.

A business enterprise architecture is used to optimize often fragmented processes (both manual and automated) into an integrated environment that is responsive to change and supportive of the business strategy. The Zachman Framework has been around for many years and has been used by many organizations to build or better define their business environment. This framework is not security oriented, but it is a good template to work with because it offers direction on how to understand an actual enterprise in a modular fashion.

The Open Group Architecture Framework

Another enterprise architecture framework is *The Open Group Architecture Framework (TOGAF)*, which has its origins in the U.S. Department of Defense. It provides an approach to design, implement, and govern an enterprise information architecture.

TOGAF is a framework that can be used to develop the following architecture types:

- Business architecture
- Data architecture
- Applications architecture
- Technology architecture

TOGAF can be used to create these individual architecture types through the use of its *Architecture Development Method (ADM)*. This method is an iterative and cyclic process that allows requirements to be continuously reviewed and the individual architectures

to be updated as needed. These different architectures can allow a technology architect to understand the enterprise from four different views (business, data, application, and technology) so she can ensure her team develops the necessary technology to work within the environment and all the components that make up that environment and meet business requirements. The technology may need to span many different types of networks, interconnect with various software components, and work within different business units. As an analogy, when a new city is being constructed, people do not just start building houses here and there. Civil engineers lay out roads, bridges, waterways, and zones for commercial and residential development. A large organization that has a distributed and heterogeneous environment that supports many different business functions can be as complex as a city. So before a programmer starts developing code, the architecture of the software needs to be developed in the context of the organization it will work within.

NOTE Many technical people have a negative visceral reaction to models like TOGAF. They feel it's too much work, that it's a lot of fluff, is not directly relevant, and so on. If you handed the same group of people a network schematic with firewalls, IDSs, and virtual private networks (VPNs), they would say, "Now we're talking about security!" Security technology works within the construct of an organization, so the organization must be understood also.

Military-Oriented Architecture Frameworks

It is hard enough to construct enterprise-wide solutions and technologies for one organization—think about an architecture that has to span many different complex government agencies to allow for interoperability and proper hierarchical communication channels. This is where the *Department of Defense Architecture Framework (DoDAF)* comes into play. When the U.S. DoD purchases technology products and weapon systems, enterprise architecture documents must be created based upon DoDAF standards to illustrate how they will properly integrate into the current infrastructures. The focus of the architecture framework is on command, control, communications, computers, intelligence, surveillance, and reconnaissance systems and processes. It is not only important that these different devices communicate using the same protocol types and interoperable software components but also that they use the same data elements. If an image is captured from a spy satellite, downloaded to a centralized data repository, and then loaded into a piece of software to direct an unmanned drone, the military personnel cannot have their operations interrupted because one piece of software cannot read another software's data output. The DoDAF helps ensure that all systems, processes, and personnel work in a concerted effort to accomplish its missions.

NOTE While DoDAF was developed to support mainly military missions, it has been expanded upon and morphed for use in business enterprise environments.

When attempting to figure out which architecture framework is best for your organization, you need to find out who the stakeholders are and what information they need from the architecture. The architecture needs to represent the company in the most useful manner to the people who need to understand it the best. If your company has people (stakeholders) who need to understand the company from a business process perspective, your architecture needs to provide that type of view. If there are people who need to understand the company from an application perspective, your architecture needs a view that illustrates that information. If people need to understand the enterprise from a security point of view, that needs to be illustrated in a specific view. So one main difference between the various enterprise architecture frameworks is what type of information they provide and how they provide it.

Other Frameworks

Along with ensuring that we have the proper controls in place, we also want to have ways to construct and improve our business, IT, and security processes in a structured and controlled manner. The security controls can be considered the "things," and processes are how we use these things. We want to use them properly, effectively, and efficiently.

ITIL

ITIL (formerly the *Information Technology Infrastructure Library)* was developed in the 1980s by the UK's Central Computer and Telecommunications Agency (which was subsumed in the late 1990s by the now defunct Office of Government Commerce). ITIL is now controlled by AXELOS, which is a joint venture between the government of the UK and the private firm Capita. ITIL is the de facto standard of best practices for IT service management. ITIL was created because of the increased dependence on information technology to meet business needs. Unfortunately, as previously discussed, a natural divide exists between business people and IT people in most organizations because they use different terminology and have different focuses within the organization. The lack of a common language and understanding of each other's domain (business versus IT) has caused many companies to ineffectively blend their business objectives and IT functions. This improper blending usually generates confusion, miscommunication, missed deadlines, missed opportunities, increased cost in time and labor, and frustration on both the business and technical sides of the house.

ITIL blends all parts of an organization using a four-dimensional model built around the concept of value for the stakeholders. The dimensions in this model, illustrated in Figure 4-7, are organizations and people, value streams and processes, information and technology, and partners and suppliers. These exist in a broader context that is influenced by factors that can be political, economic, social, technological, legal, or environmental. Effective organizations must consider all four dimensions within their broader context when planning, developing, and offering products and/or services if they are to provide value.

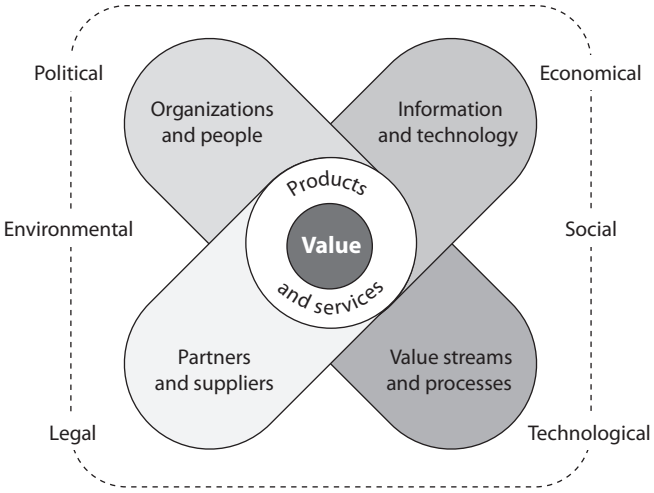

Figure 4-7
ITIL

Six Sigma

Six Sigma is a process improvement methodology. Its goal is to improve process quality by using statistical methods of measuring operation efficiency and reducing variation, defects, and waste. Six Sigma is being used in the security assurance industry in some instances to measure the success factors of different controls and procedures. Six Sigma was developed by Motorola with the goal of identifying and removing defects in its manufacturing processes. The maturity of a process is described by a sigma rating, which indicates the percentage of defects that the process contains. While it started in manufacturing, Six Sigma has been applied to many types of business functions, including information security and assurance.

Capability Maturity Model

While we know that we constantly need to make our security program better, it is not always easy to accomplish because "better" is a vague and nonquantifiable concept. The only way we can really improve is to know where we are starting from, where we need to go, and the steps we need to take in between. Every security program has a maturity level, which could range from nonexistent to highly optimized. In between these two extremes, there are different levels. An example of a Capability Maturity Model (CMM) is illustrated in Figure 4-8. Each maturity level within this model represents an evolutionary stage. Some security programs are chaotic, ad hoc, unpredictable, and usually insecure. Some security programs have documentation created, but the actual processes are not taking place. Some security programs are quite evolved, streamlined, efficient, and effective.

EXAM TIP The CISSP exam puts more emphasis on CMM compared to ITIL and Six Sigma because it is more heavily used in the security industry.

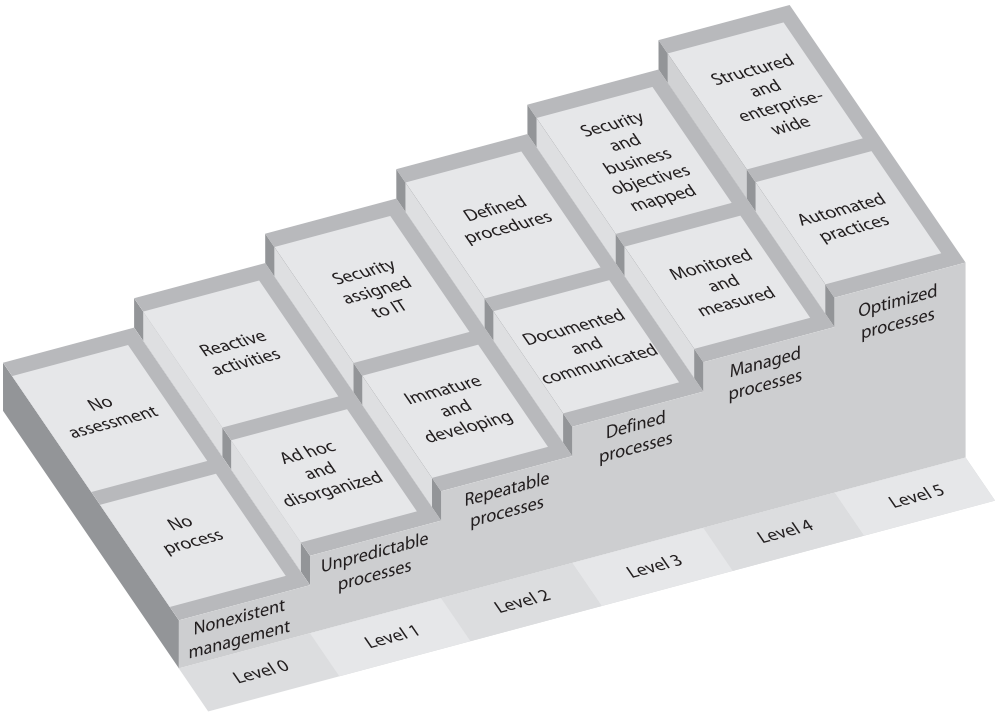

Figure 4-8 Capability Maturity Model for a security program

Security Program Development

No organization is going to put all the previously listed items (NIST RMF, OCTAVE, FAIR, ISO/IEC 27000, NIST CSF, NIST SP 800-53, CIS Controls, COBIT 2019, Zachman Framework, ITIL, Six Sigma, CMM) into place. But it is a good toolbox of things you can pull from, and you will find some fit the organization you work in better than others. You will also find that as your organization's security program matures, you will see more clearly where these various standards, frameworks, and management components come into play. While these items are separate and distinct, there are basic things that need to be built in for any security program and its corresponding controls. This is because the basic tenets of security are universal no matter if they are being deployed in a corporation, government agency, business, school, or nonprofit organization. Each entity is made up of people, processes, data, and technology, and each of these things needs to be protected.

Top-Down Approach

A security program should use a top-down approach, meaning that the initiation, support, and direction come from top management; work their way through middle management; and then reach staff members. In contrast, a bottom-up approach refers to a situation in which staff members (usually IT) try to develop a security program without getting proper management support and direction. A bottom-up approach is commonly less effective, not broad enough to address all security risks, and doomed to fail. A top-down approach makes sure the people actually responsible for protecting the company's assets (senior management) are driving the program. Senior management are not only ultimately responsible for the protection of the organization but also hold the purse strings for the necessary funding, have the authority to assign needed resources, and are the only ones who can ensure true enforcement of the stated security rules and policies. Management's support is one of the most important pieces of a security program. A simple nod and a wink will not provide the amount of support required.

The crux of CMM is to develop structured steps that can be followed so an organization can evolve from one level to the next and constantly improve its processes and security posture. A security program contains a lot of elements, and it is not fair to expect every part to be properly implemented within the first year of its existence. And some components, as in forensics capabilities, really cannot be put into place until some rudimentary pieces are established, as in incident management. So if we really want our baby to be able to run, we have to lay out ways that it can first learn to walk.

Putting It All Together

While the cores of these various security standards and frameworks are similar, it is important to understand that a security program has a life cycle that is always continuing, because it should be constantly evaluated and improved upon. The life cycle of any process can be described in different ways. We will use the following steps:

1. Plan and organize
2. Implement
3. Operate and maintain
4. Monitor and evaluate

Without setting up a life-cycle approach to a security program and the security management that maintains the program, an organization is doomed to treat security as merely another project. Anything treated as a project has a start and stop date, and at the stop date everyone disperses to other projects. Many organizations have had good intentions in their security program kickoffs, but do not implement the proper structure

to ensure that security management is an ongoing and continually improving process. The result is a lot of starts and stops over the years and repetitive work that costs more than it should, with diminishing results.

The main components of each phase are provided here.

Plan and Organize:

- Establish management commitment.
- Establish oversight steering committee.
- Assess business drivers.
- Develop a threat profile on the organization.
- Carry out a risk assessment.
- Develop security architectures at business, data, application, and infrastructure levels.
- Identify solutions per architecture level.
- Obtain management approval to move forward.

Implement:

- Assign roles and responsibilities.
- Develop and implement security policies, procedures, standards, baselines, and guidelines.
- Identify sensitive data at rest and in transit.
- Implement the following blueprints:
  - Asset identification and management
  - Risk management
  - Vulnerability management
  - Compliance
  - Identity management and access control
  - Change control
  - Software development life cycle
  - Business continuity planning
  - Awareness and training
  - Physical security
  - Incident response
- Implement solutions (administrative, technical, physical) per blueprint.
- Develop auditing and monitoring solutions per blueprint.
- Establish goals, SLAs, and metrics per blueprint.

Operate and Maintain:

- Follow procedures to ensure all baselines are met in each implemented blueprint.
- Carry out internal and external audits.
- Carry out tasks outlined per blueprint.
- Manage SLAs per blueprint.

Monitor and Evaluate:

- Review logs, audit results, collected metric values, and SLAs per blueprint.
- Assess goal accomplishments per blueprint.
- Carry out quarterly meetings with steering committees.
- Develop improvement steps and integrate into the Plan and Organize phase.

Many of the items mentioned in the previous list are covered throughout this book. This list is provided to show how all of these items can be rolled out in a sequential and controllable manner.

Although the previously covered standards and frameworks are very helpful, they are also very high level. For example, if a standard simply states that an organization must secure its data, a great amount of work will be called for. This is where the security professional really rolls up her sleeves, by developing security blueprints. *Blueprints* are important tools to identify, develop, and design security requirements for specific business needs. These blueprints must be customized to fulfill the organization's security requirements, which are based on its regulatory obligations, business drivers, and legal obligations. For example, let's say Company Y has a data protection policy, and its security team has developed standards and procedures pertaining to the data protection strategy the company should follow. The blueprint will then get more granular and lay out the processes and components necessary to meet requirements outlined in the policy, standards, and requirements. This would include at least a diagram of the company network that illustrates the following:

- Where the sensitive data resides within the network
- The network segments that the sensitive data transverses
- The different security solutions in place (VPN, TLS, PGP) that protect the sensitive data
- Third-party connections where sensitive data is shared
- Security measures in place for third-party connections
- And more…

The blueprints to be developed and followed depend upon the organization's business needs. If Company Y uses identity management, it needs a blueprint outlining roles, registration management, authoritative source, identity repositories, single sign-on solutions, and so on. If Company Y does not use identity management, it does not need to build a blueprint for this.

So the blueprint lays out the security solutions, processes, and components the organization uses to match its security and business needs. These blueprints must be applied to the different business units within the organization. For example, the identity management practiced in each of the different departments should follow the crafted blueprint. Following these blueprints throughout the organization allows for standardization, easier metrics gathering, and governance. Figure 4-9 illustrates where these blueprints come into play when developing a security program.

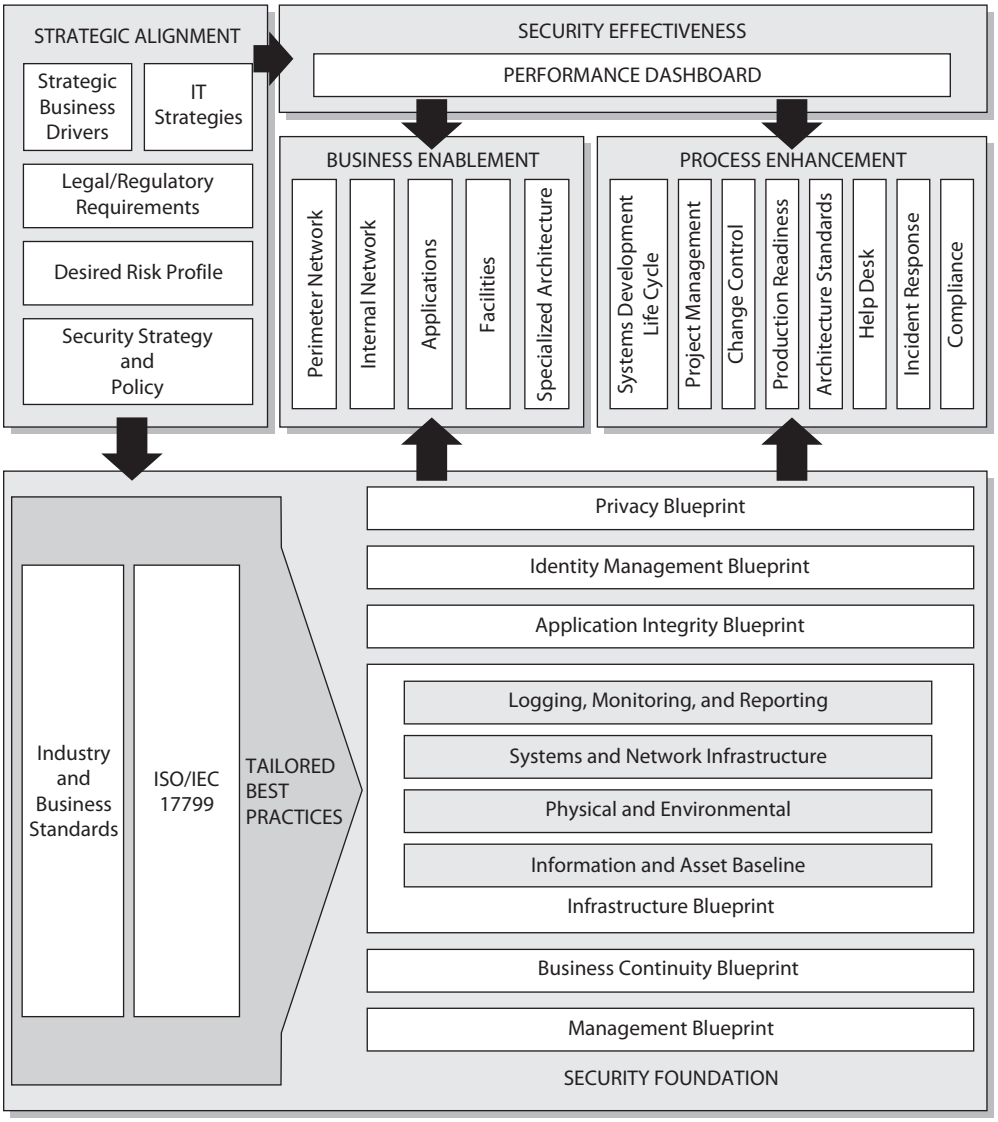

Figure 4-9 Blueprints must map the security and business requirements.

To tie these pieces together, you can think of the NIST Cybersecurity Framework that works mainly at the policy level as a *description* of the type of house you want to build (ranch style, five bedrooms, three baths). The security enterprise framework is the *architecture* layout of the house (foundation, walls, ceilings). The blueprints are the detailed descriptions of specific components of the house (window types, security system, electrical system, plumbing). And the control objectives are the building specifications and codes that need to be met for safety (electrical grounding and wiring, construction material, insulation, and fire protection). A building inspector will use his checklists (building codes) to ensure that you are building your house safely. Which is just like how an auditor will use his checklists (like NIST SP 800-53) to ensure that you are building and maintaining your security program securely.

Once your house is built and your family moves in, you set up schedules and processes for everyday life to happen in a predictable and efficient manner (dad picks up kids from school, mom cooks dinner, teenager does laundry, dad pays the bills, everyone does yard work). This is analogous to ITIL—process management and improvement. If the family is made up of anal overachievers with the goal of optimizing these daily activities to be as efficient as possible, they could integrate a Six Sigma approach where continual process improvement is a focus.

Chapter Review

This chapter should serve at least two purposes for you. First, it familiarizes you with the various frameworks you need to know to pass your CISSP exam. Though some of these frameworks don't fit neatly into one category, we did our best to group them in ways that would help you remember them. So, we have risk management, information security, enterprise architecture, and "other" frameworks. Within information security, we further subdivided the frameworks into those that are focused on program-level issues and those that are primarily concerned with controls. You don't have to know every detail of each framework to pass the exam, but you really should know at least one or two key points about each to differentiate them.

The second purpose of this chapter is to serve as a reference for your professional life. We focused our discussion on the frameworks that are most likely to show up in your work places so that you have a desktop reference to which you can turn when someone asks your opinion about one of these frameworks. While this second purpose of the chapter should apply to the whole book, it is particularly applicable to this chapter because frameworks are tools that don't change very often (especially within an organization), so you may become very familiar with the one(s) you use but a bit rusty on the rest. Grouping them all in this chapter may help you in the future.

Quick Review

- A framework is a guiding document that provides structure to the ways in which we manage risks, develop enterprise architectures, and secure all our assets.
- The most common risk management frameworks (RMFs) are the NIST RMF, ISO/IEC 27005, OCTAVE, and FAIR.

- The seven steps of the NIST RMF are prepare, categorize, select, implement, assess, authorize, and monitor.
- Security controls in the NIST frameworks can be classified as *common* (if they exist outside of a system and apply to multiple systems), *system-specific* (if they exist inside a system boundary and protect only the one system), or *hybrid* (if they are a combination of the other two).
- Risks in a risk management framework can be treated in one of four ways: mitigated, accepted, transferred, or avoided.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a team-oriented risk management methodology that employs workshops and is commonly used in the commercial sector.
- The Factor Analysis of Information Risk (FAIR) risk management framework is the only internationally recognized quantitative approach to risk management.
- The most common information security program frameworks are ISO/IEC 27001 and the NIST Cybersecurity Framework.
- ISO/IEC 27001 is the standard for the establishment, implementation, control, and improvement of the information security management system.
- The NIST Cybersecurity Framework's official name is the "Framework for Improving Critical Infrastructure Cybersecurity."
- The NIST Cybersecurity Framework organizes cybersecurity activities into five higher-level functions: identify, protect, detect, respond, and recover.
- The most common security controls frameworks are NIST SP 800-53, the CIS Controls, and COBIT.
- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, catalogs over 1,000 security controls grouped into 20 families.
- The Center for Internet Security (CIS) Controls is a framework consisting of 20 controls and 171 subcontrols organized in implementation groups to address any organization's security needs from small to enterprise level.
- COBIT is a framework of control objectives and allows for IT governance.
- Enterprise architecture frameworks are used to develop architectures for specific stakeholders and present information in views.
- Blueprints are functional definitions for the integration of technology into business processes.
- Enterprise architecture frameworks are used to build individual architectures that best map to individual organizational needs and business drivers.
- The most common enterprise architecture frameworks are the Zachman and SABSA ones, but you should also be aware of TOGAF and DoDAF.
- Zachman Framework is an enterprise architecture framework, and SABSA is a security enterprise architecture framework.

- ITIL is a set of best practices for IT service management.
- Six Sigma is used to identify defects in processes so that the processes can be improved upon.
- A Capability Maturity Model (CMM) allows for processes to improve in an incremented and standard approach.

Questions

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

1. Which of the following standards would be most useful to you in ensuring your information security management system follows industry best practices?

A. NIST SP 800-53

B. Six Sigma

C. ISO/IEC 27000 series

D. COBIT

2. What is COBIT and where does it fit into the development of information security systems and security programs?

A. Lists of standards, procedures, and policies for security program development

B. Current version of ISO 17799

C. A framework that was developed to deter organizational internal fraud

D. Open standard for control objectives

3. Which publication provides a catalog of security controls for information systems?

A. ISO/IEC 27001

B. ISO/IEC 27005

C. NIST SP 800-37

D. NIST SP 800-53

4. ISO/IEC 27001 describes which of the following?

A. The Risk Management Framework

B. Information security management system

C. Work product retention standards

D. International Electrotechnical Commission standards

5. Which of the following is *not* true about Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)?
   - **A.** It is the only internationally recognized quantitative risk management framework.
   - **B.** It was developed by Carnegie Mellon University.
   - **C.** It is focused only on risk assessments.
   - **D.** It is a team-oriented risk management methodology that employs workshops.
6. What is a key benefit of using the Zachman Framework?
   - **A.** Ensures that all systems, processes, and personnel are interoperable in a concerted effort to accomplish organizational missions
   - **B.** Use of the iterative and cyclic Architecture Development Method (ADM)
   - **C.** Focus on internal SLAs between the IT department and the "customers" it serves
   - **D.** Allows different groups within the organization to look at it from different viewpoints
7. Which of the following describes the Center for Internet Security (CIS) Controls framework?
   - **A.** Consists of over 1,000 controls, divided into 20 families, that are mapped to the security category of an information system
   - **B.** Balances resource utilization, risk levels, and realization of benefits by explicitly tying stakeholder needs to organizational goals to IT goals
   - **C.** Developed to determine the maturity of an organization's processes
   - **D.** Consists of 20 controls divided into three groups to help organizations incrementally improve their security posture
8. Which of the following is not one of the seven steps in the NIST Risk Management Framework (RMF)?
   - **A.** Monitor security controls
   - **B.** Establish the context
   - **C.** Assess security controls
   - **D.** Authorize information system
9. The information security industry is made up of various best practices, standards, models, and frameworks. Some were not developed first with security in mind, but can be integrated into an organizational security program to help in its effectiveness and efficiency. It is important to know of all of these different approaches so that an organization can choose the ones that best fit its business needs and culture. Which of the following best describes the approach(es) that should be put into place if an organization wants to integrate a way to improve its security processes over a period of time?
   - **i.** ITIL should be integrated because it allows for the mapping of IT service process management, business drivers, and security improvement.

ii. Six Sigma should be integrated because it allows for the defects of security processes to be identified and improved upon.

iii. A Capability Maturity Model should be integrated because it provides distinct maturity levels.

iv. The Open Group Architecture Framework should be integrated because it provides a structure for process improvement.

A. i, iii

B. ii, iii, iv

C. ii, iii

D. ii, iv

Use the following scenario to answer Questions 10–12. You are hired as the chief information security officer (CISO) for a medium-size research and development company. Its research file servers were recently breached, resulting in a significant loss of intellectual property. The company is about to start a critical research project and wants to ensure another breach doesn't happen. The company doesn't have risk management or information security programs, and you've been given a modest budget to hire a small team and get things started.

10. Which of the following risk management frameworks would probably *not* be well suited to your organization?

A. ISO/IEC 27005

B. NIST Risk Management Framework (RMF)

C. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

D. Factor Analysis of Information Risk (FAIR)

11. You decide to adopt the NIST Risk Management Framework (RMF) and are in the process of categorizing your information systems. How would you determine the security category (SC) of your research file servers (RFS)?

A. SC_{RFS} = (probable frequency) × (probable future loss)

B. SC_{RFS} = {(confidentiality, *high*),(integrity, *medium*),(availability, *low*)} = *high*

C. SC_{RFS} = {(confidentiality, *high*),(integrity, *medium*),(availability, *low*)} = *medium*

D. SC_{RFS} = Threat × Impact × Probability

12. When selecting the controls for the research file servers, which of the following security control frameworks would be best?

A. NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*

B. ISO/IEC 27002 code of practice for information security controls

C. Center for Information Security (CIS) Controls

D. COBIT 2019

Answers

1. **C.** The ISO/IEC 27000 series is the only option that addresses best practices across the breadth of an ISMS. NIST SP 800-53 and COBIT both deal with controls, which are a critical but not the only component of an ISMS.
2. **D.** COBIT is an open framework developed by ISACA and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and ensure IT maps to business needs.
3. **D.** NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, catalogs over 1,000 security controls. ISO/IEC 27005 and NIST SP 800-37 both describe risk management frameworks, while ISO/IEC 27001 is focused on information security management systems (ISMSs).
4. **B.** ISO/IEC 27001 provides best practice recommendations on information security management systems (ISMSs).
5. **A.** OCTAVE is not a quantitative methodology. The only such methodology for risk management we've discussed is FAIR.
6. **D.** One of the key benefits of the Zachman Framework is that it allows organizations to integrate business and IT infrastructure requirements in a manner that is presentable to a variety of audiences by providing different viewpoints. This helps keep business and IT on the same sheet of music. The other answers describe the DoDAF (A), TOGAF (B), and ITIL (C).
7. **D.** There are 20 CIS controls and 171 subcontrols organized so that any organization, regardless of size, can focus on the most critical controls and improve over time as resources become available. The other answers describe NIST SP 800-53 (A), COBIT 2019 (B), and Capability Maturity Model (C).
8. **B.** Establishing the context is a step in ISO/IEC 27005, not in the NIST RMF. While it is similar to the RMF's prepare step, there are differences between the two. All the other responses are clearly steps in the NIST RMF process.
9. **C.** The best process improvement approaches provided in this list are Six Sigma and Capability Maturity Model. The following outlines the definitions for all items in this question:
   - **TOGAF** Model and methodology for the development of enterprise architectures, developed by The Open Group
   - **ITIL** Processes to allow for IT service management, developed by the United Kingdom's Office of Government Commerce
   - **Six Sigma** Business management strategy that can be used to carry out process improvement
   - **Capability Maturity Model (CMM)** Organizational development for process improvement

10. **D.** The Factor Analysis of Information Risk (FAIR) framework uses a quantitative approach to risk assessment. As we discussed in Chapter 2, this approach requires a lot more expertise and resources than quantitative ones. Since your organization is just getting started with risk management and information security and your resources are limited, this would not be a good fit.
11. **B.** The NIST RMF relies on the Federal Information Processing Standard Publication 199 (FIPS 199) categorization standard, which breaks down a system's criticality by security objective (confidentiality, integrity, availability) and then applies the highest security objective category (the "high water mark") to determine the overall category of the system.
12. **A.** Because you're using the NIST RMF, NIST SP 800-53 is the best answer because the two frameworks are tightly integrated. None of the other answers is necessarily wrong; they're just not as well suited as SP 800-53 for the given scenario.