Over time, the CISSP exam has become more global in nature and less U.S.-centric. Specific questions on U.S. laws and regulations have been taken out of the test, so you do not need to spend a lot of time learning them and their specifics. Be familiar with why laws are developed and put in place and their overall goals, instead of memorizing specific laws and dates.

Privacy Requirements

Privacy compliance requirements stem from the various data protection laws and regulations we've already covered in this chapter (for example, CCPA, GDPR, and HIPAA). The hard part is ensuring you are aware of all the localities within which your organization gathers, stores, and processes various types of private data. The good news is that, at their core, these laws are not all that different from one another in terms of the security controls they require. In almost every case, the controls are reasonable things we would want to have anyway. So, most of the work you'll require to remain compliant is pretty straightforward.

Where things get a bit murkier is when we consider what data is covered and when we are required to notify someone. For example, the GDPR covers PII on EU persons and HIPAA covers PHI on any patient treated by a U.S. healthcare provider. So, if you suffer a data breach affecting the PHI of a German national who received care in your U.S. facilities, you will most likely have to follow both reporting procedures in these two laws. Under the GDPR, you'd have 72 hours from the time of discovery, while under HIPAA, you could have up to 60 days. The notified parties, in addition to the individual whose information was compromised, vary in each case, which further complicates things.

The best approach is collaborate with your business and legal colleague to develop detailed notification procedures that cover each potential breach. Once you're satisfied that your organization can comply with the notification requirements, you should exercise different scenarios to test the procedures and ensure everyone is trained on how to execute them. A breach will ruin your day all by itself, so there's no sense in adding the need to figure out compliance requirements at the point of crisis to make it worse. Furthermore, having procedures that are periodically exercised can help prove to any investigators that you were doing the right things all along.

Liability and Its Ramifications

Executives may be held responsible and liable under various laws and regulations. They could be sued by stockholders and customers if they do not practice due diligence and due care. *Due diligence* can be defined as doing everything within one's power to prevent a bad thing from happening. Examples of this would be setting appropriate policies, researching the threats and incorporating them into a risk management plan, and ensuring audits happen at the right times. *Due care*, on the other hand, means taking the precautions that a reasonable and competent person would take in the same situation. For example, someone who ignores a security warning and clicks through to a malicious website would fail to exercise due care.

EXAM TIP Due diligence is normally associated with leaders, laws, and regulations. Due care is normally applicable to everyone, and failure to exercise it could be used to show negligence.

Before you can figure out how to properly protect yourself, you need to find out what it is you are protecting yourself against. This is what due diligence is all about—researching and assessing the current level of vulnerabilities so the true risk level is understood. Only after these steps and assessments take place can effective controls and safeguards be identified and implemented.

Due Care vs. Due Diligence

Due diligence is the act of gathering the necessary information so the best decision-making activities can take place. Before a company purchases another company, it should carry out due diligence activities so that the purchasing company does not have any "surprises" down the road. The purchasing company should investigate all relevant aspects of the past, present, and predictable future of the business of the target company. If this does not take place and the purchase of the new company hurts the original company financially or legally, the decision makers could be found liable (responsible) and negligent by the shareholders.

In information security, similar data gathering should take place so that there are no "surprises" down the road and the risks are fully understood before they are accepted. If a financial company is going to provide online banking functionality to its customers, the company needs to fully understand all the risks this service entails for the company. Website hacking attempts will increase, account fraud attempts will increase, database attacks will increase, social engineering attacks will increase, and so forth. While this company is offering its customers a new service, it is also making itself a juicier target for attackers and lawyers. The company needs to carry out due diligence to understand all these risks before offering this new service so that the company can make the best business decisions. If it doesn't implement proper countermeasures, the company opens itself up to potential criminal charges, civil suits, regulatory fines, loss of market share, and more.

Due care pertains to acting responsibly and "doing the right thing." It is a legal term that defines the standards of performance that can be expected, either by contract or by implication, in the execution of a particular task. Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

If an organization does not have sufficient security policies, necessary countermeasures, and proper security awareness training in place, it is not practicing due care and can be found negligent. If a financial institution that offers online banking does not implement TLS for account transactions, for example, it is not practicing due care.

Many times due diligence (data gathering) has to be performed so that proper due care (prudent actions) can take place.

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

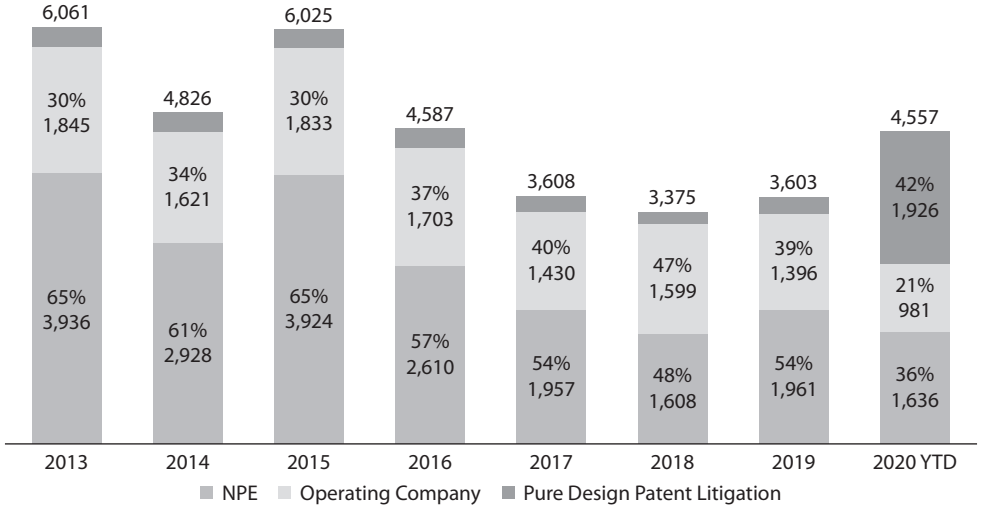


Figure 3-5 Data breach costs (Source: Ponemon Institute and IBM Security)

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.

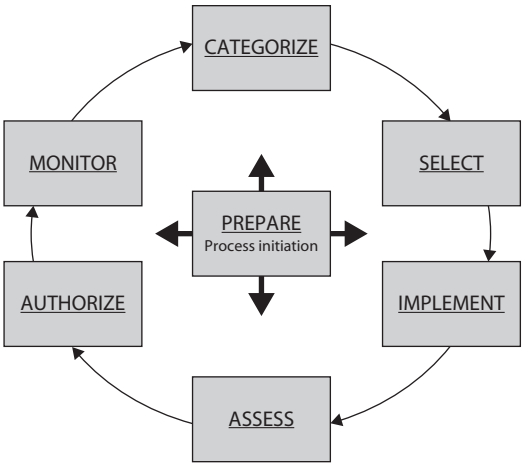


Figure 4-1 The NIST Risk Management Framework process

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

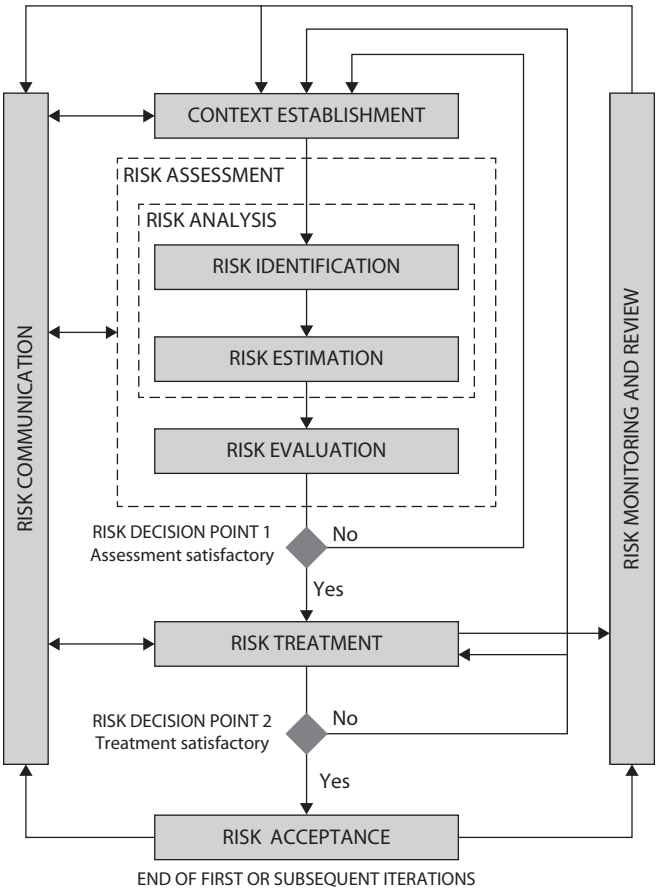


Figure 4-2 ISO/IEC 27005 risk management process

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,

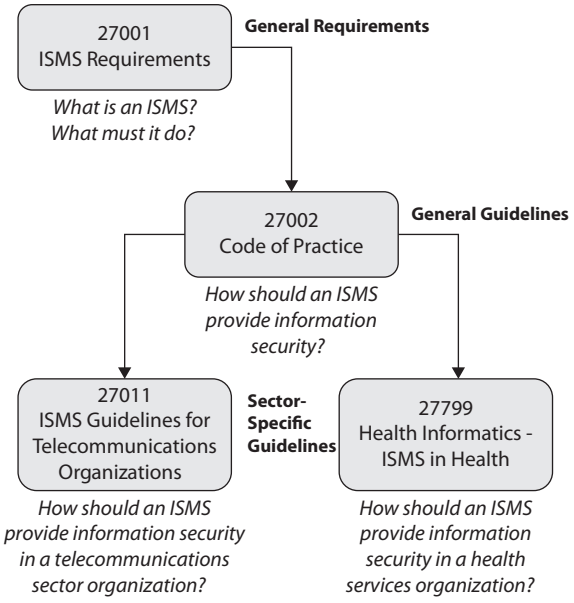


Figure 4-3 How ISO/IEC 27000 standards relate to each other

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.

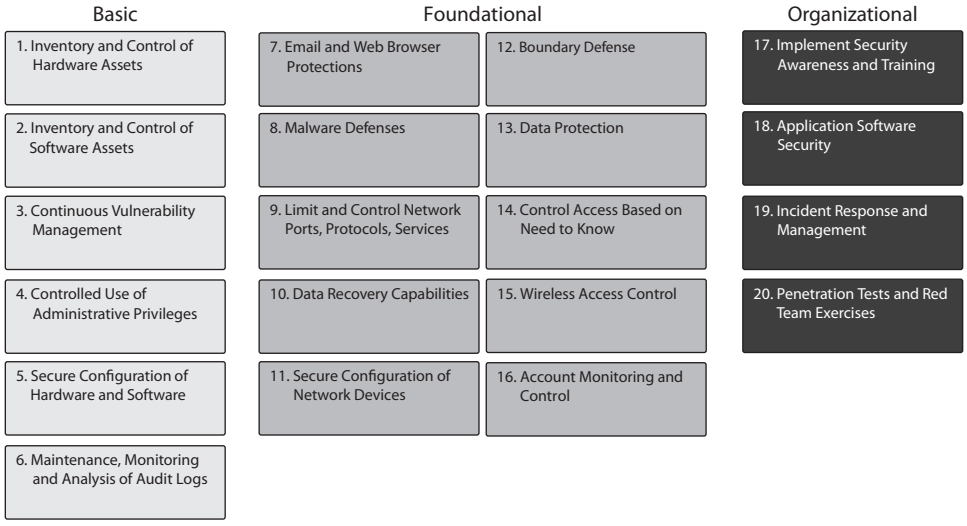


Figure 4-4 CIS Controls

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

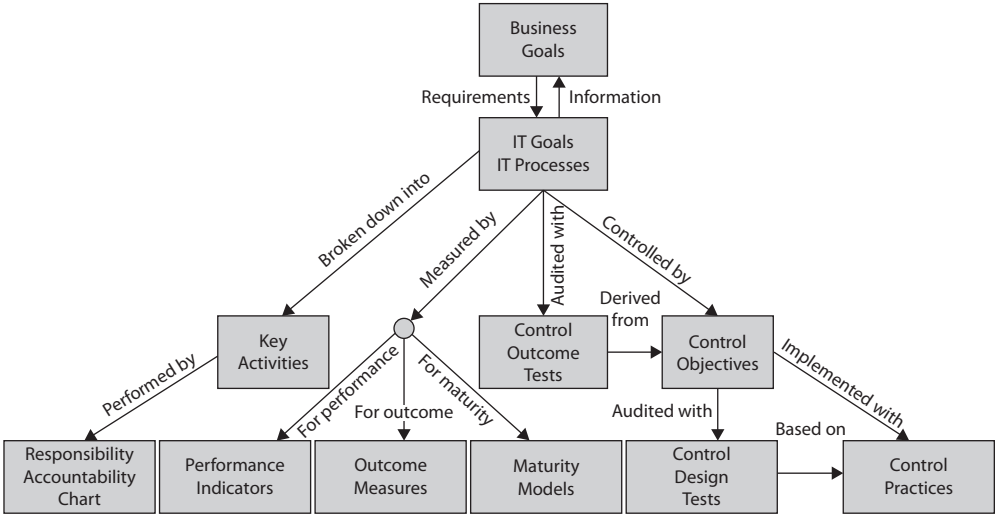


Figure 4-5 COBIT framework

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

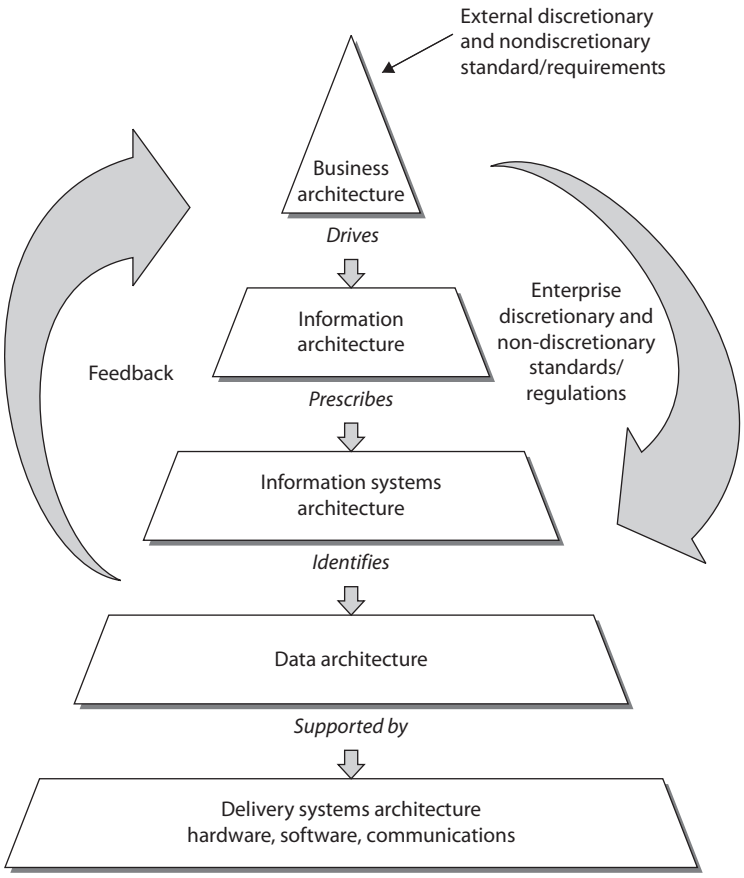


Figure 4-6
NIST enterprise architecture framework

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.

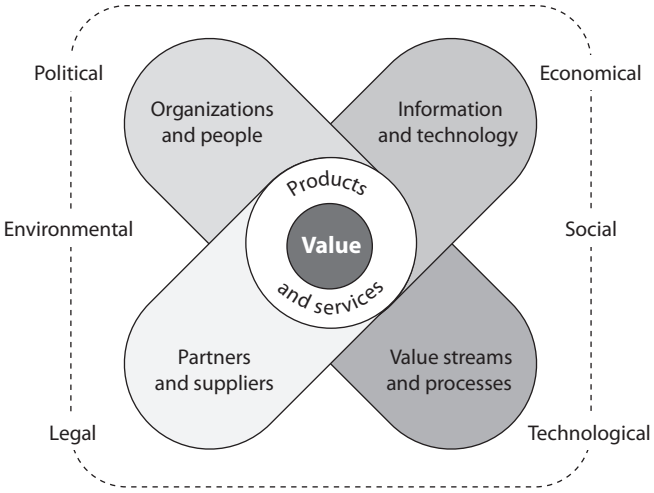


Figure 4-7
ITIL

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.

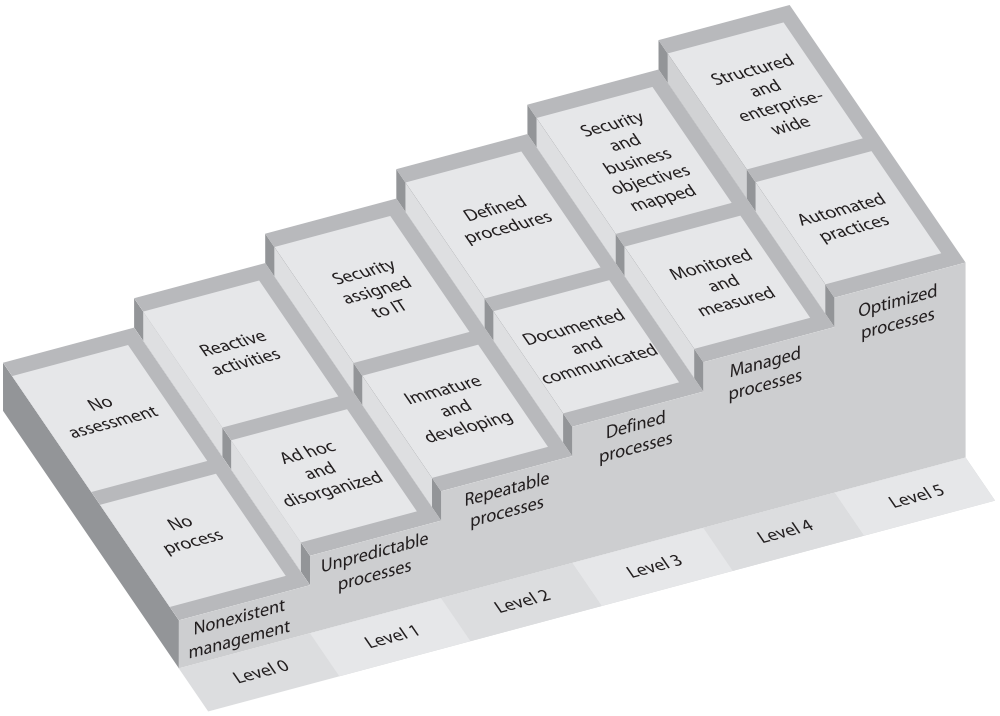


Figure 4-8 Capability Maturity Model for a security program

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.

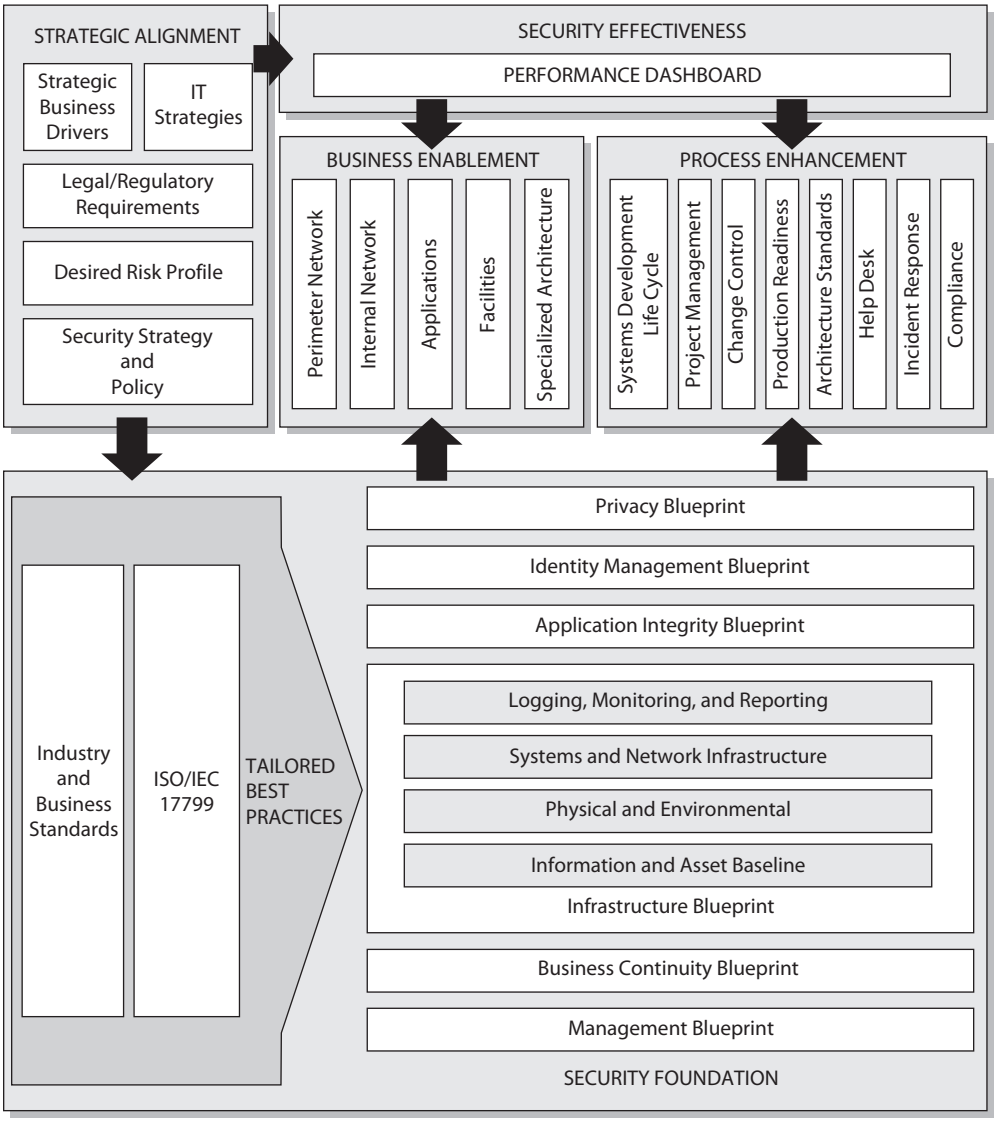


Figure 4-9 Blueprints must map the security and business requirements.

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.

This page intentionally left blank

PART II

Asset Security

This page intentionally left blank

CHAPTER 5

Assets

This chapter presents the following:

- Identification and classification of information and assets
- Information and asset handling requirements
- Secure resource provisioning
- The data life cycle
- Data compliance requirements

You don't know what you've got till it's gone.

—Joni Mitchell

An asset is, by definition, anything of worth to an organization. This includes people, partners, equipment, facilities, reputation, and information. We already touched on the importance of some of these assets when we addressed risk in Chapter 2. While every asset needs to be protected, our coverage of the second CISSP domain in this chapter and the next one focuses a bit more narrowly on protecting information assets. This is because, apart from people, information is typically the most valuable asset to an organization. It lies at the heart of every information system, so precision focus on its protection makes a lot of sense.

Information, of course, exists in context; it is acquired or created at a particular point in time through a specific process and (usually) for a purpose. It moves through an organization's information systems, sometimes adding value to processes and sometimes waiting to be useful. Eventually, the information outlives its utility (or becomes a liability) and must be disposed of appropriately. We start off our discussion of asset security by addressing two fundamental questions: "What do we have?" and "Why should we care?" The first question is probably rather obvious, since we cannot protect that of which we're not aware. The second question may sound flippant, but it really gets to the heart of how important an asset is to the organization. We've already tackled this (at least with regard to data) in Chapter 4 in our discussion of the categorize step of the NIST Risk Management Framework. Data and asset classification, as we will shortly see, is very similar to the categorization we've already explored. Let's get to it!

EXAM TIP An information asset can be either the data, the device on which it is stored and used, or both. In the exam, when you see the term *asset* by itself, it typically means only the device.

Information and Assets

An *asset* can be defined as anything that is useful or valuable. In the context of products and services, this value is usually considered financially: how much would someone pay for it minus how much does the thing cost. If that value is positive, we call the thing an asset. However, if that value is negative (that is, the thing costs more than what someone would pay for it), then we call the thing a liability. Clearly, assets can be both tangible things like computers and firewalls and intangible things like data or reputation. It is important to narrow down the definition for purposes of the CISSP exam, so in this domain, we consider assets as tangible things and we deal with data separately.

Information is a set of data items, placed in a context, and having some meaning. Data is just an item. It could be the word "yes," the time "9:00," or the name "Fernando's Café" and, by itself, has no meaning. Put this data together in the context of an answer to the question "Would you like to have coffee tomorrow morning?" and now we have information. Namely, that we'll be sharing a beverage tomorrow morning at a particular place. Data processing yields information, and this is why we often use these two terms interchangeably when talking about security issues.

Identification

Whether we are concerned with data security or asset security (or both), we first have to know what we have. Identification is simply establishing what something is. When you look at a computing device occupying a slot in your server rack, you may want to know what it is. You may want to identify it. The most common way of doing this is by placing tags on our assets and data. These tags can be physical (e.g., stickers), electronic (e.g., radio frequency identification [RFID] tags), or logical (e.g., software license keys). Using tags is critically important to establishing and maintaining accurate inventories of our assets.

But what about data? Do we need to identify it and track it like we do with our more tangible assets? The answer is: it depends. Most organizations have at least some data that is so critical that, were it to become lost or corrupted or even made public, the impact would be severe. Think of financial records at a bank, or patient data at a healthcare provider. These organizations would have a very bad day indeed if any of those records were lost, inaccurate, or posted on the dark web. To prevent this, they go to great lengths to identify and track their sensitive information, usually by using metadata embedded in files or records.

While it may not be critical (or even feasible) for many organizations to identify all their information, it is critical to most of us to at least decide how much effort should be put into protecting different types of data (or assets, for that matter). This is where classification comes in handy.

Classification

Classification just means saying that something belongs to a certain class. We could say, for example, that your personnel file belongs to the class named "private" and that your organization's marketing brochure for the latest appliance belongs to the class "public." Right away, we would have a sense that your file has more value to your organization than the brochure. The rationale behind assigning values to different assets and data is that this enables an organization to gauge the amount of funds and resources that should go toward protecting each class, because not all assets and data have the same value to an organization. After identifying all important data, it should be properly classified. An organization copies and creates a lot of data that it must maintain, so classification is an ongoing process and not a one-time effort.

Data Classification

An important metadata item that should be attached to all our information is a classification level. This classification tag, which remains attached (and perhaps updated) throughout the life cycle of the data, is important to determining the protective controls we apply to the data.

Information can be classified by sensitivity, criticality, or both. Either way, the classification aims to quantify how much loss an organization would likely suffer if the information was lost. The *sensitivity* of information is commensurate with the losses to an organization if that information was revealed to unauthorized individuals. This kind of compromise has made headlines in recent years with the losses of information suffered by organizations such as Equifax, Sina Weibo, and Marriott International. In each case, the organizations lost trust and had to undertake expensive responses because sensitive data was compromised.

The *criticality* of information, on the other hand, is an indicator of how the loss of the information would impact the fundamental business processes of the organization. In other words, critical information is that which is essential for the organization to continue operations. For example, Code Spaces, a company that provided code repository services, was forced to shut down in 2014 after an unidentified individual or group deleted its code repositories. This data was critical to the operations of the company and, without it, the corporation had no choice but to go out of business.

Once data is segmented according to its sensitivity or criticality level, the organization can decide what security controls are necessary to protect different types of data. This ensures that information assets receive the appropriate level of protection, and classifications indicate the priority of that security protection. The primary purpose of data classification is to indicate the level of confidentiality, integrity, and availability protection that is required for each type of data set. Many people mistakenly only consider the confidentiality aspects of data protection, but we need to make sure our data is not modified in an unauthorized manner and that it is available when needed.

Data classification helps ensure that data is protected in the most cost-effective manner. Protecting and maintaining data costs money, but spending money for the information that actually requires protection is important. If you were in charge of making sure Russia does not know the encryption algorithms used when transmitting information to and

from U.S. spy satellites, you would use more extreme (and expensive) security measures than you would use to protect your peanut butter and banana sandwich recipe from your next-door neighbor.

Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed. For example, in a corporation, confidential information may be accessed only by senior management and a select few trusted employees throughout the company. Accessing the information may require two or more people to enter their access codes. Auditing could be very detailed and its results monitored daily, and paper copies of the information may be kept in a vault. To properly erase this data from the media, degaussing or overwriting procedures may be required. Other information in this company may be classified as sensitive, allowing a slightly larger group of people to view it. Access control on the information classified as sensitive may require only one set of credentials. Auditing happens but is only reviewed weekly, paper copies are kept in locked file cabinets, and the data can be deleted using regular measures when it is time to do so. Then, the rest of the information is marked public. All employees can access it, and no special auditing or destruction methods are required.

EXAM TIP Each classification level should have its own handling and destruction requirements.

Classification Levels There are no hard and fast rules on the classification levels that an organization should use. Table 5-1 explains the types of classifications available. An organization could choose to use any of the classification levels presented in Table 5-1. One organization may choose to use only two layers of classifications, while another organization may choose to use four. Note that some classifications are more commonly used for commercial businesses, whereas others are military classifications.

The following are the common levels of sensitivity from the highest to the lowest for commercial business:

- Confidential
- Private
- Sensitive
- Public

And here are the levels of sensitivity from the highest to the lowest for military purposes:

- Top secret
- Secret
- Confidential
- Controlled unclassified information
- Unclassified

Classification	Definition	Example	Organizations That Would Use This
Public	• Disclosure is not welcome, but it would not cause an adverse impact to company or personnel.	• How many people are working on a specific project • Upcoming projects	Commercial business
Sensitive	• Requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized modification or deletion. • Requires higher-than-normal assurance of accuracy and completeness.	• Financial information • Details of projects • Profit earnings and forecasts	Commercial business
Private	• Personal information for use within a company. • Unauthorized disclosure could adversely affect personnel or the company.	• Work history • Human resources information • Medical information	Commercial business
Confidential	• For use within the company only. • Data exempt from disclosure under the Freedom of Information Act or other laws and regulations. • Unauthorized disclosure could seriously affect a company.	• Trade secrets • Healthcare information • Programming code • Information that keeps the company competitive	Commercial business Military
Unclassified	• Data is not sensitive or classified.	• Computer manual and warranty information • Recruiting information	Military
Controlled unclassified information (CUI)	• Sensitive, but not secret. • Information that cannot legally be made public.	• Health records • Answers to test scores	Military
Secret	• If disclosed, it could cause serious damage to national security.	• Deployment plans for troops • Unit readiness information	Military
Top secret	• If disclosed, it could cause grave damage to national security.	• Blueprints of new weapons • Spy satellite information • Espionage data	Military

Table 5-1 Commercial Business and Military Data Classifications

The classifications listed in Table 5-1 are *commonly* used in the industry, but there is a lot of variance. An organization first must decide the number of data classifications that best fit its security needs, then choose the classification naming scheme, and then define what the names in those schemes represent. Company A might use the classification level "confidential," which represents its most sensitive information. Company B might use "top secret," "secret," and "confidential," where confidential represents its least sensitive information. Each organization must develop an information classification scheme that best fits its business and security needs.

EXAM TIP The terms "unclassified," "secret," and "top secret" are usually associated with governmental organizations. The terms "private," "proprietary," and "sensitive" are usually associated with nongovernmental organizations.

It is important to not go overboard and come up with a long list of classifications, which will only cause confusion and frustration for the individuals who will use the system. The classifications should not be too restrictive either, because many types of data may need to be classified. As with every other issue in security, we must balance our business and security needs.

Each classification should be unique and separate from the others and not have any overlapping effects. The classification process should also outline how information is controlled and handled through its life cycle (from creation to termination).

NOTE An organization must make sure that whoever is backing up classified data—and whoever has access to backed-up data—has the necessary clearance level. A large security risk can be introduced if low-level technicians with no security clearance have access to this information during their tasks.

Once the scheme is decided upon, the organization must develop the criteria it will use to decide what information goes into which classification. The following list shows some criteria parameters an organization may use to determine the sensitivity of data:

- The usefulness of data
- The value of data
- The age of data
- The level of damage that could be caused if the data were disclosed
- The level of damage that could be caused if the data were modified or corrupted
- Legal, regulatory, or contractual responsibility to protect the data
- Effects the data has on security
- Who should be able to access the data
- Who should maintain the data
- Who should be able to reproduce the data
- Lost opportunity costs that could be incurred if the data were not available or were corrupted

Applications and sometimes whole systems may need to be classified. The applications that hold and process classified information should be evaluated for the level of protection they provide. You do not want a program filled with security vulnerabilities to process and "protect" your most sensitive information. The application classifications should be based on the assurance (confidence level) the organization has in the software and the type of information it can store and process.

CAUTION The classification rules must apply to data no matter what format it is in: digital, paper, video, fax, audio, and so on.

Asset Classification

Information is not the only thing we should classify. Consider that information must reside somewhere. If a confidential file is stored and processed in the CEO's laptop, then that device (and its hard drive if it is removed) should also be considered worthy of more protection. Typically, the classification of an asset (like a removable drive or a laptop) used to store or process information should be as high as the classification of the most valuable data in it. If an asset has public, sensitive, and confidential information, then that asset should be classified as private (the highest of the three classifications) and protected accordingly.

Classification Procedures

The following outlines the necessary steps for a proper classification program:

1. Define classification levels.
2. Specify the criteria that will determine how data is classified.
3. Identify data owners who will be responsible for classifying data.
4. Identify the data custodian who will be responsible for maintaining data and its security level.
5. Indicate the security controls, or protection mechanisms, required for each classification level.
6. Document any exceptions to the previous classification issues.
7. Indicate the methods that can be used to transfer custody of the information to a different data owner.
8. Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.
9. Indicate procedures for declassifying the data.
10. Integrate these issues into the security awareness program so all employees understand how to handle data at different classification levels.

Physical Security Considerations

We discuss data security in detail in Chapter 10. However, that data lives physically in devices and printed documents, both of which require protection also. The main threats that physical security components combat are theft, interruptions to services, physical damage, compromised system and environment integrity, and unauthorized access. Real loss is determined by the cost to replace the stolen items, the negative effect on productivity, the negative effect on reputation and customer confidence, fees for consultants that may need to be brought in, and the cost to restore lost data and production levels. Many times, organizations just perform an inventory of their hardware and provide value estimates that are plugged into risk analysis to determine what the cost to the organization would be if the equipment were stolen or destroyed. However, the data held within the equipment may be much more valuable than the equipment itself, and proper recovery mechanisms and procedures also need to be plugged into the risk assessment for a more realistic and fair assessment of cost. Let's take a look at some of the controls we can use in order to mitigate risks to our data and to the media on which it resides.

Protecting Mobile Devices

Mobile devices are almost indispensable. For most of us, significant chunks of our personal and work lives are chronicled in our smartphones or tablets. Employees who use these devices as they travel for work may have extremely sensitive company or customer data on their systems that can easily fall into the wrong hands. This problem can be mitigated to a point by ensuring our employees use company devices for their work, so we can implement policies and controls to protect them. Still, many organizations allow their staff members to bring their own devices (BYOD) to the workplace and/or use them for work functions. In these cases, it is not only security but also privacy that should receive serious attention.

There is no one-size-fits-all solution to protecting company, let alone personal, mobile devices. Still, the following list provides some of the mechanisms that can be used to protect these devices and the data they hold:

- Inventory all mobile devices, including serial numbers, so they can be properly identified if they are stolen and then recovered.
- Harden the operating system by applying baseline secure configurations.
- Stay current with the latest security updates and patches.
- Ensure mobile devices have strong authentication.
- Register all devices with their respective vendors, and file a report with the vendor when a device is stolen. If a stolen device is sent in for repairs after it is stolen, it will be flagged by the vendor if you have reported the theft.
- Do not check mobile devices as luggage when flying. Always carry them on with you.
- Never leave a mobile device unattended, and carry it in a nondescript carrying case.

- Engrave the device with a symbol or number for proper identification.
- Back up all data on mobile devices to an organizationally controlled repository.
- Encrypt all data on a mobile device.
- Enable remote wiping of data on the device.

Tracing software can be installed so that your device can "phone home" if it is taken from you. Several products offer this tracing capability. Once installed and configured, the software periodically sends in a signal to a tracking center or allows you to track it through a website or application. If you report that your device has been stolen, the vendor of this software may work with service providers and law enforcement to track down and return your device.

Paper Records

It is easy to forget that many organizations still process information on paper records. The fact that this is relatively rare compared to the volume of their electronic counterparts is little consolation when a printed e-mail with sensitive information finds its way into the wrong hands and potentially causes just as much damage. Here are some principles to consider when protecting paper records:

- Educate your staff on proper handling of paper records.
- Minimize the use of paper records.
- Ensure workspaces are kept tidy so it is easy to tell when sensitive papers are left exposed, and routinely audit workspaces to ensure sensitive documents are not exposed.
- Lock away all sensitive paperwork as soon as you are done with it.
- Prohibit taking sensitive paperwork home.
- Label all paperwork with its classification level. Ideally, also include its owner's name and disposition (e.g., retention) instructions.
- Conduct random searches of employees' bags as they leave the office to ensure sensitive materials are not being taken home.
- Destroy unneeded sensitive papers using a crosscut shredder, or consider contracting a document destruction company.

Safes

An organization may have need for a safe. Safes are commonly used to store backup data tapes, original contracts, or other types of valuables. The safe should be penetration resistant and provide fire protection. The types of safes an organization can choose from are

- **Wall safe** Embedded into the wall and easily hidden
- **Floor safe** Embedded into the floor and easily hidden

- **Chests** Stand-alone safes
- **Depositories** Safes with slots, which allow the valuables to be easily slipped in
- **Vaults** Safes that are large enough to provide walk-in access

If a safe has a combination lock, it should be changed periodically, and only a small subset of people should have access to the combination or key. The safe should be in a visible location, so anyone who is interacting with the safe can be seen. It should also be covered by a video surveillance system that records any activity around it. The goal is to uncover any unauthorized access attempts. Some safes have passive or thermal relocking functionality. If the safe has a *passive relocking* function, it can detect when someone attempts to tamper with it, in which case extra internal bolts will fall into place to ensure it cannot be compromised. If a safe has a *thermal relocking* function, when a certain temperature is met (possibly from drilling), an extra lock is implemented to ensure the valuables are properly protected.

Managing the Life Cycle of Assets

A life-cycle model describes the changes that an entity experiences during its lifetime. While it may seem odd to refer to assets as having a "life," the fact is that their utility for (and presence within) organizations can be described with clear start and end points. That is the lifetime of the asset within that organization (even if it gets refurbished and used elsewhere). After the asset departs, its utility is oftentimes transferred to its replacement even if the new asset is different than the original in meaningful ways. That new asset will, in turn, be replaced by something else, and so on.

The life cycle, which is shown in Figure 5-1, starts with the identification of a new requirement. Whoever identifies the new requirement either becomes its champion or

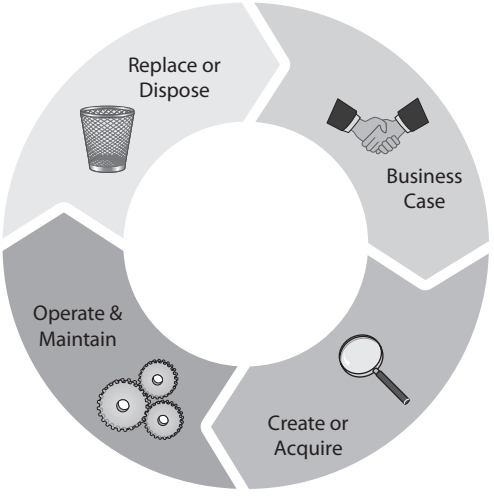


Figure 5-1 The IT asset life cycle

finds someone else to do so. The champion for this requirement then makes a business case for it that shows that the existing assets are unable to satisfy this need. The champion also explains why the organization really should get a new asset, which typically includes a conversation about risks and return on investment (ROI). If the champion is successful, senior management validates the requirement and identifies the needed resources (people, money, time).

The validated requirement then goes to a change management board, giving the different organizational stakeholders a say in what, how, and when the asset will be acquired. This board's goal is to ensure that this new asset doesn't break any processes, introduce undue risks, or derail any ongoing projects. In mature organizations, the change management process also attempts to look over the horizon and see what the long-term ramifications of this asset might be. After the board determines how to proceed, the new asset is either developed in-house or acquired from a vendor.

The third phase of asset management is also the longest one: operation and maintenance (O&M). Before the asset is put into operation, the IT and security operations teams configure it to balance three (sometimes competing) goals: it must be able to do whatever it was acquired to do, it must be able to do it without interfering or breaking anything else, and it must be secure. This configuration will almost certainly need to change over time, which is why we discuss configuration management in Chapter 20.

NOTE This initial part of the O&M phase is usually the most problematic for a new asset and is a major driver for the use of an integrated product team (IPT) such as DevOps, which we discuss in Chapter 24.

Eventually, the asset is no longer effective (in terms of function or cost) or required. At this point, it moves out of O&M and is retired. This move, as you may have already guessed, triggers another review by the change management board, because retiring the asset is likely to have effects on other resources or processes. Once the process of retirement is hashed out, the asset is removed from production. At this point, the organization needs to figure out what to do with the thing. If the asset stored any data, the data probably has to be purged. If the asset has any environmentally hazardous materials, it has to be properly discarded. If it might be useful to someone else, it might be donated or sold. At any rate, the loss of this asset may result in a new requirement being identified, which starts the whole asset management life cycle again, as shown in Figure 5-1.

Ownership

In most cases, whoever makes the business case for an asset ultimately owns it, but this is not always the case. Asset *ownership*, once the asset shows up and as long as it remains in the organization, entails responsibility for the effective management of the asset over its whole life cycle. Ownership in this sense is somewhat different than ownership in a strictly legal sense. The legal owner of a server could be the corporation that buys it, while the life cycle owner would be whatever employee or department is responsible for it on a day-to-day basis.

Inventories

One of the fundamental responsibilities for asset owners is to keep track of their assets. Though the approaches to tracking hardware and software vary, they are both widely recognized as critical controls. At the very least, it is very difficult to defend an asset that you don't know you have. As obvious as this sounds, many organizations lack an accurate and timely inventory of their hardware and software.

Tracking Hardware

Seemingly, maintaining awareness of which devices are in your organization should be an easier task than tracking your software. A hardware device can be seen, touched, and bar-scanned. It can also be sensed electronically once it is connected to the network. If you have the right tools and processes available, tracking hardware should not be all that difficult, right? Not so fast. It turns out that the set of problems ranges from supply chain security to insider threats and everything in between.

Let's start with the basics. How do you ensure that a new device you've ordered is the right one and free of back doors or piracy issues? There have been multiple reports in the news media recently of confirmed or suspected back doors installed in hardware assets by either manufacturers (e.g., pirated hardware) or by third parties (e.g., government spy agencies) before the assets get to the organization that acquired them. In response to these and other threats, the International Organization for Standardization published ISO 28000:2007 as a means for organizations to use a consistent approach to securing their supply chains. In essence, we want to ensure we purchase from trusted sources, use a trusted transportation network, and have effective inspection processes to mitigate the risk of pirated, tampered, or stolen hardware.

But even if we can assure ourselves that all the hardware we acquire is legitimate, how would we know if someone else were to add devices to our networks? Asset monitoring includes not only tracking our known devices but also identifying unknown ones that may occasionally pop up in our enclaves. Examples that come to mind from personal experience include rogue wireless access points, personal mobile devices, and even (believe it or not) telephone modems. Each introduces unknown (and thus unmitigated) risks. The solution is to have a comprehensive monitoring process that actively searches for these devices and ensures compliance with your organization's security policies.

In many cases, monitoring devices on the premises can be as simple as having a member of the security or IT team randomly walk through every space in the organization looking for things that are out of place. This becomes even more effective if this person does this after work hours and also looks for wireless networks as part of these walks. Alternatively, much of this monitoring can be done using device management platforms and a variety of sensors.

Tracking Software

Obviously, we can't just walk around and inventory our software. The unique challenges of tracking software are similar to those of managing hardware, but with a few important differences. Unlike hardware, software assets can be copied or installed multiple times. This could be a problem from a licensing perspective. Commercial applications typically

have limits on how many times you can install a single license. The terms of these licensing agreements vary wildly from single-use to enterprise-wide. It bears pointing out that tracking what software is installed on which systems, and for which users, is an important part of software asset management. Otherwise, you risk violating software licenses.

Using unlicensed software not only is unethical but also exposes an organization to financial liability from the legitimate product vendors. This liability can manifest in a number of ways, including having the organization reported to the vendor by a disgruntled employee. It could also come up when certain software packages "phone home" to the vendors' servers or when downloading software patches and updates. Depending on the number and types of licenses, this could end up costing significant amounts of money in retroactive licensing fees.

Pirated software is even more problematic because many forms of it include back doors installed by the pirates or are Trojan horses. Even if this were not the case, it would almost certainly be impossible to update or patch this software, which makes it inherently more insecure. Since no IT staff in their right mind would seriously consider using pirated software as an organizational policy, its presence on a network would suggest that at least some users have privileges that are being abused and to which they may not be entitled.

Another problem created by the fact that you can copy and install software on multiple systems, apart from unlicensed or pirated software, is security. If you lose track of how many copies of which software are on your systems, it is harder to ensure they are all updated and patched. Vulnerability scanners and patch management systems are helpful in this regard, but depending on how these systems operate, you could end up with periods (perhaps indefinitely long) of vulnerability.

The solution to the software tracking problem is multifaceted. It starts with an assessment of the legitimate application requirements of the organization. Perhaps some users need an expensive photo editing software suite, but its provisioning should be carefully controlled and only available to that set of users in order to minimize the licensing costs. Once the requirements are known and broken down by class of user, there are several ways to keep a handle on what software exists on which systems. Here are some of the most widely accepted best practices:

- **Application whitelisting** A whitelist is a list of software that is allowed to execute on a device or set of devices. Implementing this approach not only prevents unlicensed or unauthorized software from being installed but also protects against many classes of malware.
- **Using Gold Masters** A Gold Master is a standard image workstation or server that includes properly configured and authorized software. Organizations may have multiple images representing different sets of users. The use of Gold Masters simplifies new device provisioning and configuration, particularly if the users are not allowed to modify them.
- **Enforcing the principle of least privilege** If the typical users are not able to install any software on their devices, then it becomes a lot harder for rogue applications to show up in our networks. Furthermore, if we apply this approach, we mitigate risks from a very large set of attacks.

- **Device management software** Unified endpoint management (UEM) systems allow you to fully and remotely manage most devices, including smartphones, tablets, laptops, printers, and even Internet of Things (IoT) devices.
- **Automated scanning** Every device on your network should be periodically scanned to ensure it is running only approved software with proper configurations. Deviations from this policy should be logged and investigated by the IT or security team.

Licensing Issues

Companies have the ethical obligation to use only legitimately purchased software applications. Software makers and their industry representation groups such as The Software Alliance (BSA) use aggressive tactics to target companies that use pirated (illegal) copies of software.

Companies are responsible for ensuring that software in the corporate environment is not pirated and that the licenses (that is, license counts) are being abided by. An operations or configuration management department is often where this capability is located in a company. Automated asset management systems, or more general system management systems, may be able to report on the software installed throughout an environment, including a count of installations of each. These counts should be compared regularly (perhaps quarterly) against the inventory of licensed applications and counts of licenses purchased for each application. Applications that are found in the environment and for which no license is known to have been purchased by the company, or applications found in excess of the number of licenses known to have been purchased, should be investigated.

When applications are found in the environment for which the authorized change control and supply chain processes were not followed, they need to be brought under control, and the business area that acquired the application outside of the approved processes must be educated as to the legal and information security risks their actions may pose to the company. Many times, the business unit manager would need to sign a document indicating he understands this risk and is personally accepting it.

An application for which no valid business need can be found should be removed, and the person who installed the application should be educated and warned that future such actions may result in more severe consequences—like termination. This may sound extreme, but installing pirated software is not only an ethical violation but also both a liability risk and a potential vector for introducing malware. Organizations that use or tolerate unlicensed products are sometimes turned in by disgruntled employees as an act of revenge.

Companies should have an acceptable use policy (AUP) that indicates what software users can install and informs users that the environment will be surveyed from time to time to verify compliance. Technical controls should be emplaced to prevent unauthorized users from being able to install unauthorized software in the environment.

A fundamental best practice in software asset management is to prevent users from installing software and requiring them to submit a request for a system administrator to do so instead. This allows the administrator to ensure the software is properly licensed and added to the appropriate management systems. It also enables effective configuration management across the enterprise.

Controlling the existing hardware and software on our networks should be a precondition to provisioning new services and capabilities. To do otherwise risks making an already untenable position even worse.

Secure Provisioning

The term "provisioning" is overloaded in the technology world, which is to say that it means different actions to different people. To a telecommunications service provider, it could mean the process of running wires, installing customer premises equipment, configuring services, and setting up accounts to provide a given service (e.g., DSL). To an IT department, it could mean the acquisition, configuration, and deployment of an information system (e.g., a new server) within a broader enterprise environment. Finally, to a cloud services provider, provisioning could mean automatically spinning up a new instance of that physical server that the IT department delivered to us.

For the purpose of the CISSP exam, *provisioning* is the set of all activities required to provide one or more new information services to a user or group of users ("new" meaning previously not available to that user or group). Though this definition is admittedly broad, it does subsume all that the overloaded term means. As you will see in the following sections, the specific actions included in various types of provisioning vary significantly, while remaining squarely within our given definition.

At the heart of provisioning is the imperative to provide these information services in a secure manner. In other words, we must ensure that both the services and the devices on which they rely are secure. We already discussed supply chain risks in asset acquisition in Chapter 2. So, assuming you have a trusted supply chain, you would want to start with a Gold Master image applied to your devices as soon as you receive them. Ideally, you would then configure them according to the needs defined in the business and adapted to whatever classes of user they will support. Finally, you scan for vulnerabilities (just to be sure) and deploy it on the network. Easy, right?

Well, it gets a bit trickier when you deal with remote employees, which for many organizations are an increasing portion of their workforce. Some of the added concerns to consider are listed here:

- Securely shipping the devices to users
- Securely sending credentials to users
- Requirements for virtual private network (VPN) connectivity
- Remote monitoring of whether or not the device is on the VPN
- Making remote configuration changes
- Multifactor authentication while the device is disconnected

Obviously, the list of issues will very much depend on your particular situation. You may not have any remote users but perhaps you have a data center or hosting provider who owns the physical environment in which your assets reside. That presents its own set of concerns you need to think through in terms of secure provisioning. Finally, and perhaps inescapably, many of us have to consider unique issues when dealing with cloud assets.

Provisioning Cloud Assets

Generally, cloud provisioning is the set of all activities required to provide one or more new cloud assets to a user or group of users. So what exactly are these cloud assets? As we will see in Chapter 7, cloud computing is generally divided into three types of service: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The provisioning of each type of service presents its own set of issues.

When we are dealing with provisioning IaaS assets, our user population is limited to the IT department. To see why this is true, we need only consider a noncloud (that is, physical) equivalent: provisioning a new server or router. Because these assets typically impact a large number of users in the organization, we must be very careful in planning and testing their provisioning. Accordingly, these provisioning actions often require the approval of the senior leadership or of the change control committee. Only a very small group of IT personnel should be able to perform such provisioning.

PaaS is similar to IaaS in terms of organizational impact, but oftentimes has a more limited scope. A platform, in this context, is typically a service such as a web or database management service. Though the IT team typically handles the provisioning, in some cases someone else in the organization may handle it. Consider, for example, the case of a development (intranet-only) web service that is being provisioned to test a web application that a team of coders is developing. Depending on the scope, context, and accessibility, this provisioning could be delegated to any one of the developers, though someone in IT would first constrain the platform to ensure it is accessible only to that team.

Finally, SaaS could be provisioned by a larger pool of users within the constraints established by the IT team in accordance with the organizational policy. If a given group of users is authorized to use the customer relationship management (CRM) system, then those users should be able to log into their accounts and self-provision that and any other applications to which they are authorized.

As you can see, the provisioning of cloud assets should be increasingly more controlled depending on the organizational impact and the risk profile of the specific asset. The key to secure provisioning is carefully setting up the cloud computing environment so that properly configured applications, platforms, and infrastructure are rapidly available to authorized users when and where they need them. After all, one of the benefits of cloud computing is the promise of self-service provisioning in near real time.

Asset Retention

Assets typically remain in use until they are no longer required, they become obsolete, or their O&M costs exceed their value to the organization. If they are no longer required, they may still be retained for some time in anticipation of future needs or perhaps for emergency use. Asset retention should be a deliberate decision that is documented and periodically revisited. Ideally, this is done as part of the change management process to ensure the retained (and no longer in use) assets don't pose undue risks.

Suppose your organization has a policy of refreshing laptops for its workforce every three years. After the latest refresh, you end up with a dozen laptops that are no longer required. Someone suggests you keep them around in case of an emergency, so you do. A couple of refresh cycles later, you end up with dozens of laptops (some of them potentially unable to run modern software) clogging up your storage spaces. This is a problem for at least four reasons. Firstly, you've run out of storage space. Secondly, there is a risk of theft since nobody is paying much attention to the laptops in the closet. Thirdly, they may no longer work when that emergency finally happens and you decide to pull them out and use them. Finally, and perhaps most seriously, unless they were properly decommissioned, they could have sensitive data in their disk drives that nobody is aware of.

Your asset retention decision-making should consider the fact that your asset life cycle may differ from its manufacturer's intended one. Original equipment manufacturers (OEMs) sell a particular product only for a specific period of time, typically one to three years. After that, they'll move on to the next version or may stop making it altogether. Either way, the product is no longer sold. OEMs will, however, continue to support their product after this point for some time, usually another three to six years. Replacement parts may still be sold and customer support resources will remain available to registered owners. *End-of-life (EOL)* for an asset is that point in time when its OEM is neither manufacturing nor sustaining it. In other words, you can't send it in for repairs, buy spare parts, or get technical assistance from the OEM. The risk in using assets after their announced EOL is that hardware failures will be much more difficult to address at reasonable costs.

There is a related term, *end-of-support (EOS)*, which is sometimes also called end-of-service-life (EOSL), that means that the manufacturer is no longer patching bugs or vulnerabilities on the product. Typically, manufacturers will continue issuing patches after a product reaches EOL for another few years. Sometimes, however, EOL and EOS coincide. Either way, we face significant risk after the product reaches EOS because whatever vulnerabilities are discovered will remain unpatched, meaning the asset is much more likely to be exploited.

Whether the business needs change or the asset reaches EOL or EOS, eventually it's time to retire it, which may drive a new business case. Before throwing an asset in the recycling bin, however, we need to properly decommission it.

Decommissioning Assets

Once an asset has reached the end of its useful life in your organization, it's important to follow a thorough process to decommission it. *Decommissioning* is the set of all activities required to permanently remove an existing asset from an operational environment. In a way, it is the opposite of provisioning.

The specific tasks required to decommission assets vary greatly depending on what the asset is. However, there are some overarching thoughts to consider before pulling the proverbial plug. These include the following:

- *Decommission only within the change management process.* The only way to minimize the risk of unintended (adverse) consequences when you pull the plug is to ensure that everyone who may have a stake in the asset is part of the decision.

- *Ensure that the asset is no longer in use.* It may seem obvious, but there may be unknown users (or uses) of the asset that were never properly documented. You'd hate to pull the plug, only to find out you killed a critical business process.
- *Review the impact on data retention.* We'll discuss data retention later in this chapter, but you have to ensure that there isn't any data in the asset (and only in that asset) that needs to be preserved.
- *Securely wipe any data on the asset.* It seems like just about every asset has the potential to hold sensitive data in nonvolatile memory or disk. Be sure you understand the persistent data storage capabilities in the asset, and you wipe them.
- *Safely dispose of the hardware.* Many assets have hazardous components such as lithium batteries that require special handling. Don't just toss that old computer into the dumpster before checking for environmental or safety hazards first.

Data Life Cycle

The data life cycle differs from the asset life cycle in some important ways. First, it usually doesn't cost anything to acquire most of the data our organizations use. Sure, there are notable exceptions, but, overall, we don't really have to demonstrate the ROI or get the chief financial officer (CFO) to agree that we need to know what each customer buys on an e-commerce site. (Actually, a CFO should be justifiably worried if that data is *not* being collected.) Another significant difference is that we can share our data with as many others as we'd like without losing it. Finally, data tends to be archived rather than disposed of when it is no longer immediately useful. Sure, we can put a workstation in a storage room in case we need it later, but this is the exception rather than the norm when dealing with tangible assets.

There are a number of data life-cycle models out there. The one we will use for our discussion is fairly simple but still effective when considering the changing nature of data and the security implications of those dynamics. At a macro level, we can divide the life of our data into six phases: acquisition, storage, use, sharing, archival, and destruction, as shown in Figure 5-2.

Data Acquisition

Generally speaking, data is acquired by an organization in one of three ways: collected directly, copied from elsewhere, or created from scratch. Collection is possible when an organization has sensors in an environment of interest. For example, an e-commerce site has a web server that can *collect* the IP address of visitors and what page referred them to the site. The application server can further collect the identity of each customer, which products they explored, and what they eventually bought. All this data can be enhanced by buying customer data from ad agencies and having it *copied* into a local data store. Finally, the marketing department can analyze all that data and *create* reports and forecasts.

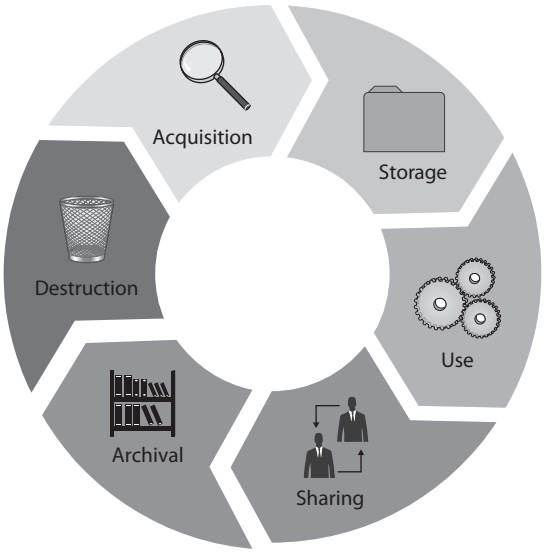


Figure 5-2
The data life cycle

Data Collection

We must ensure that the data we collect, particularly when it is personal in nature, is necessary for our jobs. Generally speaking, organizations should collect the least amount of private personal data required for the performance of their business functions. In many cases, this is not a matter of choice but of law. As of 2020, over 128 countries have enacted privacy protection laws that affect organizations within their jurisdictions. It is important to note that privacy protections vary widely among countries. The European Union is one of the most restrictive regions with respect to privacy, while China effectively has no restrictions, and therefore no real privacy protections. The United States has very few restrictions on the collection of private data by nongovernmental organizations at the national level, but has states such as California with protections similar to those of the EU. The point is that you have to be aware of the specific privacy laws that pertain to the places in which your organization stores or uses its data. This is particularly important when you outsource services (which may require access to your data) to third parties in a different country.

Apart from applicable laws and regulations, the types of personal data that your organization collects, as well as its life-cycle considerations, must be a matter of explicit written policy. Your privacy policy needs to cover your organization's collection, use, disclosure, and protection of employee and client data. Many organizations break their privacy policy into two documents: an internal document that covers employee data, and an external document that covers customer information. At a minimum, you want to answer the following questions when writing your policy:

- What personal data is collected (e.g., name, website visits, e-mail messages, etc.)?
- Why do we collect this data and how do we use it (e.g., to provide a service, for security)?

- With whom do we share this data (e.g., third-party providers, law enforcement agencies)?
- Who owns the collected data (e.g., subject, organization)?
- What rights does the subject of this data have with regard to it (e.g., opt out, restrictions)?
- When do we destroy the data (e.g., after five years, never)?
- What specific laws or regulations exist that pertain to this data (e.g., HIPAA, GDPR)?

Data Storage

After data is acquired, but before it can be used, it must be stored somewhere. There are also other steps we must take to make the information useful. Typically, we attach both system metadata (e.g., author, date/time of creation, and permissions) and business process metadata (e.g., classification, project, and owner) to it. Finally, the data is indexed to facilitate searching and assigned to one or more data stores. In smaller organizations, much of this process is invisible to the user. All that person knows is that when they create a contact in the CRM system, an order in the purchasing system, or a ticket in the workflow system, the entry is magically available to everyone in the organization who needs to access the information. In larger organizations, the process needs to be carefully architected.

Finally, there are policy controls that we have to apply. For instance, we have to encrypt credit card numbers and certain other personally identifiable information (PII) wherever

Where in the World Is My Data?

Data location can be a particularly important issue, especially when dealing with personal, healthcare, or national security data. As we discussed in Chapter 3, some countries have *data localization* laws that require certain types of data to be stored and processed in that country (examples include China and Russia). Other countries have enacted *data sovereignty* laws that stipulate that anyone who stores or processes certain types of data (typically personal data on their citizens), whether or not they do so locally, must comply with those countries' laws. Meeting these requirements can be impossible without data classification. It can also be either enabled or hindered by cloud services. Used properly, cloud service providers can help ensure data localization requirements are met by restricting certain classifications of data to a region or even a specific country. If, on the other hand, data location is not considered when architecting a cloud solution, it is very likely that sensitive data will end up in some random location at some point, potentially causing no shortage of headaches (and perhaps legal and financial liability) to its owners.

we store them. We also have to implement strict controls on who gets to access sensitive information. Additionally, we may have to provide some sort of rollback capability to revert data to a previous state, particularly if users or processes may be able to corrupt it. These and many other important considerations must be deliberately addressed as we store the data and not as an afterthought.

Data Retention

There is no universal agreement on how long an organization should retain data. Legal and regulatory requirements (where they exist) vary among countries and business sectors. What is universal is the need to ensure your organization has and follows a documented data retention policy. Doing otherwise is flirting with disaster, particularly when dealing with pending or ongoing litigation. It is not enough, of course, to simply have a policy; you must ensure it is being followed, and you must document this through regular audits.

NOTE When outsourcing data storage, it is important to specify in the contract language how long the storage provider will retain your data after you stop doing business with them and what process they will use to eradicate your data from their systems.

A very straightforward and perhaps tempting approach would be to look at the lengthiest legal or regulatory retention requirement imposed on your organization and then apply that timeframe to all your data retention. The problem with this approach is that it will probably make your retained data set orders of magnitude greater than it needs to be. Not only does this impose additional storage costs, but it also makes it more difficult to comply with electronic discovery (e-discovery) orders. When you receive an e-discovery order from a court, you are typically required to produce a specific amount of data (usually pretty large) within a given timeframe (usually very short). Obviously, the more data you retain, the more difficult and expensive this process will be.

A better approach is to segregate the specific data sets that have mandated retention requirements and handle those accordingly. Everything else should have a retention period that minimally satisfies the business requirements. Commonly, different business units within medium and large organizations have different retention requirements. For instance, a company may want to keep data from its research and development (R&D) division for a much longer period than it keeps data from its customer service division. R&D projects that are not particularly helpful today may be so at a later date, but audio recordings of customer service calls probably don't have to hang around for several years.

NOTE Be sure to get buy-in from your legal counsel when developing or modifying data retention and privacy policies.

Developing a Retention Policy

At its core, every data retention policy answers three fundamental questions:

- What data do we keep?
- How long do we keep this data?
- Where do we keep this data?

Most security professionals understand the first two questions. After all, many of us are used to keeping tax records for three years in case we get audited. The "what" and the "how long" are easy. The last question, however, surprises more than a few of us. The twist is that the question is not so much about the location per se, but rather the manner in which the data is kept at that location. In order to be useful to us, retained data must be easy to locate and retrieve.

Think about it this way. Suppose your organization had a business transaction with Acme Corporation in which you learned that Acme was involved in the sale of a particular service to a client in another country. Two years later, you receive a third-party subpoena asking for any data you may have regarding that sale. You know you retain all your data for three years, but you have no idea where the relevant data may be. Was it an e-mail, a recording of a phone conversation, the minutes from a meeting, or something else? Where would you go looking for it? Alternatively, how could you make a case to the court that locating and providing the data would be too costly for your organization?

What Data We Retain There are many reasons to retain data. Among the more common ones are data analysis (to plot trends and make predictions), historical knowledge (how did we deal with this in the past?), and regulatory requirements. Again, legal counsel must be involved in this process to ensure all legal obligations are being met. Beyond these obligations, there will be specific information that is important to the business for a variety of reasons. It is also worth considering what data might be valuable in light of business arrangements, partnerships, or third-party dealings.

The decision to retain data must be deliberate, specific, and enforceable. We want to keep only the data that we consciously decide to keep, and then we want to ensure that we can enforce that retention. Importantly, there should be a way for us to ensure that data that should not be retained is promptly and properly disposed of. If this sounds painful, we need only consider the consequences of not getting this process right. Many companies have endured undue hardships because they couldn't develop, implement, and enforce a proper retention policy. Among the biggest challenges in this realm is the balance between business needs and employee or customer privacy.

How Long We Retain Once upon a time, there were two main data retention longevity approaches: the "keep nothing" camp and the "keep everything" camp. As the legal processes caught up with modern computer technology, it became clear that (except in very limited cases) these approaches were not acceptable. For starters, whether they

Data Retention in the Age of Big Data

The term *big data* refers to collections of data that exhibit five characteristics: volume, velocity, variety, veracity, and value. Volume refers to the sheer size of the data collection, which exceeds what can reasonably be stored in traditional systems like a regular data server or a conventional database management system. Velocity describes the high speed with which new data is added, while variety means that the data is not all in the same format or even concerning the same things. Because the data comes from a multitude of sources, its veracity is difficult to establish, but we oftentimes deal with this by looking for trends and clusters rather than individual data points. Finally, there is an expectation that all this data adds value to our organizations, which justifies the costs of storing and processing it in the first place.

This last point is the crux of data retention in the age of big data: just because we *can* keep every data point from every business unit and occasionally get valuable insights is not sufficient reason to keep the data. It is far easier (and way more cost effective) to develop a retention policy that allows us to build big data stores as needed, but does so in a way that balances risks, costs, and value. Are there privacy or confidentiality issues concerning any of the data? Could any data create a legal liability for the organization? Is any of the data likely to be subject to e-discovery? If so, how difficult would it be to comply with an e-discovery order?

Apart from any legal or regulatory concerns, there's also the practical one of deciding what data is useful and what is just taking up storage space. Even if the price tag of storage doesn't seem excessive now, left unchecked, we can get there quicker than expected if we keep pumping data in. And when we get there, how would we go about removing the data we no longer want or need?

This all underscores the importance of being deliberate about building our big data stores and having policies and procedures that support valid organizational requirements, while mitigating risks at a reasonable cost.

retained nothing or everything, organizations following one of these extreme approaches found out it was difficult to defend themselves in lawsuits. The first group had nothing with which to show due diligence, for instance, while those in the second group had too much information that plaintiffs could use against them. So what is the right data retention policy? Ask your legal counsel. Seriously.

There are myriads of statutory and regulatory retention requirements, which vary from jurisdiction to jurisdiction (sometimes even within the same country). There are also best practices and case law to consider, so we won't attempt to get too specific here. Still, Table 5-2 provides some general guidelines sufficient to start the conversation with your attorneys.

Type of Data	General Period of Retention
Business documents (e.g., meeting minutes)	7 years
Invoices	5 years
Accounts payable and receivable	7 years
Human resource files	7 years (for employees who leave) or 3 years (for candidates who were not hired)
Tax records	3 years after taxes were paid
Legal correspondence	Permanently

Table 5-2 Typical Retention Periods for Different Types of Data

How We Retain Data In order for retained data to be useful, it must be accessible in a timely manner. It really does us no good to have data that takes an inordinate (and perhaps prohibitive) amount of effort to query. To ensure this accessibility, we need to consider various issues, including the ones listed here.

- **Taxonomy** A taxonomy is a scheme for classifying data. This classification can be made using a variety of categories, including functional (e.g., human resources, product development), chronological (e.g., 2020), organizational (e.g., executives, union employees), or any combination of these or other categories.
- **Classification** The sensitivity classification of the data determines the controls we place on it both while it is in use and when it gets archived. This is particularly important because many organizations protect sensitive information while in use, but not so much after it goes into the archives.
- **Normalization** Retained data comes in a variety of formats, including word processing documents, database records, flat files, images, PDF files, video, and so on. Simply storing the data in its original format is not sufficient in any but the most trivial cases. Instead, we need to develop tagging schemas that make the data searchable.
- **Indexing** Retained data must be searchable if we are to quickly pull out specific items of interest. The most common approach to making data searchable is to build indexes for it. Many archiving systems implement this feature, but others do not. Either way, the indexing approach must support the likely future queries on the archived data.

Ideally, archiving occurs in a centralized, regimented, and homogenous manner. We all know, however, that this is seldom the case. We may have to compromise in order to arrive at solutions that meet our minimum requirements within our resource constraints. Still, as we plan and execute our retention strategies, we must remain focused on how we will efficiently access archived data many months or years later.

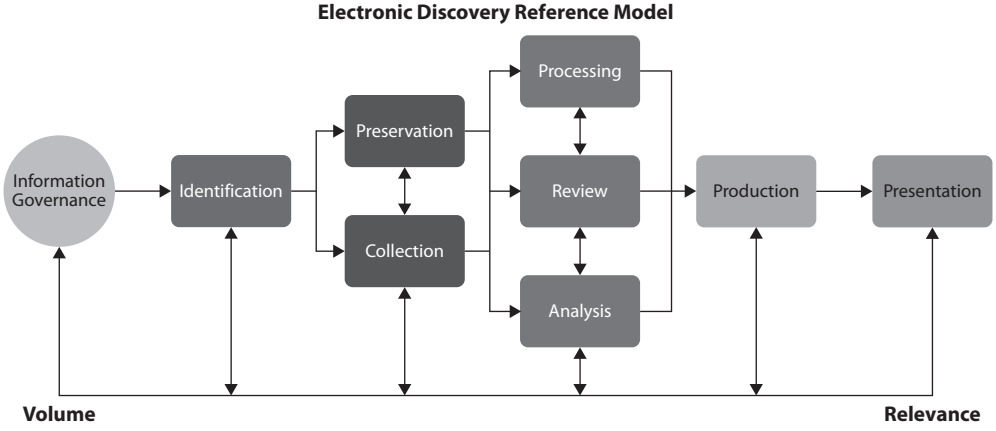
E-Discovery

Discovery of electronically stored information (ESI), or *e-discovery*, is the process of producing for a court or external attorney all ESI pertinent to a legal proceeding. For example, if your company is being sued for damages resulting from a faulty product,

the plaintiff's attorney could get an e-discovery order compelling you to produce all e-mail between the QA team and senior executives in which the product's faults are discussed. If your data retention policy and procedures are adequate, e-discovery should not require excessive efforts. If, on the other hand, you have been slack about retention, such an order could cripple the organization.

The Electronic Discovery Reference Model (EDRM) identifies eight steps, though they are not necessarily all required, nor are they performed in a linear manner:

1. **Identification** of data required under the order.
2. **Preservation** of this data to ensure it is not accidentally or routinely destroyed while complying with the order.
3. **Collection** of the data from the various stores in which it may be.
4. **Processing** to ensure the correct format is used for both the data and its metadata.
5. **Review** of the data to ensure it is relevant.
6. **Analysis** of the data for proper context.
7. **Production** of the final data set to those requesting it.
8. **Presentation** of the data to external audiences to prove or disprove a claim.



(Source: EDRM; www.edrm.net)

Data Use

After data is acquired and stored, it will spend much of its time being used. That is to say it will be read and modified by a variety of users with the necessary access level. From a security perspective, this stage in the data life cycle presents the most challenges in terms of ensuring confidentiality, integrity, and availability. You want the information available, but only to the right people who should then be able to modify it in authorized ways.

Consistency is also an issue with regard to policy and regulatory compliance. As the information is used and aggregated, it may trigger requirements that must be automatically enforced. For example, a document that refers to a project using a code word or name

may be unclassified and freely available, but if that word/name is used in conjunction with other details (a place, purpose, or team members' names), then it would make the entire document classified. Changes in the information as it is in use must be mapped to the appropriate internal policies, and perhaps to regulations or laws.

Data Maintenance

As data is being used, we have to ensure that it remains accurate and internally consistent. Suppose that Sally is a salesperson in our organization. She meets a prospective customer named Charlie and enters his contact information and other details into a CRM system. E-mails are exchanged, meetings are scheduled, and documents are filed with Charlie's data. One day, Charlie gets a promotion and moves to corporate headquarters. Just like that, his title, phone number, and address all change. How do we ensure that we update this data and that we do it across the entire organization? Sure, the CRM piece is easy, but what about the myriad of other places in which the now obsolete data exists? We need to have a plan for maintaining the accuracy of data that is being used and may be critical to our business processes.

We must also consider what happens when the data is incorrect when it is first acquired. There was a recent story in the news about a police clerk who incorrectly entered the personal information of a convicted murderer who had just been transferred to his station. The information was actually that of an innocent citizen who had, earlier that day, applied for a permit. The erroneous information was shared across the country with local, national, and even private organizations. By the time the error was discovered, there was no way to globally correct the entry. To this day, that innocent man is periodically denied employment or services because some system shows that he is a convicted murderer. For most of our organizations, this scenario would likely result in hefty fines or a major lawsuit unless we had an effective way to maintain our data.

Another case for data maintenance deals with corruption and inconsistencies. For instance, if we have multiple data stores for performance or reliability purposes, we must ensure that modifications to the data are replicated. We also need to have mechanisms for automatically resolving inconsistencies, such as those that would occur from a server having a power outage after data has been modified but before it has been replicated. This is particularly important in very dynamic systems that have rollback capabilities.

Data Sharing

Gone are the days when any of us could accomplish anything significant solely on our own. Virtually every organization in the world, particularly those with information systems, is part of a supply chain. Information sharing is a key enabler of modern supply chains. Without it, we wouldn't be able to log into our systems (especially if you have a third-party identity management service like Google or Facebook), send or receive e-mail, or sell widgets online (it's hard to sell something without sharing payment card information with a payment processor).

While we all have some data sharing requirements imposed by our IT infrastructure, we also willingly share data with others for specific business reasons. For example, an e-commerce site will almost certainly partner with a digital advertising firm to drum up

business and with a logistics company to deliver tangible goods. It may also partner with other companies that offer complementary goods or services and collect referral fees from each other. There are many other reasons to share data, but the important concept here is that this sharing needs to be deliberate. If you share the wrong data, or do so in the wrong way, you could lose competitive advantage or even break the law.

To avoid data sharing nightmares, be sure to involve all the necessary staff (business, IT, security, legal) in the conversation early. Discuss the business need to share data and restrict that data to the minimum essential to satisfy that need. Document the agreement in a legally binding contract that's been approved by your legal counsel. This agreement needs to specify the obligations of each party with regard to the entire shared data life cycle. For example, what data will be shared, how it will be stored and used by each party, with whom it may be shared, how it will be archived and for how long, and, finally, when and how it will be destroyed.

Data Archival

The data in our systems will likely stop being used regularly (or at all) at some point. When this happens, but before we get rid of it, we probably want to retain it for a variety of reasons. Maybe we anticipate that it will again be useful at a later time, or maybe we are required to keep it around for a certain period of time, as is the case with certain financial information. Whatever the reason for moving this data off to the side, the fact that it is no longer regularly used could mean that unauthorized or accidental access and changes to it could go undetected for a long time if we don't implement appropriate controls. Of course, the same lack of use could make it easier to detect this threat if we do have the right controls.

Another driver for retention is the need for backups. Whether we're talking about user or back-end backups, it is important to consider our risk assessment when deciding which backups are protected and how. To the extent that end-user backups are performed to removable disk drives, it is difficult to imagine a scenario in which these backups should not be encrypted. Every major operating system provides a means to perform automatic backups as well as encrypt those backups. Let's take advantage of this.

This all leads us to the question of how long we need to retain data. If we discard it too soon, we risk not being able to recover from a failure or an attack. We also risk not being able to comply with e-discovery requests or subpoenas. If we keep the data for too long,

Backup vs. Archive

The terms backup and archive are sometimes used interchangeably. In reality, they have different meanings that are best illustrated using the life-cycle model described in this section. A data *backup* is a copy of a data set currently in use that is made for the purpose of recovering from the loss of the original data. Backup data normally becomes less useful as it gets older.

A data *archive* is a copy of a data set that is no longer in use, but is kept in case it is needed at some future point. When data is archived, it is usually removed from its original location so that the storage space is available for data in use.

we risk excessive costs as well as increased liabilities. The answer, once again, is that this is all part of our risk management process and needs to be codified in policies.

Data Destruction

Sooner or later, every organization will have to dispose of data. This usually, but not always, means data destruction. Old mailboxes, former employee records, and past financial transactions are all examples of data sets that must, at some point, be destroyed. When this time comes, there are two important issues to consider: that the data does in fact get destroyed, and that it is destroyed correctly. When we discuss roles and responsibilities later in this chapter, we'll see who is responsible for ensuring that both of these issues are taken care of.

A twist on the data destruction issue is when we need to transfer the data to another party and then destroy it on our data stores. For instance, organizations hosting services for their clients typically have to deal with requests to do a bulk export of their data when they migrate to another provider. Companies sometimes sell accounts (e.g., home mortgages) to each other, in which case the data is transferred and eventually (after the mandatory retention period) destroyed on the original company's systems.

No matter the reason, we have to ensure that the data is properly destroyed. How this is done is, again, tied to our risk management. The bottom line is that the data must be rendered sufficiently difficult for an adversary to recover so that the risk of such recovery is acceptable to our organization. This is not hard to do when we are dealing with physical devices such as hard disk drives that can be wiped, degaussed, or shredded (or all of these in particularly risk-adverse organizations such as certain government entities). Data destruction can be a bit more complicated when we deal with individual files (or parts thereof) or database records (such as many e-mail systems use for mailbox storage). Further complicating matters, it is very common for multiple copies of each data item to exist across our information systems. How can you ensure that all versions are gone? The point is that the technical details of how and where the data is stored are critical to ensuring its proper destruction.

Data Remanence

Even when policies exist (and are enforced and audited) to ensure the protection of privacy, it is possible for technical issues to threaten this privacy. It is a well-known fact that most data deletion operations do not, in fact, erase anything; normally, they simply mark the memory as available for other data, without wiping (or even erasing) the original data. This is true not only of file systems but also of databases. Since it is difficult to imagine a data store that would not fit in either of these two constructs, it should be clear that simply "deleting" data will likely result in data remanence issues.

NOTE NIST Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization* (December 2014), describes the best practices for combating data remanence.

Let's consider what happens when we create a text file using the File Allocation Table (FAT) file system. Though this original form of FAT is antiquated, its core constructs

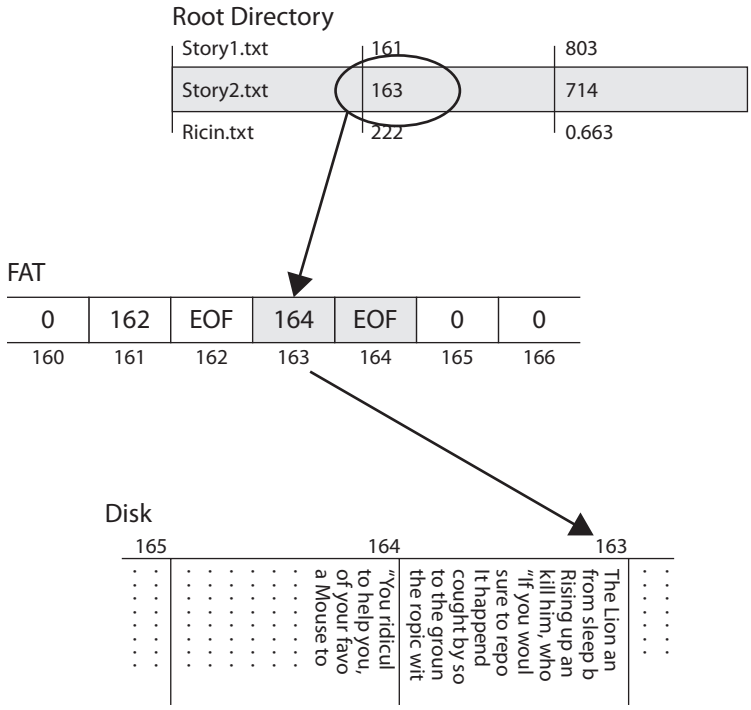


Figure 5-3
Writing a text file to disk

(e.g., disk blocks, free block list/table, file metadata table) are also found at the heart of all other modern file systems. Its simplicity makes it a wonderful training tool for the purpose of explaining file creation and deletion.

Suppose we type up the famous Aesop fable titled "The Lion and the Mouse" in a text editor and save it to disk. The operating system will ask us for a filename, which will be Story2.txt for this example. The system will then check the File Allocation Table for available blocks on which to store the text file. As shown in Figure 5-3, the system creates a directory entry for the file containing the name (Story2.txt), location of the first block (163), and the file size in bytes (714). In our simplistic example, each block is 512 bytes in size, so we'll need two of them. Fortunately, block 164 is right next to the start block and is also free. The system will use the entry for block 163 (the first block of the file) to point to the next block containing it (164). This allows files to occupy discontinuous blocks if the disk is heavily fragmented. That chain of blocks could be quite long if the file was big enough and we didn't run out of disk space first. In our simple example, however, we just need two blocks, so block 164 is the final one in use and gets a special label of EOF to denote the end of the file.

Suppose we decide to delete the file. Instead of cleaning up the table, the FAT file system will simply replace the first character of the filename in the directory table with a reserved character (shown in Figure 5-4 as a question mark) to indicate that the file was deleted. The starting block will be preserved in the directory, but the corresponding entries in the File Allocation Table are zeroed out to show that those blocks are available

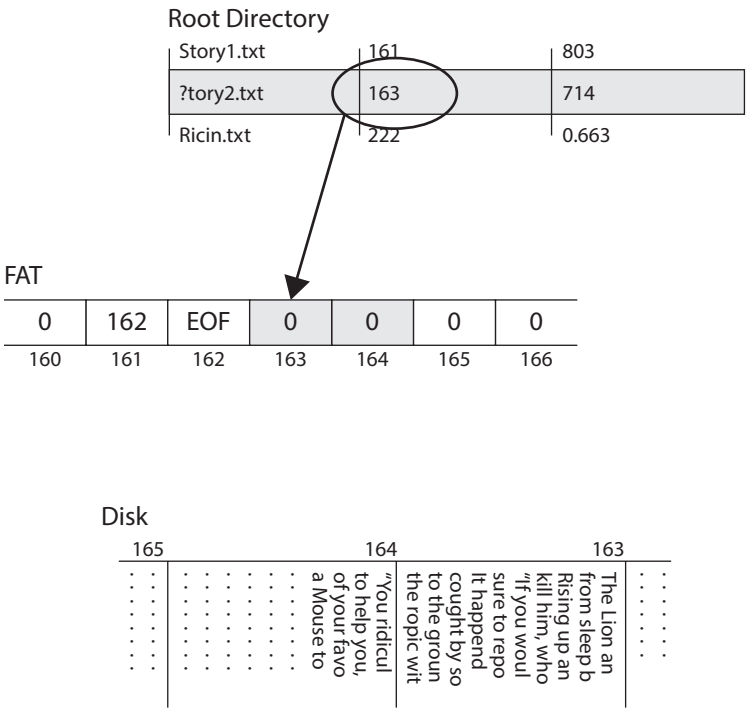


Figure 5-4
Deleting a file

for other files. As you can see in Figure 5-4, the contents of the file on the disk remain intact. This is why data remanence is such a big problem: because file systems almost never securely wipe data when deleting files.

At some point, however, users will create new files and save them to disk, which could result in our original data being partly or completely overwritten. This is shown in Figure 5-5. In this case, the new file requires only one block of disk space because it only contains the text "Hello World!" Suppose the user calls this file "hello.txt" and the system stores it in block 163, which used to be the start block for the previous Story2.txt file. That block will be overwritten with the new file's content and almost certainly padded with empty characters to fill out the block. The next block, however, contains the remainder of the deleted file, so partial contents are still available to anyone with the right recovery tools. Note also that the original file's metadata is preserved in the directory table until that block is needed for another file.

This example, though simplistic, illustrates the process used by almost every file system when creating and deleting files. The data structures may be named differently in modern versions of Windows, Linux, and macOS, but their purpose and behavior remain essentially the same. In fact, many databases use a similar approach to "deleting" entries by simply marking them as deleted without wiping the original data.

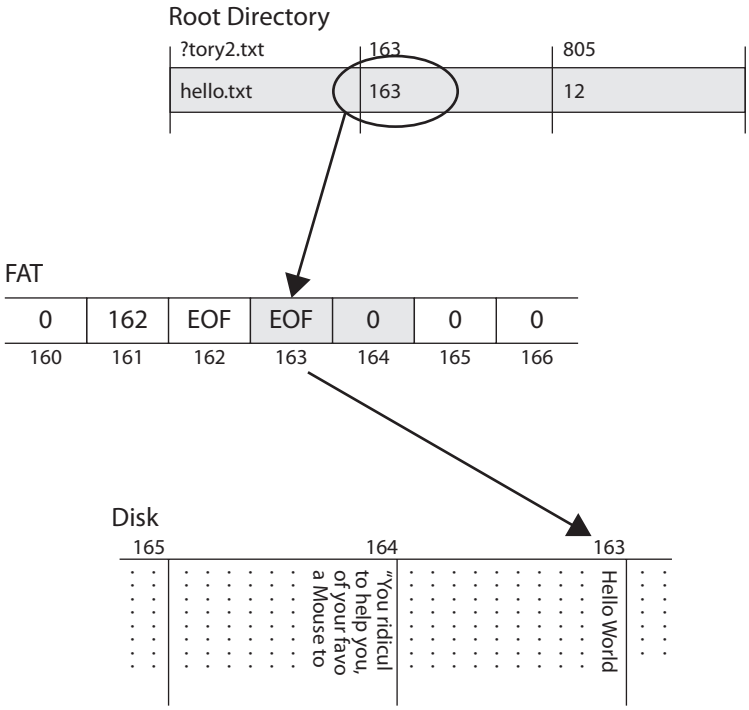


Figure 5-5 Partially overwriting a file

To counter data remanence, it is important to identify procedures for ensuring that private data is properly removed. Generally speaking, there are four approaches to eliminating data remanence:

- **Overwriting** Overwriting data entails replacing the 1's and 0's that represent it on storage media with random or fixed patterns of 1's and 0's in order to render the original data unrecoverable. This should be done at least once (e.g., overwriting the medium with 1's, 0's, or a pattern of these), but may have to be done more than that. For many years the U.S. Department of Defense (DoD) standard 5220.22-M required that media be overwritten seven times. This standard has since been superseded. DoD systems with sensitive information must now be degaussed.
- **Degaussing** This is the process of removing or reducing the magnetic field patterns on conventional disk drives or tapes. In essence, a powerful magnetic force is applied to the media, which results in the wiping of the data and sometimes the destruction of the motors that drive the platters. While it may still be possible to recover the data, it is typically cost prohibitive to do so.
- **Encryption** Many mobile devices take this approach to quickly and securely render data unusable. The premise is that the data is stored on the medium in encrypted format using a strong key. To render the data unrecoverable, the system simply needs to securely delete the encryption key, which is many times faster than deleting the encrypted data. Recovering the data in this scenario is typically computationally infeasible.

- **Physical destruction** Perhaps the best way to combat data remanence is to simply destroy the physical media. The two most commonly used approaches to destroying media are to shred it or expose it to caustic or corrosive chemicals that render it unusable. Another approach is incineration.

Data Roles

The data life cycle and, just as importantly, its protection, is driven by responsible and accountable individuals within each organization. We've already seen how data breaches can wreak havoc on otherwise successful companies and even drive them (or their key leaders) out of business. While this is not an exhaustive list, the following sections describe some of the key responsibilities by role when it comes to protecting data.

Data Controllers

Data controllers decide why and how different types of data will be processed. These are the senior managers that set policies with regard to the management of the data life cycle, particularly with regard to sensitive data such as personal data. Once these controllers set the policy, it is up to the rest of the organization to abide by it.

Data Owners

Data owners are responsible for the life cycle management of a set of data. Among the responsibilities of the data owners are data classification and the approval of disclosure requests. The data owners, therefore, indirectly or directly decide who gets access to specific data. This is particularly important given that these individuals typically are senior managers within the organization. In reality, the majority of these decisions should be codified in formal written policies. Any exceptions to policy should be just that—exceptions—and must be properly documented.

Data Custodians

It is good and well to have policies addressing the life cycle of your data, but someone needs to implement them at the technical level. These individuals are the data custodians, who are responsible for controlling access to the data, implementing the required security controls, and ensuring that both the data and manner in which it is used can be audited. Data custodians also participate in the change management process for all matters pertaining to the data life cycle.

Data Processors

The group of users best positioned to protect (or compromise) data consists of those who deal with that data on a routine basis: *data processors*. These individuals can be found in a variety of places within the organization depending on what particular data is of concern. The critical issue here is that these individuals understand the boundaries of what acceptable behavior is and (just as importantly) know what to do when data is accidentally or intentionally handled in a manner that does not conform to applicable policies. The

best ways to address this issue are through training and auditing. On the one hand, data processors must be properly trained to handle their duties and responsibilities. On the other hand, there must be routine inspections to ensure their behavior complies with all applicable laws, regulations, and policies.

Data Subjects

All personal data concerns a real individual. The person about whom the data is concerned is the data subject. While data subjects are seldom involved in the organizational data life cycle, we all have a solemn duty to protect them and their privacy as we use their data for our own purposes. Respect for the data subjects is foundational to ensuring the protection and privacy of their data.

Chapter Review

Protecting assets, particularly information, is critical to any organization and must be incorporated into the comprehensive risk management process described in Chapter 2. This protection will probably require different controls at different phases in the data life cycle, so it is important to consider phase-specific risks when selecting controls. Rather than trying to protect all information equally, our organizations need classification standards that help us identify, handle, and protect data according to its sensitivity and criticality. We must also consider the roles played by various people in the organization. From the senior executives to the newest and most junior member of the team, everyone who interacts with our information has (and should understand) specific responsibilities with regard to protecting our assets.

A key responsibility is the protection of privacy of personal information. For various legal, regulatory, and operational reasons, we want to limit how long we hold on to personal information. There is no one-size-fits-all approach to data retention, so it is incumbent on the organization's leadership to consider a multitude of factors when developing privacy and data retention policies. These policies, in turn, should drive risk-based controls, baselines, and standards applied to the protection of our data. A key element in applying controls needs to be the proper use of strong cryptography.

Quick Review

- Data goes through a life cycle that starts with its acquisition and ends with its disposal.
- Each phase of the data life cycle requires different considerations when assessing risks and selecting controls.
- New information is prepared for use by adding metadata, including classification labels.

- Ensuring the consistency of data must be a deliberate process in organizations that use data replication.
- Cryptography can be an effective control at all phases of the data life cycle.
- The data retention policy drives the timeframe at which data transitions from the archival phase to the disposal phase of its life cycle.
- Information classification corresponds to the information's value to the organization.
- Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed.
- Senior executives are ultimately responsible to the shareholders for the successes and failures of their corporations, including security issues.
- The data owner is the manager in charge of a specific business unit and is ultimately responsible for the protection and use of a specific subset of information.
- Data owners specify the classification of data, and data custodians implement and maintain controls to enforce the set classification levels.
- The data retention policy must consider legal, regulatory, and operational requirements.
- The data retention policy should address what data is to be retained, where, how, and for how long.
- Electronic discovery (e-discovery) is the process of producing for a court or external attorney all electronically stored information (ESI) pertinent to a legal proceeding.
- Normal deletion of a file does not permanently remove it from media.
- NIST SP 800-88, Revision 1, *Guidelines for Media Sanitization*, describes the best practices for combating data remanence.
- Overwriting data entails replacing the 1's and 0's that represent it on storage media with random or fixed patterns of 1's and 0's to render the original data unrecoverable.
- Degaussing is the process of removing or reducing the magnetic field patterns on conventional disk drives or tapes.
- Privacy pertains to personal information, both from your employees and your customers.
- Generally speaking, organizations should collect the least amount of private personal data required for the performance of their business functions.
- Mobile devices are easily lost or stolen and should proactively be configured to mitigate the risks of data loss or leakage.
- Paper products oftentimes contain information that deserves controls commensurate to the sensitivity and criticality of that information.

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 statements is true about the data life cycle?
   - **A.** The data life cycle begins with its archival and ends with its classification.
   - **B.** Most data must be retained indefinitely.
   - **C.** The data life cycle begins with its acquisition/creation and ends with its disposal/destruction.
   - **D.** Preparing data for use does not typically involve adding metadata to it.
2. Ensuring data consistency is important for all the following reasons, *except*
   - **A.** Replicated data sets can become desynchronized.
   - **B.** Multiple data items are commonly needed to perform a transaction.
   - **C.** Data may exist in multiple locations within our information systems.
   - **D.** Multiple users could attempt to modify data simultaneously.
3. Which of the following makes the most sense for a single organization's classification levels for data?
   - **A.** Unclassified, Secret, Top Secret
   - **B.** Public, Releasable, Unclassified
   - **C.** Sensitive, Controlled unclassified information (CUI), Proprietary
   - **D.** Proprietary, Trade Secret, Private
4. Which of the following is the most important criterion in determining the classification of data?
   - **A.** The level of damage that could be caused if the data were disclosed
   - **B.** The likelihood that the data will be accidentally or maliciously disclosed
   - **C.** Regulatory requirements in jurisdictions within which the organization is not operating
   - **D.** The cost of implementing controls for the data
5. Who bears ultimate responsibility for the protection of assets within the organization?
   - **A.** Data owners
   - **B.** Cyber insurance providers
   - **C.** Senior management
   - **D.** Security professionals

6. During which phase or phases of the data life cycle can cryptography be an effective control?
   - **A.** Use
   - **B.** Archival
   - **C.** Disposal
   - **D.** All the above
7. A transition into the disposal phase of the data life cycle is most commonly triggered by
   - **A.** Senior management
   - **B.** Insufficient storage
   - **C.** Acceptable use policies
   - **D.** Data retention policies
8. Information classification is most closely related to which of the following?
   - **A.** The source of the information
   - **B.** The information's destination
   - **C.** The information's value
   - **D.** The information's age
9. The data owner is most often described by all of the following *except*
   - **A.** Manager in charge of a business unit
   - **B.** Ultimately responsible for the protection of the data
   - **C.** Financially liable for the loss of the data
   - **D.** Ultimately responsible for the use of the data
10. Who has the primary responsibility of determining the classification level for information?
    - **A.** The functional manager
    - **B.** Senior management
    - **C.** The owner
    - **D.** The user
11. If different user groups with different security access levels need to access the same information, which of the following actions should management take?
    - **A.** Decrease the security level on the information to ensure accessibility and usability of the information.
    - **B.** Require specific written approval each time an individual needs to access the information.
    - **C.** Increase the security controls on the information.
    - **D.** Decrease the classification label on the information.

12. What should management consider the most when classifying data?

- **A.** The type of employees, contractors, and customers who will be accessing the data
- **B.** Availability, integrity, and confidentiality
- **C.** Assessing the risk level and disabling countermeasures
- **D.** The access controls that will be protecting the data

13. Which of the following requirements should the data retention policy address?

- **A.** Legal
- **B.** Regulatory
- **C.** Operational
- **D.** All the above

14. Which of the following is *not* addressed by the data retention policy?

- **A.** What data to keep
- **B.** For whom data is kept
- **C.** How long data is kept
- **D.** Where data is kept

15. Which of the following best describes the mitigation of data remanence by a physical destruction process?

- **A.** Replacing the 1's and 0's that represent data on storage media with random or fixed patterns of 1's and 0's
- **B.** Converting the 1's and 0's that represent data with the output of a cryptographic function
- **C.** Removing or reducing the magnetic field patterns on conventional disk drives or tapes
- **D.** Exposing storage media to caustic or corrosive chemicals that render it unusable

16. Which of the following best describes the mitigation of data remanence by a degaussing destruction process?

- **A.** Replacing the 1's and 0's that represent data on storage media with random or fixed patterns of 1's and 0's
- **B.** Converting the 1's and 0's that represent data with the output of a cryptographic function
- **C.** Removing or reducing the magnetic field patterns on conventional disk drives or tapes
- **D.** Exposing storage media to caustic or corrosive chemicals that render it unusable

17. Which of the following best describes the mitigation of data remanence by an overwriting process?
    - **A.** Replacing the 1's and 0's that represent data on storage media with random or fixed patterns of 1's and 0's
    - **B.** Converting the 1's and 0's that represent data with the output of a cryptographic function
    - **C.** Removing or reducing the magnetic field patterns on conventional disk drives or tapes
    - **D.** Exposing storage media to caustic or corrosive chemicals that render it unusable

Answers

1. **C.** Although various data life-cycle models exist, they all begin with the creation or acquisition of the data and end with its ultimate disposal (typically destruction).
2. **B.** Although it is typically true that multiple data items are needed for a transaction, this has much less to do with the need for data consistency than do the other three options. Consistency is important because we oftentimes keep multiple copies of a given data item.
3. **A.** This is a typical set of classification levels for government and military organizations. Each of the other options has at least two terms that are synonymous or nearly synonymous.
4. **A.** There are many criteria for classifying data, but it is most important to focus on the value of the data or the potential loss from its disclosure. The likelihood of disclosure, irrelevant jurisdictions, and cost considerations should not be central to the classification process.
5. **C.** Senior management always carries the ultimate responsibility for the organization.
6. **D.** Cryptography can be an effective control at every phase in the data life cycle. During data acquisition, a cryptographic hash can certify its integrity. When sensitive data is in use or in archives, encryption can protect it from unauthorized access. Finally, encryption can be an effective means of destroying the data.
7. **D.** Data retention policies should be the primary reason for the disposal of most of our information. Senior management or lack of resources should seldom, if ever, be the reason we dispose of data, while acceptable use policies have little, if anything, to do with it.
8. **C.** Information classification is very strongly related to the information's value and/or risk. For instance, trade secrets that are the key to a business's success are highly valuable, which will lead to a higher classification level. Similarly, information that could severely damage a company's reputation presents a high level of risk and is similarly classified at a higher level.

9. **C.** The data owner is the manager in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. In most situations, this person is not financially liable for the loss of his or her data.
10. **C.** A company can have one specific data owner or different data owners who have been delegated the responsibility of protecting specific sets of data. One of the responsibilities that goes into protecting this information is properly classifying it.
11. **C.** If data is going to be available to a wide range of people, more granular security should be implemented to ensure that only the necessary people access the data and that the operations they carry out are controlled. The security implemented can come in the form of authentication and authorization technologies, encryption, and specific access control mechanisms.
12. **B.** The best answer to this question is B, because to properly classify data, the data owner must evaluate the availability, integrity, and confidentiality requirements of the data. Once this evaluation is done, it will dictate which employees, contractors, and users can access the data, which is expressed in answer A. This assessment will also help determine the controls that should be put into place.
13. **D.** The data retention policy should follow the laws of any jurisdiction within which the organization's data resides. It must similarly comply with any regulatory requirements. Finally, the policy must address the organization's operational requirements.
14. **B.** The data retention policy should address what data to keep, where to keep it, how to store it, and for how long to keep it. The policy is not concerned with "for whom" the data is kept.
15. **D.** Two of the most common approaches to destroying data physically involve shredding the storage media or exposing it to corrosive or caustic chemicals. In certain highly sensitive government organizations, these approaches are used in tandem to make the risk of data remanence negligible.
16. **C.** Degaussing is typically accomplished by exposing magnetic media (such as hard disk drives or magnetic tapes) to powerful magnetic fields in order to change the orientation of the particles that physically represent 1's and 0's.
17. **A.** Data remanence can be mitigated by overwriting every bit on the storage medium. This is normally accomplished by writing all 0's, or all 1's, or a fixed pattern of them, or a random sequence of them. Better results can be obtained by repeating the process with different patterns multiple times.

This page intentionally left blank

CHAPTER 6

Data Security

This chapter presents the following:

- Data states
- Data security controls
- Data protection methods

Data is a precious thing and will last longer than the systems themselves.

—Tim Berners-Lee

Having addressed assets in general in the previous chapter, we now turn our attention to specific ways in which we go about protecting one of our most precious assets: data. One of the facts that makes securing data so difficult is that it can seemingly flow and rest anywhere in the world, literally. Even that virtual sticky note on your home computer's desktop reminding you to pick up some milk can be backed up automatically and its contents stored almost anywhere in the world unless you take steps to control it. The same issue arises, though with more significant consequences, when we consider data in our organizations' IT systems.

Clearly, the manner in which we protect our data depends on where it is and what it is doing (or having done to it). That sticky note on your desktop has different security implications than a confidential message being transmitted between two government organizations. Part of the decision deals with the data classification we discussed in Chapter 5, but another part deals with whether the data is just sitting somewhere, moving between places, or actively being worked on. These are the data states, and they determine what security controls make sense over time.

Data Security Controls

As described in Chapter 5, which types of controls should be implemented per classification depends upon the level of protection that management and the security team have determined is needed. The numerous types of controls available are discussed throughout this book. But some considerations pertaining to sensitive data and applications are common across most organizations:

- Strict and granular access control for all levels of sensitive data and programs
- Encryption of data while stored and while in transit

- Auditing and monitoring (determine what level of auditing is required and how long logs are to be retained)
- Separation of duties (determine whether two or more people must be involved in accessing sensitive information to protect against fraudulent activities; if so, define and document procedures)
- Periodic reviews (review classification levels, and the data and programs that adhere to them, to ensure they are still in alignment with business needs; data or applications may also need to be reclassified or declassified, depending upon the situation)
- Backup and recovery procedures (define and document)
- Change control procedures (define and document)
- Physical security protection (define and document)
- Information flow channels (where does the sensitive data reside and how does it traverse the network)
- Proper disposal actions, such as shredding, degaussing, and so on (define and document)
- Marking, labeling, and handling procedures

Clearly, this is not an exhaustive list. Still, it should be a good start as you delve into whatever specific compliance requirements apply to your organization. Keep in mind that the controls that constitute adequate data protections vary greatly between jurisdictions. When it comes to compliance, always be sure to consult your legal counsel.

Data States

Which controls we choose to use to mitigate risks to our information depend not only on the value we assign to that information but also on the dynamic state of that information. Generally speaking, data exists in one of three states: at rest, in motion, or in use. These states and their interrelations are shown in Figure 6-1. The risks to each state are different in significant ways, as described next.

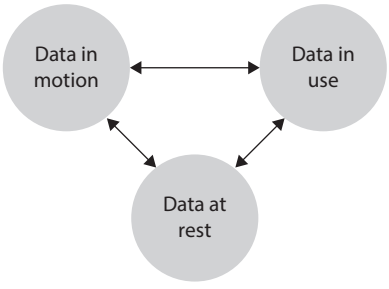


Figure 6-1
The states of data

Data at Rest

Information in an information system spends most of its time waiting to be used. The term *data at rest* refers to data that resides in external or auxiliary storage devices, such as hard disk drives (HDDs), solid-state drives (SSDs), optical discs (CD/DVD), or even on magnetic tape. A challenge with protecting data in this state is that it is vulnerable, not only to threat actors attempting to reach it over our systems and networks but also to anyone who can gain physical access to the device. It is not uncommon to hear of data breaches caused by laptops or mobile devices being stolen. In fact, one of the largest personal health information (PHI) breaches occurred in San Antonio, Texas, in September 2009 when an employee left unattended in his car backup tapes containing PHI on some 4.9 million patients. A thief broke into the vehicle and made off with the data. The solution to protecting data in such scenarios is as simple as it is ubiquitous: encryption.

Every major operating system now provides means to encrypt individual files or entire volumes in a way that is almost completely transparent to the user. Third-party software is also available to encrypt compressed files or perform whole-disk encryption. What's more, the current state of processor power means that there is no noticeable decrease in the performance of computers that use encryption to protect their data. Unfortunately, encryption is not yet the default configuration in any major operation system. The process of enabling it, however, is so simple that it borders on the trivial.

Many medium and large organizations now have policies that require certain information to be encrypted whenever it is stored in an information system. While typically this applies to PII, PHI, or other regulated information, some organizations are taking the proactive step of requiring whole-disk encryption to be used on all portable computing devices such as laptops and external hard drives. Beyond what are clearly easily pilfered devices, we should also consider computers we don't normally think of as mobile. Another major breach of PHI was reported by Sutter Health of California in 2011 when a thief broke a window and stole a desktop computer containing the unencrypted records on more than 4 million patients. We should resolve to encrypt all data being stored anywhere, and modern technology makes this easier than ever. This approach to "encrypt everywhere" reduces the risk of users accidentally storing sensitive information in unencrypted volumes.

NOTE NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, provides a good, if somewhat dated (2007), approach to this topic.

Data in Motion

Data in motion is data that is moving between computing nodes over a data network such as the Internet. This is perhaps the riskiest time for our data: when it leaves the confines of our protected enclaves and ventures into that Wild West that is the Internet. Fortunately, encryption once again rises to the challenge. The single best protection for our data while it is in motion (whether within or without our protected networks) is strong encryption such as that offered by Transport Layer Security (TLS version 1.2 and later)

or IPSec. We will discuss strong (and weak) encryption in Chapter 8, but for now you should be aware that TLS and IPSec support multiple cipher suites and that some of these are not as strong as others. Weaknesses typically are caused by attempts to ensure backward compatibility, but result in unnecessary (or perhaps unknown) risks.

NOTE The terms data in motion, data in transit, and data in flight are all used interchangeably.

By and large, TLS relies on digital certificates (more on those in Chapter 8) to certify the identity of one or both endpoints. Typically, the server uses a certificate but the client doesn't. This one-way authentication can be problematic because it relies on the user to detect a potential impostor. A common exploit for this vulnerability is known as a man-in-the-middle (MitM) attack. The attacker intercepts the request from the client to the server and impersonates the server, pretending to be, say, Facebook. The attacker presents to the client a fake web page that looks exactly like Facebook and requests the user's credentials. Once the user provides that information, the attacker can forward the log-in request to Facebook and then continue to relay information back and forth between the client and the server over secure connections, intercepting all traffic in the process. A savvy client would detect this by noticing that the web browser reports a problem with the server's certificate. (It is extremely difficult for all but certain nation-states to spoof a legitimate certificate.) Most users, however, simply click through any such warnings without thinking of the consequences. This tendency to ignore the warnings underscores the importance of security awareness in our overall efforts to protect our information and systems.

Another approach to protecting our data in motion is to use trusted channels between critical nodes. Virtual private networks (VPNs) are frequently used to provide secure connections between remote users and corporate resources. VPNs are also used to securely connect campuses or other nodes that are physically distant from each other. The trusted channels we thus create allow secure communications over shared or untrusted network infrastructure.

Data in Use

Data in use is the term for data residing in primary storage devices, such as volatile memory (e.g., RAM), memory caches, or CPU registers. Typically, data remains in primary storage for short periods of time while a process is using it. Note, however, that anything stored in volatile memory could persist there for extended periods (until power is shut down) in some cases. The point is that data in use is being touched by the CPU or ALU in the computer system and will eventually go back to being data at rest, or end up being deleted.

As discussed earlier, data at rest should be encrypted. The challenge is that, in most operating systems today, the data must be decrypted before it is used. In other words, data in use generally cannot be protected by encrypting it. Many people think this is safe, the thought process being, "If I'm encrypting my data at rest and in transit already,