When designing and implementing the information security and privacy program described in Chapters 4 and 5, it is critical to benchmark against the best practices in this discipline. Best practices should be understood as the minimum aspirations for an organization’s policies, procedures, and controls. Due to the unique requirements of individual organizations and their differing geographies, industries, and clients, no one set of best practices will govern the ultimate selections by any organization. But any variances from accepted best practices should be justified and documented. This chapter begins with some best practices that should be appropriate for almost any organization’s information security and privacy policies. It then discusses in more detail a best practice approach to responding to a data breach, including working with external resources. After the best practice policies and controls have been implemented, their effectiveness must be assessed and reported to external stakeholders. So the final section of the chapter discusses information security, privacy, and website audits and certifications.

**What Global Executives Need to Know**

- How the organization’s information security and privacy policies compare to best practices
- The compliance of the organization’s website privacy policies with the statutes and regulations in all countries where the organization has customers
- The organization’s plan to respond to data breach in all locations where it collects, uses, or stores personal data
- The types of information security and privacy audits the organization undergoes and the key findings from these reports
- The status of the organization’s pursuit of information security and privacy certifications and trustmarks
6.1 INFORMATION SECURITY AND PRIVACY POLICIES

The policies listed in this section illustrate many of the key provisions in best practice information security and privacy policies. The direction set by these policies will lead to the controls covered in depth in Chapter 5. As such, the policies related to some of those controls will not be repeated here, but can be easily abstracted from the discussion in the previous chapter. Although stated as separate policies in this discussion, for documentation, presentation, and training purposes, these policies may be consolidated into a single information security and privacy policy, with many subpolicies included.

A. Policies Involving Business Judgment

These information security and privacy policies require significant input from senior leadership of the organization. The nature and implementation of these policies may vary radically from one organization to another. Decisions on the most appropriate design of these policies will involve input from a variety of departments and require executive oversight to ensure organization-wide acceptance and follow-through.

1. Top-Level Information Security and Privacy Policy

The purpose of a written information security and privacy policy is to demonstrate the organization’s commitment to information security and privacy. The policy therefore not only should be approved by the highest-level leadership possible but must be communicated and practiced from the top. It must apply to all members of the organization, including all those external parties who interact with the organization. An individual should be designated to head the organization’s information security and privacy efforts. This individual must be empowered to make decisions quickly when necessary to safeguard systems or data. This policy should articulate the complexity of information security and privacy and the need for all policy-level changes to be vetted by legal counsel. The policy should be reviewed on a regular basis—no less than annually—and revised accordingly.

The policy should also describe the roles of the various stakeholders in the information security and privacy program. These stakeholders include executive management, the owners of information, the users of information, the business departments, internal audit, and the information security and privacy departments. Executive management must meet regularly to review the state of information security and privacy in the organization, make decisions about any identified information security and privacy risks, and allocate sufficient resources to be able to carry out these responsibilities.

2. Risk Management Program

All organizations must adopt a risk management program, as described in Chapter 4. The goal of the risk management program is to provide the information necessary for the organization’s leadership to make the business decisions necessary to reduce risk. In short, the program identifies and quantifies those risks faced by the organization and provides cost-benefit analysis of potential mitigation options. A risk-management program provides the risk-weighted analysis upon which to base risk reduction, retention, transfer/sharing, and avoidance decisions.
3. **Acceptable Use Policy**

An acceptable use policy provides guidance to employees and leaders by outlining how the organization’s information systems are to be used, in the workplace and remotely. The policy should also specifically describe which uses are strictly prohibited. A typical acceptable use policy will state that information systems provided by the company (1) shall be used only for business purposes; (2) shall not be used to harass, discriminate against, or defame others; (3) shall not be accessed by unauthorized persons; (4) shall not be used to access pornographic material; and (5) shall not be used to violate or aid in the violation of intellectual property rights.

The recent Supreme Court decision on the use of an organization’s information devices by its public sector employees should provide employers with sufficient foundation to perform reasonable audits covering the use of corporate assets by employees but in all cases organizations should make it clear in their written policies and in awareness training that is the organization’s intent to monitor and audit their employees’ use of all corporate information assets.¹

Acceptable use policies should not be overly restrictive, as this can create problems, and should therefore be approached pragmatically. As employees are expected to abide by such policies, a clear distinction must be made between productivity and security measures. It should also be made clear that the objective is risk-weighted security, not simply employee monitoring. Personal uses such as web surfing, even when performed on an employee’s personal time, can open computer systems to innumerable Internet-based threats. Where an organization does allow personal use of an organization’s information assets, employees should be provided with appropriate tools and training to ensure that all such use is performed under appropriate safeguards.

Acceptable use policies must address use of the Internet, including the downloading of files and all types of software (nonapproved and approved) and the proper usage of company and external blogs, use of the organization’s e-mail and other communication systems, use of personal e-mail systems from work locations or on work equipment, access to inappropriate or disallowed websites, and the use of social networking and messaging services. While the employee’s access to these services may utilize a personal account, if done on corporate equipment or corporate time or if it can be linked back to the organization, then express limits must be stated and disseminated to all users.

Restrictive acceptable use policies should not be undertaken lightly. Many employees, particularly tech-savvy young employees, will react negatively to limitations on how they communicate. A boilerplate “no personal use” policy is rarely effective and often foments an “us versus them” culture whereby employees take steps to hide evidence of personal uses. The adoption of liberal, flexible, acceptable policies is therefore a defensible business decision.

4. **Access Compartmentalization**

No person should be given access to sensitive data or information systems beyond that needed for his or her role. Strictly hierarchical access-granting structures should

---

¹ City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (June 2010).
be avoided, as seniority within an organization does not warrant greater access. Lateral compartmentalization protects systems from accidental interference by unqualified persons and reduces the damage done if security devices such as encryption keys fall into the wrong hands. This policy even applies to executives operating outside their organizational responsibilities.

The scope of an employee’s clearance should be defined by his or her day-to-day needs, not by the theoretical limits of that employee’s job description. For example, an employee may on occasion make emergency repairs to a critical system. The employee would of course need access to that system, but this temporary need does not mean that the employee requires 24/7 access. When the occasional emergency occurs, the employee can then be granted temporary access or be directly supervised as a guest.

Guests, if they are to be given access to organization resources, should never be allowed access to sensitive information, and their access should always be granted with a preset termination date.

5. Communications Monitoring Policy

Organizations must decide whether they have a business interest in monitoring electronic communications. Communications monitoring, particularly of customer communications, may also have negative business consequences. A hotel might provide Internet access to patrons, but many patrons would react negatively to warnings that the websites they visit while in their rooms were being monitored. The technological systems for monitoring can themselves be subject to abuse, particularly by those wishing to blackmail or spy upon others. Use of the monitoring system must therefore itself be subject to monitoring. Given these complexities, organizations must carefully decide whether they have an actual business interest in the adoption of a monitoring policy.

Communications monitoring may run afoul of wiretap legislation (discussed in Chapter 3). Other safe harbor legislation may also protect organizations from liability where they choose not to engage in monitoring. Organizations must therefore consult legal counsel regarding any changes to communications monitoring policies.

The communications monitoring policy ensures that users realize and affirm that communications via company equipment may be monitored. Organizations should adopt such a policy regardless of whether they presently engage in active monitoring.

If an organization has a business need to monitor e-mail or other forms of digital communication, it must clearly disclose to employees, business partners, customers, and other communicators who access the organization’s equipment that such access constitutes express consent to monitoring. This policy must be outlined and disclosed to the user prior to use of the equipment. The user should be required to acknowledge that he or she is aware of any monitoring policy prior to accessing the equipment, and such acknowledgment should be recorded if possible.

Although communication equipment and the electronic data generated by or stored within that equipment are generally considered the property of the organization, various statutes prohibit the monitoring of wire and electronic communications unless some exception applies. Consequently, an employer generally may not monitor the use of the equipment, including e-mail, unless it does so to protect an organization’s assets or
obtains the consent of the individual parties to such communications. The statutes are discussed in Chapter 2.

Monitoring can take many forms, but may involve verbatim recording of communications. This action presents privacy and security concerns. Access to intercepted communications must be restricted to a similar degree as the communications themselves. For instance, allowing IT auditors to intercept communications involving the organization’s legal counsel may impact attorney-client privilege. It may be that some intercepted activity, particularly communications either to or from an attorney, should never be subject to verbatim monitoring.

6. Breach Reporting

Security breaches must be planned for. Employees should be encouraged to report any unusual activity, regardless of whether they believe a breach has occurred. Something as innocuous as a sluggish computer may be evidence of a major security breach. There are three forms of breach, each requiring a different protocol:

- **Breaks from policy or established routine:** Such events are the lowest form of breach and may or may not present a security risk. Leaders should note them and, where appropriate, pass the information along to the risk management team for further evaluation. Any incident involving sensitive data must be reported.

- **Detected breaches:** Any incident involving unauthorized access to information systems containing sensitive data, or any other breach of security protocols, must be reported to both risk management and legal counsel. Risk management will determine the extent of the breach, and legal counsel whether breach notification obligations have been triggered.

- **Potential vulnerabilities or undetectable breaches of system security:** An undetectable breach is one that, if it had occurred in the past, would not have been detected. So-called zero-day vulnerabilities (discussed in Chapter 4) are typical in that while the vulnerability has existed for some time, it has only recently become known to the organization. All such vulnerabilities require immediate investigation by the risk management team, regardless of whether any actual breach has been detected. The risk management team will then report its findings to both legal counsel and leadership.

Response to data breach is discussed in more detail later in this chapter.

7. Outsourcing

Before outsourcing any activity involving sensitive information, organizations must consult qualified legal counsel. Many jurisdictions now regulate how organizations handle personal and sensitive information. Regardless of legal obligations, every organization considering outsourcing should ensure that the contracted provider enforces equivalently robust security policies and practices. Any agreement should carefully delineate responsibilities, risks, and liabilities borne by the organization and those borne by the service provider. Organizations should strive to monitor and supervise the provider’s personnel and periodically audit the provider’s performance. The organization should maintain contingency plans in the event that the provider is no longer able to perform.
“Equivalently robust” requires line-item comparison of the information security and privacy policies. The two organizations may have equivalent general policies and may even be certified by the same organizations, but that is not enough. The outside organization must maintain equivalent or higher standards in every respect. Any deficiency in the external organization, should it result in a breach, will defeat any notion of equivalence. If the organization has determined that 256-bit encryption is the required minimum for its data, outsourcing to an external organization using 128-bit encryption would increase its risk, regardless of whether 128-bit encryption would normally be considered sufficient. Each standard and control utilized by the external organization must be clearly understood.

Outsourcing, especially to vendors operating outside the organization’s country, introduces new security issues. The movement of data to and from the external organization will normally occur via the Internet, necessitating encryption. The external organization may be subject to a very different legal regime in the other country. Many governments are not burdened by the same warrant requirements prior to accessing electronic information as may be used domestically. Intellectual property and contract rights also differ greatly around the globe. Additionally, any information regarding governments, defense, or other high technology may be subject to export limitations. Therefore legal counsel, including international legal counsel, must be consulted prior to the outsourcing of any sensitive information across national boundaries.

8. **Document Retention**

An effective document retention policy (DRP) will address which documents need to be retained, the purpose for which they are to be retained, and stated retention periods. The DRP should also outline a system for identifying whether any alterations have been made to a document, including any associated metadata, while in storage. If changes are to be permitted, the DRP should describe who is permitted to make such changes and outline a method to record what, how, and when changes are made. Normally this verification is accomplished through a combination of digital signatures and hashing. The DRP should describe a method and schedule for the effective destruction of documents that need no longer be retained. Such documents should be destroyed as soon as practicable. Permanent storage should be considered only where required by law, regulations, or other rules governing the organization.

9. **Other**

A policy should describe how change control is practiced in all aspects of the organization’s hardware, software, and network resources, including those done by third-party providers. The software development lifecycle and the promotion process must also be described in a policy. The separation of duties must be shown between those with the ability to change applications and systems and those who own and act as custodians for data. No developer or systems administrator should have the ability to initiate and approve his or her own changes into production. And commitment to third-party verifications, such as external information security audits and network and application penetration testing and vulnerability analyses, should be part of the organization’s policy.
6.1 Information Security and Privacy Policies

B. Technical Policies

Technical policies cover areas that, while still important, are more technical in nature. The specifics of each will be less a matter of business judgment and more of technological expertise. Senior leadership must still oversee and approve these policies, but will normally rely on expert opinion as to their design, implementation, and effectiveness.

1. Encryption

The proper use of encryption technology is a cornerstone of information security. Encryption protects data from being read by unauthorized persons. Many organizations are subject to legal or contractual requirements that certain data remain encrypted. Above and beyond these, an organization’s encryption policy should demand that all data be encrypted whenever possible. The policy should address three distinct areas:

- **Data at rest**: Data that is stored on media is considered “at rest” in that it is not moving through a network. This data should always be encrypted in a manner that protects it should the media containing it be lost or stolen.

- **Data in transit**: Data or other communications moving across a network must remain properly encrypted if the network through which it moves is in any way accessible by persons not authorized to read the data. All sensitive information transitioning the Internet must be encrypted.

- **Data in use**: There are times when data simply cannot be encrypted. Data displayed on a computer screen or on printed paper cannot be encrypted and simultaneously be readable. Similarly, data stored on Random Access Memory modules with computer systems cannot be easily encrypted. The encryption policy should anticipate these situations. Encryption cannot answer every security threat. It may be necessary that some data never be displayed outside a physically secured environment.

The appropriate method of encryption will depend on the circumstances. See Chapter 5 for an in-depth discussion of which method to use in each circumstance.

2. Wireless Communications

Given the increasing prevalence of mobile devices, all organizations must adopt a wireless communications policy regardless of whether they plan on using wireless technology. All communications transitioning to a wireless connection must be treated as transitioning to a publicly accessible medium. Communications containing sensitive information must therefore be encrypted, but the risk of eavesdropping is so great that all wireless communications should probably be encrypted.

All wireless transmissions that may contain sensitive information should, over and above TLS, be encrypted via Wi-Fi Protected Access 2.0 (WPA2) or better. Wired Equivalent Privacy (WEP) should not be used under any circumstances, as it is an easy target for cracking. The encryption keys used should be treated as the most important passwords. They should be computationally very complex (16 characters or more), subject to extensive wordlist testing, and changed monthly.
All employees using wireless technologies must be trained in their safe use. Where public wireless networks are used (i.e., the cellular networks) it may not be possible to implement wanted encryption protocols. Employees must recognize such situations and restrict their activities appropriately.

3. Password Policy
Memorized passwords are by far the most common method of authentication used. Organizations should adopt a password policy suited to their particular security needs and the attacks to which the password may be subject. Longer passwords using a wider range of characters are computationally more complex and are therefore less subject to guessing, “brute force,” or dictionary attacks. They are therefore considered more secure, but complex passwords are more difficult for humans to remember. Passwords that are too short are insecure, too long and users start writing them down on notepads which are eventually lost or stolen, defeating the purpose of the password.

Passwords should be altered periodically. This alteration will reduce the useful life of any copied or stolen password but if done too often will cause users to either simplify their passwords or write them down. Organizations should realize that a compromised password will be misused within hours if not minutes. Forcing users to renew their passwords on even a daily basis will not prevent this. The renewal period should therefore be based on the password’s susceptibility to attack or theft and the importance of the authentication for which it is used. Renewal of important passwords should require authorization from multiple persons.

All new passwords should be checked against lists of commonly used passwords. Many such wordlists are available commercially. A good list will contain hundreds of millions of words.

4. Authentication of Persons
There is no single best practice for authentication of persons. The degree of rigor applied to any particular authentication should vary depending on the nature of the privileges granted by that authentication. For instance, an authentication procedure prior to permitting a person access to sensitive customer information should be more rigorous than that used in deciding whether to allow access to the company cafeteria. Organizations should establish specific written policies outlining both general procedures and specific requirements for access to crucial systems or information.

There are three primary methods of authenticating physical persons:

- **Something they know**, typically a secret password.
- **Something they have** or an object they possess, such as an employee badge or security token. The reliability of this method depends on the reliability of the authentication process prior to the issuance of the object and the chances that the object has been copied or stolen.
- **Something they are** or a physical measurement (e.g., a fingerprint). Often referred to as “biometrics,” this form of authentication runs the gamut from the ability of a security guard to recognize a face to an electronic scan of the person’s retinal blood vessels.
The three approaches are normally combined. For access to critical systems or locations, a person may have a password, a smart card or other token, and an employee badge with a picture. But no matter how many credentials are used, they are no more reliable than the process behind them. Therefore it is vitally important to thoroughly vet everyone prior to issuing them any sort of security credential. See Chapter 5 for an in-depth discussion of authentication.

5. Authentication of Network Actors or Information Systems

Authentication of persons within computer networks presents unique difficulties. Without face-to-face interaction, persons must be identified via possession of passwords, codes, or other data. Biometrics aren’t a realistic option, but cryptographic tokens such as smart cards are still useful. The greater challenge is authentication of nonhuman network actors. Websites and other network locations can be faked or “spoofed” in an effort to acquire sensitive information.

The answer to this problem involves third-party authentication via digital certificates. Certificates are digital tokens that allow their holder to prove that it is what it claims to be. For instance, a bank’s website will have a certificate issued to that bank by a certificate authority whose digital signature is integrated into the certificate. Those accessing the website can trust that the website is under the control of the bank because they trust the certificate authority. In such situations the user’s web browser software will indicate that the connection is both trusted and encrypted. The entire system has been integrated into the TLS cryptographic standard. Any transmission of sensitive information between systems across a public network should utilize TLS or a similar certificate-based protocol. Organizations should also outline which certificate authorities are to be trusted and ensure that their systems are configured appropriately.

6. Authentication of Electronic Communications

As with persons, data itself must be authenticated prior to being allowed access to information systems. The standard technique involves the use of digital signatures. These tools, through the cryptographic methods discussed in Chapter 5, allow the recipient of data to verify the identity of the sender and detect whether the data has been altered in transit. All important data, even if not encrypted, should be accompanied by a digital signature. This is especially true for e-mail. All employees using e-mail or similar methods should be trained in the safe use of digital signatures.

7. Disaster Recovery Policies

Disaster recovery and business continuity policies should be broad enough to encompass any number of disasters that might realistically befall the organization, from natural disasters that may physically destroy equipment to denial-of-service attacks that may restrict access to networks. These policies should include measures to ensure that crucial information is backed up on alternative equipment, preferably off-site, so that business may continue despite the loss of one facility or set of equipment.

Disasters take many forms. Natural disasters are one, but more common are criminal actions or widespread hardware failures. Disaster and continuity plans are equally useful if an office is robbed of equipment or if the cooling system for the server room fails. A com-
plete plan will also anticipate software failures such new zero-day vulnerabilities that can render software temporarily unreliable. Well-prepared organizations should be capable of moving to alternative software platforms as easily as they move to alternative hardware.

Disaster recovery policies should also anticipate the need to quickly abandon facilities. Floodwaters can rise in a matter of hours, and security guards cannot be expected to remain at their stations. In such situations, systems must be in place to remove, encrypt, or even destroy sensitive information prior to abandonment.

8. **Employee Termination**

Organizations must establish procedures to ensure that terminated employees have no access to secure information or secure areas. They should return all keys, access devices, and other tokens permitting access to physical locations or computer systems. Any user accounts and passwords for network access should be disabled. Organizations should also secure the return of critical property given to terminated employees, such as laptops.

Once the decision to terminate an employee has been made, the organization should move quickly to terminate the employee’s access to critical or sensitive information prior to the employee learning of his or her termination. The former employee should then be treated as a guest. All further access to information systems, such as to retrieve personal files, should be strictly supervised. All memory devices, especially flash drives, should be either inspected or destroyed prior to leaving with the employee.

These procedures are equally applicable to the termination of business relationships with business partners, customers, contractors, or any other third parties who may have access to information systems.

9. **Intrusion Detection**

Organizations should make use of and maintain intrusion detection systems, network-monitoring software, and security assessment tools to detect attempts to penetrate the organization’s networks. Organizations can either employ qualified personnel or outsource the process to a qualified security firm. The best approach is to do both.

Once an intrusion is detected, the organization must be capable of immediate action to identify an incident, contain any damage, and properly preserve evidence.

Organizations should perform periodic network penetration, or “pen,” testing to determine whether their networks are vulnerable to attack. Such testing is most effective when both inside and outside personnel participate in planning and execution.

10. **Patching**

Software developers regularly release patches to update their application or systems software. These patches involve the installation of new software code, often without opportunity for security testing. Patching must therefore not be taken casually. The organization’s technology team should remain alert to patch-related announcements and verify the authenticity of patches prior to installing them. Only qualified IT personnel should be allowed to install software patches. All major patches and all patches to critical systems should be recorded.
11. **Anti-Phishing**
Employees should be trained to be alert for social engineering attacks. Employees should be able to recognize suspicious e-mails or other communications asking for passwords or other private information. Such e-mails should never be responded to, but instead reported to the organization’s information security team.

12. **Malware**
If applicable, organizations should obtain, install, and regularly update antivirus software for workstations and servers and all access devices to the extent possible with rapidly emerging technologies. The extent of and/or necessity for this protection will depend on the nature of the software running on each device and on known and unknown vulnerabilities and threats.

13. **Elimination of Unnecessary Software Processes**
Organizations should harden their operating systems, other software, and hardware using industry-recognized guidelines. For instance, organizations should remove or turn off unnecessary software services and applications, some of which may be turned on by default. The fewer the number of applications on a system, the easier it is to maintain its security.

14. **Physical Security**
All information systems are valuable, regardless of whether they contain sensitive information. All hardware devices should, at a minimum, be locked or otherwise protected from physical manipulation by nonauthorized persons. Critical systems should be behind locked doors manned by human security guards where necessary. Guests or other third parties in such areas should be heavily supervised by persons knowledgeable enough to detect suspicious behavior. Guests entering or leaving should be searched, both to deter theft and to guard against listening devices.

C. **Website Privacy Policies**
Organizations should have privacy policies posted on each customer-facing website, either because such posting is mandated by law or for reasons of business competitive advantage. These policies must include requirements from privacy statutes for all jurisdictions and industries that the organization operates within (as discussed in Chapter 2). For example, organizations operating websites in the United States involved with financial consumers must comply with the privacy policy set forth under GLBA. Those dealing with children must comply with the privacy policies dictated by COPPA, and those dealing commercially with California residents have a California state statute to comply with. The sum of such applicable statutes can serve as a minimum best practice for website privacy policies.

Website privacy policies explain an organization’s policy with respect to use and disclosure of personal information collected from the user. In general, a privacy policy will address what type of information is collected, why it is collected, how it is used, and under what circumstances, if any, the information will be disclosed to third parties. In
addition, a privacy policy will frequently explain whether cookies, web beacons, and similar devices are placed on a user’s computer and, if so, why.\textsuperscript{2}

It is also important that the privacy policy consider what happens if an organization were to go out of business or become bankrupt. In a recent case,\textsuperscript{1} the potential sale of the names and personal information gathered from a bankrupt firm’s website drew a letter from the FTC, stating that the sale or transfer of sensitive personal information to a new owner that occurs as part of a bankruptcy proceeding must be in accordance with the privacy policy of the bankrupt entity.\textsuperscript{4} Otherwise the sale would be considered a deceptive or unfair business practice, in violation of section 5 of the FTC Act, as this company’s privacy policy had stated that they would never transfer such information. The FTC Act is discussed in Chapter 2.

1. **COPPA**

Under COPPA, the website must post a link to its privacy policy on its home page and on every other page where personal information is collected. The link must be clear, prominent, and distinguishable from other links on the site. The notice itself must be clear and understandable and include the following information:

- the name and contact information of the operator of the website who is collecting or maintaining children’s personal information obtained from the site;
- the kinds of information collected from children and how the information is collected (i.e., directly from the children or through cookies);
- how the website operator uses the information;
- whether the information is disclosed to third parties and, if so, the kinds of businesses to which information is disclosed and the general purpose for which the information is used;
- whether these third parties have agreed to any confidentiality or security of the information;
- the option to consent to the collection but not the disclosure of information to third parties;
- a disclosure that the website operator cannot require a child to disclose more information than is reasonably necessary to participate in an activity as a condition of participation; and
- the procedures to be followed by parents in reviewing a child’s personal information, requesting that some be deleted, and refusing to allow any further collection or use of the child’s information.\textsuperscript{5}

A separate notice for parents must advise that the parents’ consent is required for the collection, use, and disclosure of information and must explain how that consent is to be

\textsuperscript{2} Frequently, a privacy policy will explain that a cookie is used to enhance a user’s experience on the website by recognizing the user and adding greater functionality for recognized users.

\textsuperscript{3} Letter from FTC’s Bureau of Consumer Protection regarding XY brand name personal information (July 1, 2010).

\textsuperscript{4} See 11 USC § 363(b).

given by the parents. A new notice and consent are required to be sent to parents when any material changes in the collection, use, or disclosure of information occur.

2. GLBA

GLBA also requires a privacy policy for consumers. The privacy policy must disclose the categories of third parties to whom personal information will be disclosed, the policies and practices of the institution of disclosing personal information of people who are no longer customers, types of personal information collected, and the institution’s confidentiality and security policies. This privacy policy must be provided when a relationship with a consumer is established. To facilitate the creation of privacy policies under GLBA, the FTC and other federal regulatory agencies released a final rule amending the GLBA privacy rules in late 2009.

The Final Model Privacy Form can be used by financial institutions to describe their privacy policies and how consumers can opt out of letting their information be disseminated to unaffiliated third parties. This form is not required, but its proper use will allow compliance (safe harbor) with the obligations for initial and annual notice to the consumer on disclosure of his or her nonpublic personal information and for opt-out procedures to prevent the sharing of his or her information with unaffiliated third parties. There are three versions of the model form, allowing opt-out by mail, opt-out by telephone/online, or no opt-out option. The existing sample clauses are no longer the approved safe harbor for compliance after December 31, 2010.

3. State Law

California's Online Privacy Protection Act imposes privacy obligations on any “operator” of a website or online service if the website or online service has a commercial purpose and is accessed or used by a California resident. “Operator” is defined as “any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes.” The law mandates the use of a privacy policy that may be accessed from each website page and that contains the following information:

- the effective date of the policy;
- a list of the categories of personally identifiable information collected by the operator from consumers who use or access the website and a list of the types of third parties to whom the operator discloses such information;
- an explanation of how the operator will notify users if the privacy policy is materially changed; and

---

8. Consumers include people who have applied for loans or used automated teller machines but have not used the institution for any further services.
• an explanation of how users may review and change their personally identifiable information—if the operator allows such review and changes—or a statement that the operator does not permit such review and changes.

### 6.2 RESPONSE TO DATA BREACH

Data breach can result in loss of intellectual property, employee personal and sensitive data, customer data held by the organization, or other corporate confidential or secret information. It can result in reputational harm; loss of business revenue and profit; loss of competitiveness; loss of employee, partner, or client confidence; and noncompliance with statutes, regulations, and standards. Regardless of what is breached, when any information is disclosed, modified, or lost due to a data breach, the organization must respond swiftly and effectively to the incident.

#### A. Incident Response Plan

Even organizations with a well-managed information security and privacy program must rigorously prepare for such a breach event. The incident response plan must include:

• Initiating of the computer incident response team (CIRT), whose members were selected based on the appropriate skill sets;
• Rapid assessment of the data breach activity to determine the type of incident and extent of its damage;
• Appropriate breach containment activities; and
• Guidelines for involving other parties, including law enforcement and officials requiring notification under data breach laws.

The CIRT should be a group within an organization that has various skills including technology officers (CTO, CISO), IT and information security staff, human resources staff, communications staff, and corporate counsel. Each CIRT member brings his or her area of expertise to ensure that the organization is properly responding to an incident. For the CIRT to be effective, it must have authorization to act quickly, in areas such as declaring, prioritizing, and escalating incidents, taking systems and networks off-line, contacting other parties, and deploying external resources. Reacting quickly to an incident requires an initial understanding of the incident and the extent of damage that was or may be caused by it.

#### B. Responding to an Incident

The assessment of incoming reports about the incident includes prioritization of incidents and verification about the nature of the incident. This assessment will help the business understand the balance of focus on remediation (i.e., preventing further damage to systems) and investigation (i.e., preserving evidence in order to track down the attacker). Companies should strive to both remediate and investigate—processes that often complement and enhance each other. In any situation, the incident must be fully documented while attempting to maintain the confidentiality of the information that was breached.

If an occurring incident has a detrimental effect on a business, one of the key steps is to identify and isolate the affected systems from the network without altering its files.
(i.e., not powering off the system, logging into it, or deleting any files). If an ongoing incident does not have an immediate business impact and information from monitoring the incident can assist with an investigation, it may be best to closely watch the activity. In any case, the incident investigation must stay active until the root cause is understood and the incident can be reviewed, appropriate remedial actions taken, and the episode officially closed. To create such procedures, organizations could, for example, start with the series of questionnaires ISACA developed to facilitate the evaluation of the internal controls necessary when responding to cyber incidents\textsuperscript{10} and NIST SP 800-61 on security incident handling.\textsuperscript{11}

The CIRT should decide whether to monitor or resolve the issue and may involve the assistance of law enforcement in this decision. In general, in determining when to contact law enforcement, companies should report incidents that are malicious and have a real and substantial impact on the organization or activity that is noteworthy as defined by the CIRT. Law enforcement should be contacted if an incident appears to involve criminal activity, indicated by any of the following events:

- An unauthorized user has logged on to the system, including root access;
- A heavy volume of packets has bombarded the system in a short period of time (from the same or varied sources) evidencing a denial-of-service attack;
- An incidence of social engineering has led to security breach;
- Continuous network scanning or probing is occurring;
- A demonstrated exploit of a public-facing website or web application has taken place; or
- The attack appears to be aimed at critical information or areas of the network affecting critical infrastructure.

Once an organization has decided to involve law enforcement in the activity, determining the proper agency can be complex. The Department of Justice’s Computer Crime and Intellectual Property Section has compiled a useful table that lists the type of crime and the corresponding appropriate federal investigative law enforcement agencies.\textsuperscript{12} In addition, CIO magazine, in conjunction with the U.S. Secret Service and the FBI, has issued response and reporting guidelines that list federal law enforcement agencies and their areas of responsibility, along with the local offices to contact in the event of an information security attack or breach.\textsuperscript{13}

Reporting of an incident requires a careful analysis. Reporting to law enforcement or other agencies is often very difficult for companies because of fear of negative publicity. Not reporting, however, undermines general deterrence of computer crime, which leaves all networks much less secure. In addition to the benefit of deterring cybercrime, many state laws and contractual obligations require that certain breaches be reported. But there are also legal requirements to report to avoid civil or even criminal sanctions.

\textsuperscript{10} ISACA, Cybercrime: Incident Response and Digital Forensics, Internal Control Questionnaires (2005).
\textsuperscript{11} NIST SP 800-61 Rev 1, Computer Security Incident Handling Guide (2008).
\textsuperscript{12} Available at http://www.cybercrime.gov/reporting.htm.
\textsuperscript{13} Available at http://www.cio.com/research/security/incident_response.pdf.
Almost all U.S. states and many countries require some sort of notification after data breaches, especially when the data is not encrypted, is of a personally identifiable or sensitive nature, and affects the records of more than a stated number of individuals. Regulated companies should check with their regulator to determine if they have a duty to report incidents and to whom they should report, as such duties often will be industry-specific. For example, a financial institution may be required to complete a Suspicious Activity Report (SAR) and file the signed form with the Financial Crimes Enforcement Network (FinCEN).

If the cyber incident results in the unauthorized disclosure of unsecured individually identifiable health information and is also a security breach as defined in the HITECH Act, HIPAA-covered entities are required to give notice of breach. Payment card brands such as Visa and MasterCard also have specific reporting requirements for retail merchants that suffer a data breach. In addition, some cyber insurance policies (discussed in Chapter 4) require the insured to report security incidents to law enforcement before a claim can be paid under the policy. Therefore, if the insured desires the loss to be covered under the policy, the incident must be reported to law enforcement.

C. Digital Forensics

An investigation into a security incident must be carefully conducted in order to ensure quality evidence and admissibility in court. “A basic tenet of evidence handling is to maintain the item of evidence in its original state and to thoroughly document access to the item as well as the reason and process associated with any changes.” In order to preserve evidence in its original state, a proper forensic examination must occur, potentially including digital forensics.

Digital forensics is the application of scientific methods and techniques to recover data from electronic media. Digital forensics investigators can collect and analyze digitally stored information to show where, when, and how the incident occurred. The key to any forensic investigation is to gather the data in a forensically sound manner, using appropriate forensic protocols. The digital media must be copied or imaged in a way that preserves the original data and results in a complete snapshot. The forensic imaging

14. “Unsecured” means “not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services.” See also HHS Guidance at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

15. “Breach” means “an impermissible use or disclosure . . . that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual,” with a few specified exceptions. State laws that are inconsistent with the HITECH Act notice of breach requirements are preempted by federal law, without regard to those exceptions. In other words, once it has been determined that there has been a “breach” under federal law, inconsistent state notice of breach laws are preempted. On the Web, go to http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/ for HIPAA breach notification requirements.


17. For a more detailed analysis of data breaches, see LUCY L. THOMSON, DATA BREACH AND ENCRYPTION HANDBOOK (American Bar Association 2011).

system must not alter the original data in any way. The data must be collected in a manner that maintains the authenticity and integrity of the data existing at the time of the incident, to the extent possible. The process used for collection of the data must be documented, and the chain of custody of the data must be complete and fully documented.

Understanding which data is relevant to the incident and where the data resides is critical to the investigation. Relevant data may be located on servers, desktops, laptops, or even USB devices, PDAs, and home computers.

In the event of a lawsuit involving digital evidence, location, collection, and preservation of the evidence are critical for both plaintiff and defendant. Failure to preserve evidence may result in sanctions for spoliation. Digital evidence is often collected, processed, and authenticated at trial using hardware and software supplied by vendors. Because these forensic tools often play a critical role in how digital evidence is collected, processed, and authenticated in court, the reliability of these products is of the utmost importance.

It should be noted that the work of a digital forensics investigator is different from that of the corporate IT professional who is responsible for the day-to-day operations of the company’s system. Although the CIRT should be involved in the forensic investigation to determine the scope of the incident and the appropriate method for restoration of service, digital forensics requires specialized knowledge and protocols. For assistance in building forensic capabilities, NIST has created SP 800-86.

D. Public-Private Partnerships

The CIRT often can work with local or national law enforcement to ensure that a proper investigation is completed. This type of public-private partnership is not unusual in the information security arena. National, state, and local governments offer opportunities for private organizations to work collaboratively to improve information security. In many cases, the primary emphasis of these partnerships is on protecting the nation’s critical infrastructure (e.g., transportation, power, food, health) or preventing crime (e.g., protection from computer fraud or data theft). The government also invites private party participation in setting standards and defining best practices.

One of the most well-known public-private partnerships in the information security arena in the United States is Infragard. The FBI hosts Infragard, through which law enforcement, corporations, and academia exchange information about threats and attacks on the nation’s critical infrastructure (e.g., transportation, power, food, health) or preventing crime (e.g., protection from computer fraud or data theft). The government also invites private party participation in setting standards and defining best practices.

The Department of Homeland Security hosts multiple public-private programs that address different aspects of information security. These programs include Sector

---

Coordinating Councils focused on Critical Infrastructure/Key Resources\textsuperscript{22} and the U.S.-Computer Emergency Response Team (US-CERT), which collects information and educates nonprofessionals about computer and cyber security threats and vulnerabilities.

Although public-private partnerships have become a critical element of information security and privacy, attorneys need to research and inform their clients if there are potential legal issues associated with sharing information with government entities. For example, Congress explicitly included a protection\textsuperscript{23} for companies sharing trade secrets with the Department of Homeland Security in relation to critical infrastructure protection, but many programs do not have such explicit legal authority.

Private corporations also may find themselves encouraged or even required to adopt a government directive if the corporation is working with a government entity. For example, the Personal Identity Verification (PIV) standard\textsuperscript{24} was created in response to a 2004 White House order\textsuperscript{25} to standardize identity credentials for federal employees and contractors and was to be used to support both physical and logical access. That order was followed by the Personal Identity Verification—Interoperable (PIV-I)\textsuperscript{26} standard released in 2009 to address the challenges for interoperating across organizations—federal, state, local, and private. Some corporations are mandated to adopt the standard as a result of their federal contractor status, and others are encouraged to adopt it to facilitate their work as first responders or as part of the nation’s critical infrastructure. It has been proposed that eventually the standard be expanded to support private-sector secure transactions and that a public-private partnership help establish the initiative.\textsuperscript{27}

6.3 \textbf{AUDIT AND CERTIFICATION}

After the information security and privacy controls have been designed and implemented and staff appropriately trained, the effectiveness of the controls must be monitored, measured, reviewed and remediated, and reported to the interested stakeholders, including existing and potential customers, shareholders, creditors, and executive leadership. Whether to comply with regulatory requirements or to promote competitive differentiators, organizations pursue a variety of audit opinions and certifications that cover information security and privacy. Depending on the audience, the type of assurance or certification sought, and the nature of the controls, these opinions and certifications can be categorized as follows:

- Information Security Certification: ISO 27001, U.S. government
- Information Security Assurance: SAS 70/ISAE 3402, SOX

\textsuperscript{22} Cf. Homeland Security Presidential Directive 7 (HSPD-7) and the National Infrastructure Protection Plan (NIPP).
\textsuperscript{23} 6 U.S.C. § 133.
\textsuperscript{24} Federal Information Processing Standard (FIPS) 201.
\textsuperscript{26} “Personal Identity Verification Interoperability for Non-Federal Issuers,” Federal CIO Council (May 2009).
\textsuperscript{27} Written testimony of Vivek Kundra, Federal Chief Information Officer, before the House Committee on Oversight and Government Reform Subcommittee Government Management, Organization, and Procurement (March 24, 2010) (referencing the establishment of the National Strategy for Secure Online Transactions).
- Privacy Assurance: GAPP, Privacy audit
- Privacy Certification: National/regional standards
- Website Certification/Assurance: WebTrust, trustmarks

A. ISO 27001
The ISO 27001 information security standard describes the components of an adequate information security management system. The specific controls for the information security management program are contained in a related standard, ISO 27002. Metrics for the information management security system and controls are covered in ISO 27004. The risk management and assessment process to identify controls for external or internal threats and internal vulnerabilities is under ISO 27005. Certification is sought under ISO 27001, which may involve these other ISO standards.

As discussed in Chapter 1, there are three significant parts of an information security program. The first part is the information security and privacy policy, whereby a corporation’s executives document their support of and participation in the protection of organizational, employee, and customer data. The high-level security direction is laid out here, as well as the standards for acceptable usage of corporate assets, physical as well as informational. The written information security and privacy policy is then disseminated to all employees and awareness training held. Some best practices for these policies were described earlier in this chapter. The second part of an information security program is the risk management program, which documents the information assets a corporation has and assesses the threats to those assets from either external (e.g., viruses) or internal (e.g., employee theft) sources, the vulnerabilities in practices and systems, and the exploits possible for the interaction of the threats and vulnerabilities. Decisions are then made on how to respond to each of these risks, including creating controls, outsourcing the risk, or accepting the risk. This process was described in Chapter 4. The third part of the information security program is the controls discussed in Chapter 5, which must be designed, tested, and implemented and then monitored, measured, reviewed, and revised as appropriate. The ISO 27002 controls are grouped into technical, administrative, and physical categories, including the separation of duties, periodic reviews by management and auditors, physical access limits to facilities, virus software, access controls on applications and file systems, change management processes, backups, limits on wireless and mobile device usage, encryption, training, monitoring, incident management, and operational tasks.

To bestow certification, the certifier will examine the design of the controls and interview the organization’s management and employees to determine the organization’s commitment to information security in the normal course of operations. It is essential to show both that management has a deep commitment to information security and that information security is embedded in what the organization does on a daily basis in all major processes and not viewed as some external process taken up periodically. After providing suggested remediations, the certifier will return to review the implementation of those remediations and to determine if the controls as designed and implemented are working effectively. Keeping records of control activities is essential. If the policies, procedures, and controls described in the standard are appropriately implemented, maintained, moni-
tored, reviewed, and revised and if the organization’s commitment is demonstrated, ISO certification will then be granted.

B. U.S. Federal Government

Under the Federal Information Security Management Act (FISMA) of 2002, U.S. federal agencies are required to implement and report on effective information security controls. This process includes “periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices.” The law designates the Director of the Office of Management and Budget to oversee the implementation of this and other information security requirements for federal civilian agencies, the Secretary of Defense for Defense Department systems, and the Director of Central Intelligence for the CIA. NIST, in coordination with the National Security Agency (NSA), is responsible for providing more detailed guidance in defining and implementing the security controls described in FISMA. Additionally, OMB Circular A-130, Appendix III, and subsequent annual FISMA reporting guidance requires agencies to authorize processing on a system-by-system basis, defining a system as “an interconnected set of information resources under the same direct management control which shares common functionality.”

These systems are subdivided into general support systems and major applications, but agencies have flexibility in what constitutes a system. It is ultimately up to the agency head or his or her designee to accept the risk for each information system in use at the agency. In furtherance of this process, NIST has proposed and OMB has endorsed a Risk Management Framework for the ongoing information security protection of each federal system. The defense and intelligence communities have a similar process, and there is ongoing work to consolidate these processes into a single risk management process for the federal government. Consequently, the NIST process is the focus, which will likely absorb the processes from the defense and intelligence communities with some minor changes. The steps in the framework and the related standards are as follows:

1. Categorize the information system—FIPS 199/SP 800-60
2. Select the security controls—FIPS 200/SP 800-53
3. Implement the security controls—SP 800-70
4. Assess the security controls—SP 800-53A
5. Authorize the information system—SP 800-37
6. Monitor security state—SP 800-37/SP 800-53

The first step, highlighted in Federal Information Processing Standard (FIPS) 199, is to categorize a system. Under FIPS 199 guidance and more detailed guidance found in

---

NIST Special Publication (SP) 800-60,\(^{31}\) agencies are to select the types of information that are found in the system and use the guidance to determine whether that information falls into a low-, medium-, or high-impact category. Using that impact category, agencies are to select the controls relevant to that system. Under FIPS 200,\(^{32}\) the control framework and associated impact levels specified in NIST SP 800-53\(^{33}\) are mandatory. However, there is consensus that some flexibility exists where certain controls are not feasible or where other compensating controls are used. SP 800-53 offers agencies a fair amount of latitude as to how the controls are to be implemented on specific platforms.

For more detailed guidance, NIST has developed a variety of platform and application-specific guidance documents. Some, such as the Federal Desktop Core Configuration, have been made mandatory by OMB. The Defense Information Systems Agency (DISA) offers a wide range of Security Technical Implementation Guides (STIGs) that are frequently used by both the public and private sectors as examples of sound, albeit very stringent, security controls to implement at a very granular level. Following implementation, controls are typically documented in a System Security Plan (SSP) that is described in NIST SP 800-18.\(^{34}\) At minimum, agencies are to describe how the controls in SP 800-53 are being implemented. Ideally, detailed information should be included so that an auditor can readily verify whether the controls are in fact implemented. However, in most cases, agencies simply parrot the language from SP 800-53 and leave it to the interpretation of the person assessing the system to determine whether a particular configuration setting adequately satisfies the control requirements. That assessment process is described in NIST SP 800-53A,\(^{35}\) which breaks down the SP 800-53 controls into a series of test steps to be performed. It is also expected that supplemental guidance such as DISA STIGs and platform-specific NIST guidance be used to confirm that the controls are implemented and effective.

The next step is officially the certification and accreditation (C&A) step that is spelled out in NIST SP 800-37.\(^ {36}\) This step is largely a paperwork exercise once a system is assessed. It is here that the assessment team formally delivers its assessment report. Usually this assessment is done on behalf of the CIO, who generates a letter to the accrediting authority indicating the state of the security controls and provides a recommendation as to whether the system is sufficiently secure so as to allow it to begin or continue operating. Based on that recommendation, the system owner, who, under FISMA, is effectively acting on behalf of the agency head, generates an accreditation letter or, in the Defense Department context, an authorization to operate. Under traditional C&A guidance, this authorization must be renewed at least every three years, and under FISMA, the system must undergo some assessment on an annual basis. At this

---

point, any deficiencies are also noted and a Plan of Action and Milestones (POA&M) is generated to track the findings. The status of any high- or medium-risk findings needs to be reported to OMB as part of the annual reporting process. The current trend is to implement a process described in SP 800-37 called continuous monitoring, which will ultimately rely on automated tools to verify controls on an ongoing basis making formal assessments less onerous. OMB mandates continuous monitoring and automated reporting in its latest FISMA reporting guidance.\(^\text{37}\) Some agencies are scrapping their traditional C&A process that relies on doing exhaustive assessments every three years and instead are relying on the use of automated tools on an ongoing basis to ensure compliance. While reauthorization every three years is still required under OMB Circular A-130, that process would usually only involve packaging the already generated automated reports with the required certification and accreditation letters.

C. \textit{SAS 70/ISAE 3402}

The AICPA’s Statement on Auditing Standards (SAS) 70 auditing standard (or local national equivalents such as those in the United Kingdom, Japan, and Canada) is a methodology for auditing the internal controls of a third-party outsourcing vendor. This older standard is now being replaced by the International Auditing and Assurance Standards Board’s (IAASB) International Standard on Assurance Engagements (ISAE) 3402.\(^\text{38}\) It is commonly used in SOX audits for assessing the internal controls—in this case, information security and privacy—relevant and material to outsourcing entities’ financial reporting. Although frequently utilized for reporting on internal controls of service organizations for any purpose, such as confidentiality, availability, and integrity of the user entity’s information, these standards are strictly only for internal controls over financial reporting.

Unlike an ISO 27001 certification, there is no predescribed set of policies, procedures, and controls to check the service organization’s controls against. Rather, it is up to the service auditor’s judgment. Management of the service organization creates a description of the outsourcing services provided to users and how the services are performed, including the controls utilized. The result of the attestation engagement is based on the judgment of the auditor about the design and effectiveness of the controls in scope (management determines which controls or organizational groups are in scope). The ISAE 3403 standard does now require that management of the service organization provide a written assertion of the fairness of their description of their system and control design and (if in scope) control effectiveness.

The reports (and examination procedures to produce the reports) can be one of two types. Type I reports examine only the design of the controls. Type II reports examine both control design and effectiveness over a period of time (at least six months), including the description of the tests used by the auditor. To perform this engagement, the

\(^{37}\) OMB Memorandum M-10-15 (2010).

\(^{38}\) SAS 70 is being replaced in the United States by SAS Audit Considerations Relating to an Entity Using a Service Organization and Statement on Standards for Attestation Engagement (SSAE) 16 Reporting on Controls at a Service Organization. SSAE 16 is based on the IAASB’s ISAE 3402.
service auditor will visit the service organization to examine the control objectives and control design, interview the control users and management, review applicable documentation, and perform appropriate control testing (if a Type II report). The resulting Service Auditor’s Report contains the auditor’s conclusion as to the adequacy of controls and lists the control objectives, the controls tested, and the results of testing as well as, under ISAE 3402, the conclusion on management’s assertions. The reports are used by organizations that outsource and their auditors when preparing the organization’s financial statement audits. Strictly speaking, these reports are not intended for use by potential customers of service organizations, only by existing customers and their auditors.

D. SOX

In reaction to the Enron and WorldCom scandals and other financial frauds, the Sarbanes-Oxley Act (SOX) was passed in 2002. The intention of SOX is to stop fraudulent financial and accounting practices. Indirectly, SOX has had far-reaching impacts on information security practices.

As a consequence of SOX, the Securities and Exchange Commission (SEC) has issued guidance directing how corporations report on internal control over financial reporting (ICFR).39 ICFR is a process that a corporation uses to ensure that its financial reports are prepared in a proper manner. The SEC guidance states that “management’s annual assessment of the effectiveness of ICFR must be made in accordance with a suitable control framework’s definition of internal control.” In a footnote, the SEC gives examples of suitable frameworks, such as the ones developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the Canadian Institute of Chartered Accountants (CICA) Criteria of Control (CoCo),40 and the Internal Control: Guidance for Directors on the Combined Code (The Turnbull Report)41 from the Institute of Chartered Accountants in England. The COSO framework is the one most commonly cited in 10-K reports filed with the SEC.

1. COSO

Five professional organizations formed COSO in 1985 to study the causal factors leading to fraudulent financial reporting.42 COSO’s recommendations are primarily directed at public companies and their independent auditors. COSO published its primary work,
Integrated Control—Integrated Framework, in 1992. The initial components of the framework were:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

While information technology (IT) security falls within the framework’s control activities and monitoring components, COSO’s output is high level and has limited direct impact on IT security.

2. Public Company Accounting Oversight Board (PCAOB)

SOX established the PCAOB as a private-sector, nonprofit corporation to oversee the auditors of public companies. It protects investors and the public interest by promoting informative, fair, and independent audit reports. Many of COSO’s recommendations were incorporated into SOX and the work of the PCAOB.

For companies subject to SEC regulation under U.S. law, the PCAOB has the authority to set standards for auditors who attest to an organization’s financial statements and to management’s statement of internal control. SOX also requires that management describe those controls. In 2007, the PCAOB issued Auditing Standard No. 5. It states:

As part of evaluating the period-end financial reporting process, the auditor should assess—

- Inputs, procedures performed, and outputs of the processes the company uses to produce its annual and quarterly financial statements;
- The extent of information technology (“IT”) involvement in the period-end financial reporting process.

In short, IT controls—including IT security controls—are included in the independent auditor’s evaluation. “The use of IT . . . affects the fundamental manner in which transactions are initiated, recorded, processed, and reported.” The PCAOB, as well as the AICPA, however, give minimal guidance on what types of controls are meaningful in an IT environment.

44. The framework has since been expanded to eight components and rechristened the Enterprise Risk Management (ERM) Integrated Framework (2004).
47. 15 U.S.C. § 7262 (2010) (this section is commonly known as “Sec. 404, Management Assessment of Internal Controls”).
49. Id., § 27.
3. **COBIT**

As discussed in Chapter 5, COBIT is ISACA’s enterprise governance of IT framework. In the IT controls aspects of SOX and similar internal controls audits, COBIT audit techniques may be the preferred choice. ISACA has developed a number of tools to assist in these audits, including the Information Technology Assurance Framework (ITAF) that provides guidelines, terminology, tools, techniques, and general performance and reporting standards for IT audits. One of the tools is the Information Security Management Audit/Assurance Program. This program starts with an evaluation of the 11 areas under the COBIT IT process DS5, *Ensure systems security*, from the Deliver and Support (DS) domain and ends with an evaluation of the maturity level of the COBIT control framework, using an approach derived from the software development maturity model defined by the Software Engineering Institute (SEI) of Carnegie Mellon University.51

**E. GAPP**

A privacy audit compares an organization’s actual privacy practices against a known benchmark, such as national statutes or regional frameworks. Because the privacy principles in these statutes are often at a high level, to derive a detailed audit approach, the AICPA’s/CICA’s *Generally Accepted Privacy Principles* (GAPP) can be used. A combination of the GAPP plus any additional domestic statute-specific provisions can address privacy compliance requirements in each of the organization’s jurisdictions. The AICPA and CICA allow privacy practitioners to provide either privacy advisory services or privacy audit examination services. The audit services can be performed either on management’s assertion that they maintained effective controls over the privacy of personal information in accordance with their privacy notice and GAPP or directly on the subject matter of the privacy controls and privacy notice.

The GAPP document includes a table with measurement criteria for each principle, illustrative controls and procedures, and additional considerations. This table can be used both proactively when setting up the privacy controls and then during the audit itself to measure actual operational compliance of the controls and procedures with GAPP.

**F. IT Audit/Assurance—Privacy Guidelines**

Because most data is now electronically stored, the privacy audit could fall within the realm of an IT audit, so ISACA’s IT audit and assurance standards and guidelines may be appropriate. Guideline 31 on privacy52 deals with how to apply privacy to an IS audit. There are a number of useful features in this guideline. One is a checklist of 21 questions that allows comparison of the differences between the privacy laws in each country. Another is a list of key controls, in the areas of media reuse, training, access controls, maintenance, data integrity, physical access, and risk assessments. There is also a list of considerations for the protection of personal information, covering some of the following areas: privacy management, risk assessment, security audit, professional secrecy, physical security, confi-

---

dentiality, integrity, availability, security measures, security toward external partners, and awareness and training sessions.

The audit itself requires that the IT auditor determine the existence of the following: a privacy policy, privacy officer, data controller, training and awareness plans in relation to privacy, privacy complaint management process, regime of privacy audits conducted against the privacy legislation, and privacy requirements for outsourcers and contractors. The auditor is required to undertake a privacy impact analysis and produce an audit report. The report should document the results of the privacy review, outline the scope and objectives, and provide a summary of the types of data and information collected, stored, and used by the organization. The report should include information on the privacy-related risks that the organization faces and a summary of the risk reduction measures or privacy protection strategies that exist. Weaknesses identified in the privacy review because of missing or inadequate controls should be brought to the attention of both information owners and management responsible for privacy. Any material weaknesses should be addressed immediately. The IT auditors should include appropriate recommendations for stronger privacy controls.

G. Privacy Certifications

Privacy certifications are typically country or regional programs that organizations use for business competitive advantage. The United States is not currently an international leader in this area. Two leading examples are the EU’s EuroPriSe and Japan’s Privacy Mark.

1. Japan

Japan’s Privacy Mark is a voluntary scheme under which businesses can achieve certification for their personal data protection systems. Developed by the Japan Information Processing Development Corporation (JIPDEC) in 1998, the plan requires an independent certifier to verify compliance with the Japan Industrial Standard (JIS) Q 15001 (2006). The objectives of the program are to enhance consumer awareness of personal information protection through display of the Privacy Mark symbol and to promote appropriate handling of personal information through enhanced credibility for business operators. In the certification process, the certifier will first review the applicant’s documents off-site then come onsite to further review documents, perform interviews, investigate the privacy-related procedures, and provide suggested remediations. After the material remediations are resolved, the Privacy Mark can be granted to the applicant, who may then display it prominently on the company's website, envelopes, letters, contracts, and business cards. The requirements are to establish, implement, maintain, and improve a personal information protection management system, including policies, organizations, inventories, risk assessments, plans, implementations, audits, and reviews.

2. Europe

The European Privacy Seal (EuroPriSe) allows organizations that do business in the EU to demonstrate privacy compliance for IT products and services in sales to both consumers and governments. EU-backed and involving nine data protection authorities in
the region, the audit of the products and services is against European Data Protection privacy and information security regulations. The process uses two phases, beginning with an evaluation by independent qualified IT and legal experts and followed by a verification process by the accredited certification body. The products include both hardware and software, and the services include any type of electronic commerce, search engines, and data centers. The experts are qualified only after they have proven their proficiency through working experience in IT and have passed a demanding test demonstrating a profound knowledge of privacy and data protection.

H. Trustmarks
Trustmarks are used by website operators, often those involved in electronic commerce, to demonstrate a certain degree of recognition and integrity in the operation of the website and the use of the consumer’s information. The trustmarks can signify any of the following about the website:

- Use of appropriate encryption for its consumer transactions
- Adherence to appropriate privacy standards
- Compliance with periodic security audits and vulnerability assessments
- Qualification as a legitimate business

1. Global Alliances
Most of the companies providing the trustmark services are private companies, some nonprofit and others for profit. Efforts have been made to create regional and global alliances of trustmark operators to provide an assurance level that works on the same geographic span as the Internet. The Global Trustmark Alliance included members from Europe, North America, and Asia, including the Asia-Pacific Trustmark Alliance, which allows its trustmark operators to act as “APEC privacy accreditation service providers” using the APEC Privacy Framework and so deal with market demand for privacy assurance services. The Global Trustmark Alliance also includes the Better Business Bureau in the United States, which offers BBBOnLine as a trustmark program. In Europe, the Alliance includes the Trust UK program, E-comtrust, Eurochambres, and the Federation of European Direct and Interactive Marketing.

2. WebTrust
The AICPA and CICA have a program called WebTrust for websites. This program is based on the AICPA/CICA Trust Principles and Criteria, as follows:

- **Security:** The system is protected against unauthorized access (both physical and logical).
- **Availability:** The system is available for operation and use as committed or agreed.

• **Processing integrity:** System processing is complete, accurate, timely, and authorized.

• **Confidentiality:** Information designated as confidential is protected as committed or agreed.

• **Privacy:** Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CICA.

This program covers policies, communications, procedures, and monitoring. The WebTrust family of branded assurance services includes the following, applied in the context of an e-commerce system:

• **WebTrust Online Privacy:** The scope of the assurance engagement includes the relevant online privacy principles and criteria.

• **WebTrust Consumer Protection:** The scope of the assurance engagement includes both the processing integrity and relevant online privacy principles and criteria.

• **WebTrust:** The scope of the assurance engagement includes one or more combinations of the principles and criteria not anticipated above.

• **WebTrust for Certification Authorities:** The scope of the assurance engagement includes the principles and related criteria unique to certification authorities. 55

---

55. See [www.webtrust.org](http://www.webtrust.org).