Chapter 4

What Are Controls and Why Are They Important?

After reading this chapter and completing the case project, the reader will:

- Understand the definition of controls and their importance in protecting information and communications technology (ICT) systems from security threats and vulnerabilities
- Be able to distinguish between goal-based and implementation controls while understanding each broad control type within each of the two groups
- Understand common approaches toward security control formulation and development

No matter how large or small an organization, there needs to be a plan to ensure the security of critical ICT assets. Such a plan is called a security program by information security professionals and is facilitated through the selection and implementation of appropriate control mechanisms designed to act as countermeasures for preserving confidentiality, availability, and integrity of all components that make up the organizations ICT infrastructure. Whether the plan is five or two hundred pages long, the process of creating a control-based security program will make organizations think holistically about their security. A security program provides the framework for keeping an organization at a desired security level by assessing the risks they face, deciding how they will mitigate them, and planning for how to keep the program and security practices up to date.

In this chapter, the focus will be on the controls that security programs are built on. Through a complete discussion of management and behavioral controls you will come away knowing what they are and how they are formulated. In understanding

the underlying principles associated with controls, you will also understand how they are aggregated into an everyday system of integrated security activities.

Picking Up Where Chapter 1 Left Off

In Chapter 1, you learned about three fundamental pillars for ICT security: confidentiality, integrity, and availability. However, as the security discipline has evolved, it has become apparent that a fourth core requirement is missing: accountability. Accountability addresses the need for the ability to trace the activities to the responsible source. For example, audit logs and digital signing of emails would both be controls that ensure accountability. Although you would not see the combined concept of the security objectives—confidentiality, integrity, availability, and accountability (which we will now reference with the acronym CIAA)—on a Certified Information Systems Security Professional (CISSP) exam, other certification exams, or security publications, many security professionals have been using this expanded view of cybersecurity for many years. Given the increased impact of supply chain concerns within the scope of ICT risk management, accountability requirements have come to the forefront of an organization's security priority list.

Another introductory level security concept is that there are three underlying principles that influence cybersecurity standards, guidelines, and control decisions: least privilege, separation of duties, and defensive in depth. The CIAA pillars discussed above and these three cybersecurity principles are effectively managed through the development, implementation, and audit of security controls. In cybersecurity, there are five functions of controls: identify, protective, detective, responsive, and recovery. The Framework for Improving Critical Infrastructure Cybersecurity (CSF) describes each of these five functions as indicated in the following list:

- *Identify*—develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- *Protect*—develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
- *Detect*—develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
- *Respond*—develop and implement the appropriate activities to take action regarding a detected cybersecurity event
- *Recover*—develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event (National Institute of Standards and Technology, 2014b)

Each of those functions is supported by one or more administrative, technical, and operational control categories. By definition, controls are a security

mechanism, policy, or procedure that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization. The National Institute of Standards and Technology (NIST) (2014a) Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* more formally defines controls as stated below.

> … the safeguards/countermeasures prescribed for information systems or organizations that are designed to: (i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizationsthe; and (ii) satisfy a set of defined security requirements.

Whether an organization is considering a technical or operational control to mitigate risk, or an administrative solution such as training and new procedures or policies, the control needs to focus on the hardware, telecommunications, and software that protect sensitive information in one of the following three states:

- Data at rest
- Data in transit
- Data in process

These information-centric states define what the control needs to affect. The threats and vulnerabilities that must be considered change dramatically based on the state of the data, although the sensitivity factor does not. These criteria need to be given consideration as appropriate controls are selected. Together, the underlying principles related to information states, and the information security fundamentals introduced in Chapter 1 provide the basis for security control selection, development, and audit.

Goal-Based Security Controls

Security controls help reduce risks in an organization and to be efficient, cybersecurity professionals are expected to understand them from five perspectives: their goals, and how they are classified and selected, how they are implemented, how they are tested for effectiveness, and finally how they are audited.

As stated in the previous section, it is normal to see controls referred to as countermeasures or safeguards, referencing their ability to counter threats and provide safeguards to reduce vulnerabilities, but they are all the same. More specifically, security controls attempt to prevent or limit the impact of a security incident. A security incident is an adverse event or series of events that can negatively affect the confidentiality, integrity, or availability of an organization's IT systems and data. This includes intentional attacks, malicious software (malware) infections, accidental data loss, and much more (Figure 4.1).

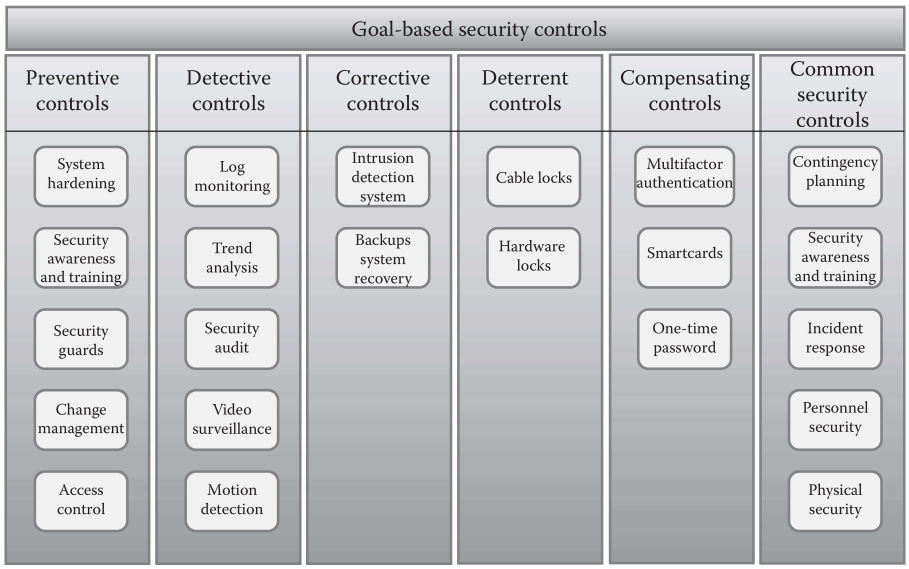

Figure 4.1 Goal-based security controls.

In this and other chapters of this book, we used the Federal Information Processing Standard Publication 199 (FIPS 199) as a means for classifying security controls supporting the five functions of the CSF throughout the risk management life cycle. Another common way of classifying controls is based on their goals in relationship to security incidents (NIST, 2004). Though we have already seen reference to one of these goal-based controls through the description of the CSF functional breakdown, some common classifications are prevention, detective, corrective, deterrent, and compensating.

- *Preventive controls:* attempt to prevent an incident from occurring.
- *Detective controls:* attempt to detect incidents after they have occurred.
- *Corrective controls:* attempt to reverse the impact of an incident.
- *Deterrent controls:* attempt to discourage individuals from causing an incident.
- *Compensating controls:* are alternative controls used when a primary control is not feasible.
- *Common controls:* are implemented across multiple ICT systems.

Preventive Controls

In a perfect world, an organization would not have any security incidents and that is the primary goal of preventive controls. Some examples include the following:

- *Hardening:* Is the process in which an ICT system or application is provided a greater level of security than its default configuration. This may include

disabling unneeded services and protocols, protecting management interfaces and applications, protecting passwords, and disabling unnecessary accounts.

- *Security awareness and training:* These involve making users aware of security vulnerabilities and threats thereby preventing incidents. When users understand how social engineers operate, for example, they are less likely to be tricked. Typically, uneducated users can be easily deceived into giving a social engineer their passwords, but educated users will see through the tactics and keep passwords secure.
- *Security guards:* These prevent and deter many physical attacks. For example, guards can prevent unauthorized access into secure areas of a building by first verifying user identities.
- *Change management:* Ensures that changes do not result in unintended outages. For example, as an alternative to managers making ad hoc changes, they could be expected to submit the change to a change management process where further review of the change takes place. Note that change management is an operational control, which attempts to prevent incidents. In other words, it is both an operational control and a preventive control.
- *Account disablement policy:* Ensures that ICT system access accounts are disabled when employment with the organization is terminated. This prevents anyone, including ex-employees, from continuing to use these accounts.

Detective Controls

While preventive controls attempt to prevent security incidents, it is inevitable that an organization will be victim to a security event at some point. Detective controls attempt to sense when vulnerabilities have been exploited, resulting in a security incident. An important point is that detective controls discover the event after it is occurred. Some examples of detective controls include the following:

- *Log monitoring:* There are many different log records that detail the activity on ICT systems and networks. For example, firewall logs record details of all traffic that the firewall blocked. By monitoring such logs, it becomes possible to detect incidents. Some automated methods of log monitoring automatically detect potential incidents and report them to the appropriate organizational personnel immediately after they have occurred.
- *Trend analysis:* In addition to monitoring logs to detect any single incident, organizations can also monitor logs to detect trends that occur in system and network activity. For example, an intrusion detection system (IDS) attempts to detect attacks and raise alerts or alarms. By analyzing past alerts, the Cybersecurity Incident Response Team (CSIRT) can identify trends such as an increase of attacks on a specific system.
- *Security audit:* As you read in Chapter 2, security audits can examine the security posture of an organization. For example, a password audit can determine

if the password policy is ensuring the use of strong passwords. Similarly, a periodic review of user rights can detect if users have more permissions than necessary, given their system access responsibilities.

- *Video surveillance:* A closed-circuit television (CCTV) system can record activity and detect what occurred. It is worth noting that video surveillance can also be used as a deterrent control.
- *Motion detection:* Many alarm systems are able to detect motion from potential intruders, and initiate alarms when the potential for physical security attack is imminent.

Comparing Detection and Prevention Controls

Before continuing, it is worth underscoring the differences between detection and prevention controls. A detection control cannot predict when an incident will occur and it cannot prevent it from taking place. Prevention security controls stop the incident from occurring at all. For example, recall our previous discussion of video cameras and guards. A simple camera that is in plain view and has no recording capabilities can prevent incidents from taking place because it acts as a deterrent. Now, compare that to a CCTV system with recording abilities. Such a device would include cameras, which can deter and prevent incidents, but the full system is also a detection control because of its recording capabilities. Cybersecurity professionals can take advantage of those capabilities by review the recordings to detect incidents after they have occurred. Likewise, guards are primarily prevention security controls. They will deter many incidents just by their presence. If attackers try to circumvent a security system, such as trying to sneak into a secured area, guards can intervene and stop the attack before it ever takes place.

Corrective Controls

Corrective controls are designed to reverse the impact of an incident or problem after it has occurred. Recall the discussion provided of the five CSF functions. Corrective controls are typically implemented in order to achieve the outcomes of response and recovery. Some examples of corrective controls are as follows:

- *Active IDS:* Active IDSs are a form of detection system that detects an attack and then makes necessary configuration changes to the environment in order to block the attack from continuing.
- *Backups and system recovery:* Backups ensure that operations personnel can recover data if it is lost or corrupted. Similarly, system recovery procedures ensure the CSIRT and oversight managers can recover a system after a failure.

Deterrent Controls

Deterrent controls are designed to discourage a threat. Some deterrent controls attempt to discourage potential attackers from initiating the event, while others focus on internal security by discouraging employees from violating established organizational security policy.

Many deterrent controls can be effectively described as preventive controls. For example, we have stated that a security guard is charged with the responsibility of controlling access to a restricted area of a building. That guard will deter most unsanctioned entry into the restricted area. This deterrence prevents security incidents related to unauthorized access. Moreover, a social engineer might try to hoax a building receptionist but if organizational security policy requires visitors to go through the security guard first, it will deter many social engineers and prevent unauthorized entry.

While deterrent controls can be implemented using physical artifacts or through software configuration, the following list identifies some physical security controls used to deter threats:

- *Cable locks:* Securing computer equipment to furniture with a cable lock deters thieves from stealing that equipment. Thieves cannot easily steal computer equipment secured this way. If they try to remove the lock, they destroy the equipment being secured. On the other hand, a thief could cut the cable with a large cable cutter. However, someone walking through a secured area with a four-foot cable cutter would certainly look suspicious.
- *Hardware locks:* Other locks such as locked doors securing a wiring closet or a server room also deter attacks. Many server bay cabinets also include locking cabinet doors.

Compensating Security Controls

Compensating controls are alternative controls used instead of a primary control. As an example, an organization might require smart cards as part of a multifactor authentication solution. However, it might take time for new employees to receive their smart card. To allow new employees to access the network and still maintain a high level of security, the organization might choose to implement a time-based one-time password (TOTP) as a compensating control. The compensating control still provides multifactor authentication.

Common Security Controls

An organization level view of an ICT security program requires the identification of common security controls that can be applied to one or more ICT systems within an organization or across an entire supply chain.

Common security controls can apply to

- All organizational ICT systems
- A group of information systems at a specific site
- Common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware embedded within ICT components) installed at multiple operational sites

While many controls are unique in their implementation, assessment, and audit procedures, common security controls have the following characteristics:

- The development, implementation, and audit of common security controls can be assigned to a centralized ICT function within the organization (other than the functional area whose systems will implement or use those common security controls).
- The results from the audit of the common security controls can be used to support the security certification and accreditation processes in the case the controls are implemented in ICT systems within federal agencies. Likewise, the results can be used for affirmation of regulatory compliance in the case the controls are implemented in ICT systems of organizations within the private sector.

Many management and operational controls (e.g., contingency planning controls, incident response controls, security awareness and training controls, personnel security controls, and physical security controls) are excellent candidates for common security control status. The underlying objective is to reduce security costs by centrally managing the development, implementation, and audit of the common security controls designated by the organization, and in turn, sharing audit results with the users of information systems where those common security controls are applied. Security controls not designated as common controls are considered system-specific controls and are the responsibility of the individual groups providing oversight of each ICT system.

A control is considered hybrid when one part of the control is common to multiple systems, while another part of the control is considered to be system specific. For example, an organization may view a security control related to incident response policy and procedures as a hybrid control with the policy portion of the control considered to be common and the procedures portion of the control, system specific.

The process of grouping security controls into either common security controls or system-specific security controls can save the organization a significant amount of money in casts associated with control development and implementation. Moreover, this grouping mechanism provides a greater degree of consistency of control application across the entire organization and its supply chain. Likewise, significant savings can also be realized in the audit process. Rather than auditing

common security controls in every information system, the audit process draws upon any applicable results from the most current assessment of the common security controls performed at the organizational level.

Implementation-Based Security Controls

Another method of classifying security controls is based on how they are implemented. The three common implementation classifications are technical, management, and operational (Figure 4.2).

- Technical controls use technology.
- Management controls use administrative or management methods.
- Operational controls are implemented by people in day-to-day operations.

Technical Controls

A technical control can be characterized as one that uses technology to reduce vulnerabilities. The security team installs and configures a technical control, and the

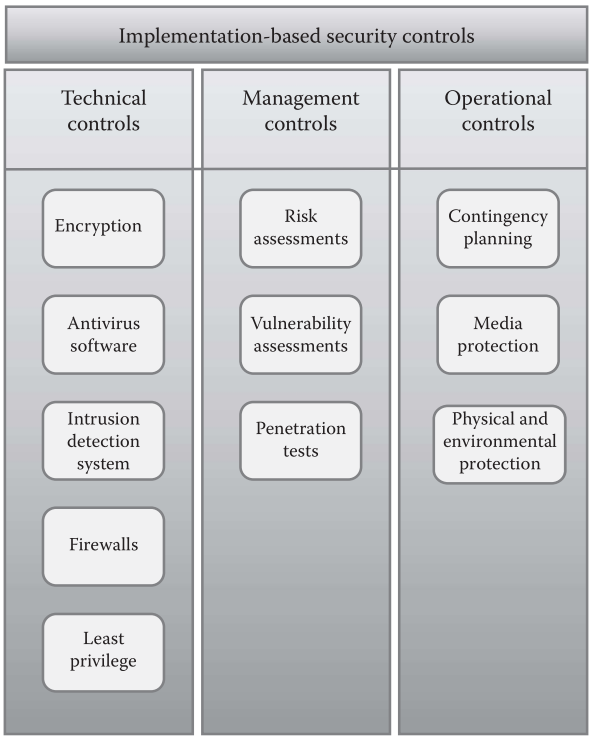

Figure 4.2 Implementation-based security goals.

technical control in turn provides the appropriate level of protection automatically. The following list provides a few examples.

- *Encryption:* Encryption is a strong technical control used to protect the confidentiality of data. This includes data transferred over a network, and data stored on devices such as servers, desktop computers, and mobile devices. Cryptography uses the combination of algorithms and public key infrastructures to convert data into an undecipherable format during transfer.
- *Antivirus software:* Once installed, the antivirus software provides protection against malware and spyware infection.
- *IDSs:* An IDS is installed and configured by an organization in order to monitor a network or host for intrusions and provide ongoing protection against identified threats.
- *Firewalls:* Network firewalls restrict network traffic going in and out of a network.
- *Least privilege:* The principle of least privilege stipulates that an individual or process is granted only the privileges needed to perform an intended task or function. Based on this principle, privileges are a combination of rights and permissions.

Management Controls

Management controls use the fundamental practices of planning and assessment to reduce and manage and mitigate risk. Most management controls require implementation of an ongoing review of an organization's risk management strategies. Some guidelines and standards refer to management controls as administrative controls, though they are two of the same. Some common management controls are as follows:

- *Risk assessment:* Is a risk management life-cycle process that serves as the means in which risks are identified, quantify, and qualified within an organization so that priorities can be established in order to focus on the most serious risks. For example, a quantitative risk assessment uses cost and asset values to quantify risks based on monetary values. A qualitative risk assessment uses judgments to categorize risks based on probability and impact.
- *Vulnerability assessment:* Is a risk management life-cycle process that attempts to identify current security vulnerabilities or weaknesses within the organization. When appropriate, additional technical and operational controls are implemented to reduce the risk from those vulnerabilities.
- *Penetration test:* Is a risk management life-cycle process that goes a step further than a vulnerability assessment by attempting to exploit identified vulnerabilities. For example, a vulnerability assessment might discover a server is not kept up-to-date with current patches making it vulnerable to security

attack. A penetration test would attempt to compromise the server by exploiting one or more of the unpatched vulnerabilities.

Operational Controls

Operational controls help ensure that day-to-day operations of an organization comply with their underlying risk management plan. The big distinction between operational and technical controls is that people (not technology) implement operational controls. Examples of operational controls include the following:

- *Contingency planning:* Business continuity includes several activities that help an organization plan and prepare for potential ICT security events. The goal is to reduce the overall impact on the organization if an event occurs.
- *Media protection:* Media includes physical media such as USB flash drives, external and internal drives, and backup tapes. The protection controls can range from protocols established for keeping media in a secure area within an organizations data center, to the secure transfer and storage of archive data at an undisclosed off-site location.
- *Physical and environmental protection:* Includes physical controls such as cameras, door locks, and environmental controls such as heating and ventilation systems. These are similar to the detective and deterrent goal-based controls discussed earlier.

Combining Implementation with Goals

It is important to note that the control types (technical, management, and operational) and control goals (preventive, detective, corrective, deterrent, and compensating) are not mutually exclusive. In other words, you can describe most controls with both terms. We just saw evidence of that in the discussion of physical and environmental protection operational controls.

As another relevant example, encryption is a preventive technical control. It prevents the loss of data confidentiality and thus classified as a preventive control and is implemented with technology so it is also classified as a technical control.

Tying Security Controls to Architecture

It is common practice for the organization to allocate security controls to an ICT system consistent with the organization's enterprise architecture and information security architecture. Enterprise architecture is a management practice employed by organizations to maximize the effectiveness of mission/business processes and information resources in helping to achieve mission/business success. "Enterprise architecture establishes a clear and unambiguous connection from investments

(including information security investments) to measurable performance improvements whether for an entire organization or portion of an organization. Enterprise architecture also provides an opportunity to standardize, consolidate, and optimize information technology assets" (Loche and Gallagher, 2011). Within the scope of standardized system life cycles, "both product and process standards contain generic advice because it has to be appropriate to all situations that the standard is written to address. For that reason, the recommendations of both product and process standards have to be customized for their advice to apply correctly. In its applied, real-world form, this customization is typically called process engineering or enterprise architecture" (Shoemaker and Sigler, 2015). Moreover, security professionals no longer view security as a product or a solution. Rather, it is commonly viewed as an in-depth system that must be incorporated throughout the business. The best way to manage security risk and compliance requirements is through a systematic approach that addresses the entire security life cycle and is built on a standards-based security infrastructure. That infrastructure is widely known as the organization's information security architecture (sometimes called enterprise information security architecture). If organizations do not implement effective security controls they place data integrity, information confidentiality, and the availability of business-critical applications at a much greater risk.

"The information security architecture is an integral part of the organization's enterprise architecture. It represents that portion of the enterprise architecture specifically addressing information system resilience and providing architectural information for the implementation of security capabilities. The primary purpose of the information security architecture is to ensure that mission/business process-driven information security requirements are consistently and cost effectively achieved in organizational information systems and the environments in which those systems operate consistent with the organizational risk management strategy" (Loche and Gallagher, 2011). As an information security architecture evolves, organizations should identify and implement common security controls supporting multiple ICT systems to the greatest extent possible. In addition to individual functional components, such ICT systems include existing and newly developed supply chain management (SCM), customer relationship management (CRM), enterprise resource planning (ERP), and electronic commerce systems. As mentioned in a previous section, when common controls are used to support a specific ICT system, they are referred to by each individual system as inherited controls. Common controls provide a cost effective and consistent information security across the organization and can, in turn, use to simplify risk management activities. Regardless of the organization's ICT infrastructure, the main point to be made is that by applying security controls to an ICT system as either system specific, hybrid, or common, it becomes a necessity for the organization to assign responsibility and accountability to each individual organizational entity to ensure the proper development, implementation, assessment, authorization, and monitoring of each of the individual controls.

The former point is not to down play the high degree of flexibility an organization has in deciding which families of security controls are appropriate to satisfy the intended identify, protect, detect, respond, and recover functional outcomes throughout the organization and its supply chain. Since the security control formulation and development process includes the assignment and establishment of security capabilities provided by the selected security controls, the organization must open the lines of effective communication among all affected individuals that are either receiving or providing the security capabilities. To that extent, the communication must include but not be limited to making certain that common control effectiveness, continuous monitoring, and audit results are readily available to the individuals within the organization and supply chain that are directly affected by the inheriting common controls, and that any configuration management applied to the common controls are effectively communicated to those affected by such changes.

Figure 4.3 illustrates how security controls are tied to enterprise IT governance and information security infrastructures within an organization using risk management to produce information for senior management, informing them on the ongoing state of organizational ICT systems security, and the missions and business processes supported by those systems.

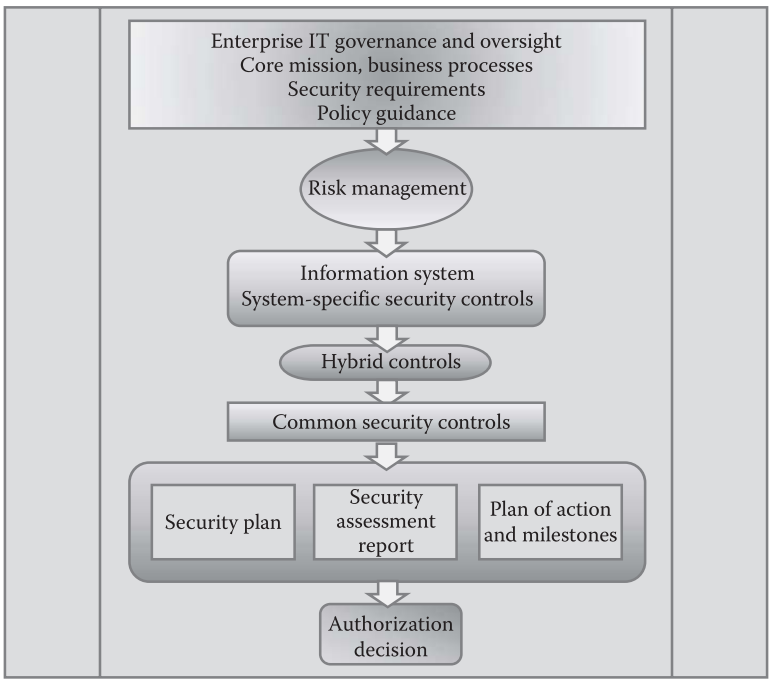

Figure 4.3 Enterprise IT governance through authorization.

The Security Control Formulation and Development Process

Any information resource with value to an organization requires some degree of security protection. For example, in the case of federal systems, the appropriate level of security is proportionate to the value of the system including the value of the system components as much as the value of the information that the system stores and processes, the degree of harm that could result from a loss of confidentiality, integrity, or availability, and the risk that such loss could occur. These factors are the focus of the risk assessment process for ICT systems and provide a starting point for formulation and development of security controls. The wide variety of ICT system components within an organization's supply chain result in significantly different security requirements, with the potential for equally different corresponding protective mechanisms to satisfy the requirements. The activities explained in this section, which make up the underlying Risk Management Framework, are intended to assist organizations in approaching cybersecurity in a consistent manner regardless of how varied or unique the ICT system components may be. The use of standard methods for categorizing, selecting, implementing authorizing, assessing, and monitoring helps to provide a consistent basis from which to make control decisions. From an organizational perspective, such a framework as associated standards provides the necessary information to align ICT risk management to organizational risk strategies and ICT governance.

Categorizing ICT Systems

The first step in the formulation and development of security controls establishes the security categorization for the ICT system. As you learned in the last chapter, federal agencies are regulated to following categorization procedures in FIPS 199 for the Federal Information Security Management Act (FISMA) systems and in Committee on National Security Systems Instruction (CNSSI) 1253 for national security systems (NIST, 2004; 2008). In addition to categorizing each ICT component and the data stored and processed within them, in step 1, the security team begins the process of developing the system security plan by documenting security categorization and system description information, while executing appropriate procedures to register the system using defined system configuration management practices. The formulation and development process begins as early in the system development life cycle (SDLC) as possible, recognizing that the tasks in this step rely on system documentation and the results of SDLC processes that must be completed first. Characterizing that statement using ISO/IEC 12207:2008—*Systems and Software Engineering—Software Lifecycle Processes* as a basis, it would be logical to suggest that the activities associated with control categorization would logically fit within the technical process group of that standard. As shown in Figure 4.4, key inputs from the early stages of the SDLC include a system concept of operations (CONOPS) or

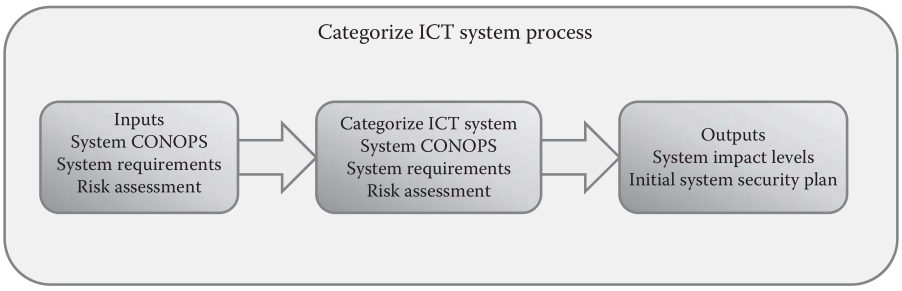

Figure 4.4 Categorize ICT system process.

other pertinent documentation, none of which are more important than the system functional and technical requirements specified within the system requirements specification. Some security and privacy documentation produced outside the control formulation process are also useful for security categorization, including privacy impact assessments and initial system risk assessments, particularly to help identify anticipated impacts from threat events and comparing those impacts to predefined levels. The impact level determined through the security categorization process is the key output of step 1, documented in the draft system security plan along with the system description.

Without discounting the importance of the planning processes that should occur before the categorization activities of the control formulation process, the ability to adequately execute subsequent steps depends largely on the results of the security categorization. Moreover, the consequence stemming from systems with higher impact level designations requiring a greater number of security controls and control enhancements, security control implementation, and assessment activities for those systems tend to take longer and require a substantially higher amount of effort and organizational resources. The tasks within the security categorization process identify the potential impact to the organization caused by the loss of confidentiality, integrity, or availability of any of the information in an ICT system. Although private sector organizations and federal agencies follow different guidelines for security categorization and security control selection, a common understanding exists on the definitions of confidentiality, integrity, and availability and of the low-, moderate-, and high-impact levels assigned to information types and information systems. Using the categorization definitions provided in CNSSI 1253 and FIPS 199 as a means to explain, Figure 4.5 shows a definition summary of each categorization level (NIST, 2004; 2008).

The process of security control categorization stipulates that organizations first identify each type of information stored or processed by an ICT system and then consider the potential impact corresponding to confidentiality, integrity, and availability. After assigning impact levels to the information types, the categorization of all data types relevant for an ICT system dictates the security categorization of the entire ICT system.

FIPS 199 security control categories and definitions	
Low	The potential impact is Low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals, other organizations, or the national security interests of the United States.
Moderate	The potential impact is Moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.
High	The potential impact is High if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

Figure 4.5 FIPS 199 security control categories and definitions.

Identifying Information Types

The first task in the security categorization process is to identify the types of information the system will receive as input, store, process, or provide as output. This step requires a thorough understanding of the system's purpose and intended use. Pertinent information resources necessary to accomplish this task are typically obtained either by reviewing the CONOPS or other system description documentation developed during the SDLC initiation phase or by discussing the system and its underlying data with the users and management from within the functional areas supported by the system. Depending on organizational policies and procedures for security categorization, organizations may group information types into categories defined by guidelines such as FIPS 199 or CNSSI 1253. Organizations need to establish and are encouraged to use catalog of information types to establish consistent information type identification and consistent security categorization determinations for information types across all the information systems an organization operates. Many federal agencies, for example, use NIST SP 800-60—*Guide to Mapping Types of Information and Information Systems to Security Categories*, as a guideline for their categorization activity (NIST, 2008). However, organizations have the flexibility to define or identify their own information types and to select their own impact levels.

Categorization of Information Types

Each information type associated with ICT systems must be evaluated to determine the potential impact to the organization stemming from the loss of the three security objectives: confidentiality, integrity, or availability. In this task, the organization considers the impact level for each security objective independently. The end

result is a three-part categorization for each information type. Syntactically, each categorization can be represented as

Information type = [confidentiality, level; integrity, level; availability, level]

Organizations need to consider many different types of possible adverse effects to accurately determine the appropriate impact level, since the impact level assigned represents the worst-case scenario, regardless of the nature of the security event. Moreover, to ensuring that system-specific impact level determinations are consistent with predetermined standards and guidelines, organizations can use impact and risk information provided in risk assessment documentation to validate their information type categorizations.

Categorization of Information Systems

Once impact levels for all information types have been assigned, the next task is to determine the security categorization for the information system by analyzing the underlying information types and adjusting the system-level categorization as necessary to reflect system-specific factors. The minimum information system security categorization for each security objective is the highest impact level assigned among any of the system's information types. This activity can be extended a step further by assigning a single security categorization value for the entire system equal to the highest impact level among the three security objectives, and using that value to determine the minimum security control baseline. In short, this means that a high-impact system is one in which at least one security objective is assigned a high-impact level, and a low-impact system would be one in which no security objectives are assigned an impact level other than low. Syntactically, each information system categorization can be represented as

Information system = [confidentiality, level; integrity, level; availability, level] = resulting level

The resulting level, as described above, is subsequently used to determine overall system security categorization and serve as the basis for selecting a security control baseline to satisfy minimum security requirements. It should be noted, that the possibility exists in which the appropriate impact level for an information system may be higher than the level produced through examination of the information types alone. Organizations may decide to raise the impact level for the system due, in part, by the following:

- The aggregate or combination of multiple information types may increase the sensitivity level, in turn increasing the risk, and as a consequence increasing the impact level.
- A connected system may have a higher impact level. Considering the interdependencies of the two systems, the impact level of the system being categorized is subsequently increased.

- Factors beyond the boundaries of the information a system may influence the potential impact to the organization if loss, damage, or compromise. In such cases, the impact level may be higher.

To that extent, organizations should categorize their systems and underlying information types based not only on the systems' intrinsic value and sensitivity of their information types but also on the impact to other systems or operational functions indirectly supported by the system.

Description of the Information Systems

The next task of the classification step of the control formulation process gathers functional and technical details about the system and documents the information in the system security plan. Because the system security plan is a vital document within the scope of the organization's overall security strategy, and also serves as the source of security requirements and corresponding controls for all organizational ICT systems, the system description should be accurate, current, and provide a significant amount of criteria that is intended to identify the characteristics of the system pertinent to the specific security measures designed to mitigate risk associated with operating the system. Each organization determines the appropriate amount of information and level of detail needed in its information system descriptions based in part by the system's security categorization, the scope or type of system, and the extent to which accompanying system documentation produced through the SDLC is available. Through this process of incorporating information system descriptions from existing security plans and other documents developed throughout the SDLC, the organization should use this as an opportunity to employ configuration management processes in order to ensure existing documents remain accurate and up-to-date.

Selection of Security Controls

The second step in the security control formulation and development process identifies the security controls necessary to satisfy an ICT system's security requirements and contains tasks associated with documenting those controls in the system security plan. From an input → processing → output perspective, the results of the system security categorization completed in the last section serve as input to the selection of security controls, considering the impact level assigned to the information system corresponds to a baseline set of security controls that, in combination, provide the minimum security necessary to protect systems categorized at each impact level. In this part of the process, organizations use security requirements and risk assessment documentation developed for the system in combination with the system security categorization to identify the appropriate security control baseline and modify that baseline to address the needs of the system. The outputs of the security control selection process, as indicated in Figure 4.6, are a tailored security control baseline, system monitoring strategy,

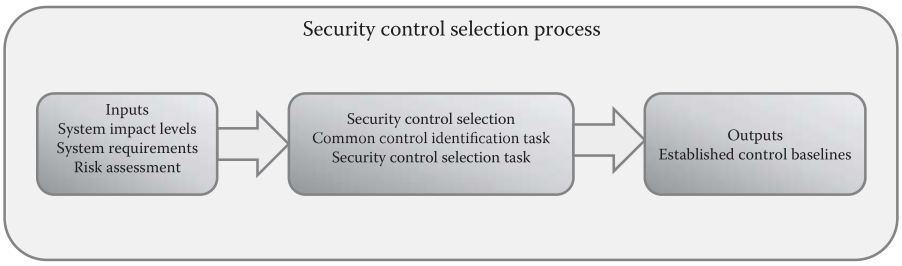

Figure 4.6 Security control selection process.

and an approved initial version of the system security plan. Security control selection identifies all the controls relevant to each ICT system regardless of which functional until or supply chain organization is responsible for providing them. Most ICT systems include a mix of system specific, common, and hybrid security controls. Security control baselines defined in system security plans indicate the type for each control and, in the case of common or hybrid controls, may incorporate control information in other system security plans. At the conclusion of this step, organizations have the information needed to finalize the resource allocation and timeline for the entire security control formulation and development process. The security control baseline defined during this step serves as the basis for security control implementation and assessment activities conducted in the next two subsequent steps. Therefore, the effectiveness of the remaining parts of the process depends on the accuracy and thoroughness of security control selection. Organizations first identify relevant controls using published standards and guidelines, as well as including system-specific considerations. Based on their knowledge of relevant controls, they are able to determine how those controls will be provided and monitored once the system is operational.

Identification of Common Controls

The entire set of security controls selected to support an ICT system typically includes both system-specific controls provided by the system or the operational and management functions dedicated to the system and common controls provided by other systems or parts of the organization (or external organizations) that protect multiple systems. As we discussed earlier in the chapter, few ICT systems have sufficient scope or resources to provide all of the necessary security controls at a system-specific level. Instead, organizations specify common controls that their ICT systems inherit, either exactly as implemented by common control providers or with some system-specific modifications, thus creating hybrid controls. Prior to selecting security controls, system owners need to identify common control providers and the security controls available for their ICT systems to use, and understand common controls in sufficient detail to determine if they meet the system's security requirements. When available common controls do not fully satisfy ICT system security

requirements, organizations must determine whether to implement a system-specific alternative or if the common control can be partially utilized as a hybrid control.

The task of identifying common controls can be performed at the organizational level, with a directory or inventory of controls made available to management overseeing the identification process. The ability to use preidentified sources of common controls vastly simplifies the control identification process for security team members and management performing the control selection process, thus eliminating the need to search for common control providers as part of the task, and allowing attention to be focused on assessing the suitability of available controls. The security team members and management performing common control identification should also be aware of the potential that more than one provider exists for the same control, as is often the case when more than one operating environment is available for information system deployment, thus adding the additional activity of evaluating the provider based on characteristics such as credibility, reliability, and their own security posture.

Based on the scope and complexity of an ICT system, many security controls are generally considered to be good candidates for inheritance from common control providers. Organizations with existing ICT security programs and well-defined management structures often take advantage of common management controls such as risk management strategies, contingency plans, and continuous monitoring strategies. Security controls that represent security requirements that many systems share can also be provided as common controls, such as those associated with security awareness and training, personnel security, and incident response. ICT systems housed within data centers or hosted by external organizations, that could extend from members of an organization's supply chain to systems that take advantage of as-a-service technologies, typically identify common controls that provide physical and environmental protection, maintenance, media protection, and configuration management, although high-impact systems or those processing other sensitive information may require system-specific controls or service-level agreements to satisfy security requirements.

We must not neglect the importance that there are also some controls for which a certain amount of system-specific implementation is expected or required, including management controls such as the system security plan, security assessments, plan of action and milestones, and privacy impact assessment. If the organization's risk management policy states that system-specific requirements be identified as part of their control implementation then hybrid controls are likely the most appropriate.

Formal Security Control Selection

While following federal standards and guidelines is not a requirement within private industries, as it is in the public sector, organizations following such standards and guidelines begin security control selection by identifying the baseline security controls corresponding to the impact level assigned to the information system during security categorization. As discussed in Chapter 3, one such guideline is NIST

Special Publication 800-53 (NIST, 2014c). Excerpts of that guide present controls based on three criteria, one each for low-impact, moderate-impact, and high-impact systems—that identify the subset of controls and control enhancements applicable to systems in each security category. The established baselines represent a starting point for the selection of security controls, serving as the basis for the reduction, or supplementation of security controls in ICT systems.

In some instances, an organization may find that a baseline security control applies for a system, but implementing the control specified in the baseline is beyond the organization's resource capacity from triple constraint (scope, time, and cost) perspective. Prior to deciding to accept, avoid, or otherwise respond to the threats and vulnerabilities affecting the organization by failing to implement a required control, management should consider the selection of compensating controls as an alternative that satisfies the same security objectives. These controls are designed to satisfy the requirement of a security measure that is determined to be too difficult or impractical to implement. For example, segregation of duties (SoD) is an internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any task. However, SoD can be difficult for businesses with small staffs. Other types of compensating controls may include maintaining and reviewing logs and audit trails. Nevertheless, compensating controls should only be used when they can be picked from a guideline such as NIST SP 800-53 or some other appropriate resource *and* the organization accepts the repercussions associated with substituting the compensating controls for those specified in the security control baseline. As with the selection of common or hybrid controls, organizations must document the selection of compensating controls and explain the rationale for choosing alternative controls instead of the ones in the baseline.

In still other cases, considering system-specific controls may also lead organizations to select supplemental security controls beyond the minimum requirements specified in the appropriate baseline for the system. Again, guidelines such as NIST SP 800-53 provide vital information for the implementation of supplemental controls and control enhancements, which organizations may elect to choose from the requirements in a higher level baseline or from among several optional controls and enhancements in the security control catalog that are not assigned a baseline. Each individual organization must determine the necessity for supplemental controls by comparing the security requirements defined for each ICT system with current capabilities and the expected effect of implementing baseline controls. Moreover, any requirements that have not been satisfied by baseline controls may indicate a need for supplemental control considerations. All decisions regarding the addition of supplemental controls or enhancements should be documented to the extent that it provides supporting feasibility analysis in order for management, and other organizations within the supply chain to understand the basis for the control implementation.

The documentation related to security controls must also include criteria related to the reductions or additions made to the security control baselines. This information

not only satisfies standardized definitions of the contents of security control documentation in the system security plan, but also provides guidance to management oversight and security team responsible for implementing and configuring the security controls to satisfy the system's defined security requirements. In most instances, management, operational, and technical controls include parameters associated with policy, acceptable use, time periods, frequency of execution, or other attributes that vary among ICT systems. Selection of controls is not complete until values for these parameters have been determined and documented at the level of abstraction necessary to support effective and efficient implementation and configuration of each control.

Milestone: Completion of the Security Plan

The completion of security control selection signifies a pivotal point within the organizations security/risk management process. While performing the tasks of control categorization and selection, organizational management responsible for along with security teams document the results of all the key activities that were performed into the system security plan and submit the plan to senior executives review and approval. This interim approval evaluates the system security plan for completeness, in addition to verifying compliance with industry and regulatory requirements in terms of content, structure, and level of detail. The approval process also aims to assess the extent to which the set of security controls selected for implementation are consistent with the impact level assigned to the system and confirm that they will satisfy the system's security requirements. At a minimum, the version of the plan submitted for approval at this stage should include a statement of the system security categorization, the system description, and also a listing of security controls selected for the system including common, hybrid, and system-specific designations. Acceptance of the system security plan by senior executives is also an important milestone in the SDLC process, as the agreed-upon set of selected security controls is a key input to system development or acquisition. It also serves as a means for verified buy-in by top-level management in terms of the significance of security requirement to the underlying efforts toward achieving the organization's strategic mission, vision, and objectives.

Implementing Security Controls

Chapter 5 will provide a complete presentation of security control activities associated with implementation. In this chapter, however, we will prepare you for that discussion by putting that process into perspective in terms of the underlying security control formulation and development process.

Through the tasks associated with security control implementation, the organization incorporates the controls identified and approved as part of the security plan within the functional and technical requirements identified for the system and its overall design. There are two primary tasks in implementation: security

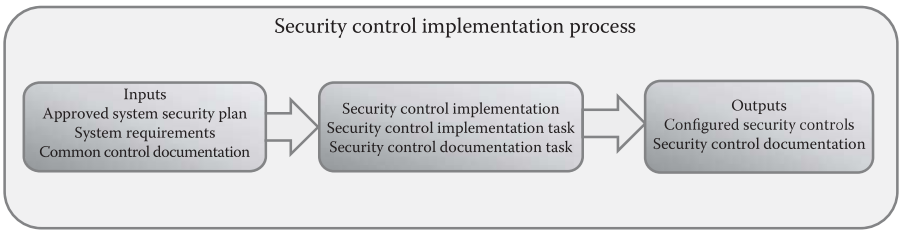

Figure 4.7 Security control implementation process.

control implementation and security control documentation. Both tasks should be completed as part of the overall development (or acquisition) and implementation processes of the SDLC. This is achieved through a series of activities in which the members of the security team responsible for ensuring the completion of the security control formulation and development process collaborate with system architects and system developers working to deliver the system. The best-case scenario would include coordinated interaction between the security team and the functional and technical members of the system development team beginning early in the SDLC so that roles and expected contributions from all team members are understood by the time the system enters the development phase. As you can see in Figure 4.7, existing documentation in the form of system requirements and descriptions of system specific and common controls developed during system categorization and security control selection provides the mechanisms from which security control implementation activities are performed. More specifically, the activities performed as part of the SDLC development phase, include architectural design, system engineering, testing, and preparation of supporting documentation. The details regarding the completion of these activities vary depending on the type of controls to be implemented and their source. That becomes important because different controls could have been custom developed, and enabled through deployment or configuration characteristics already designed into the system. Likewise, they could have been delivered using commercially available or open-source tools, or inherited from common control providers. The outputs of the implementation process include a set of implemented, correctly configured controls documented at a level of detail sufficient to support security control assessment and to allow functional and technical verification and validation against the requirements specified for the ICT system.

Setting the Stage for Control Implementation through Security Architecture Design

Coming out of the security control selection process, the security plan will provide criteria relative to what controls and control enhancements will be implemented for the ICT system. Prior to engaging in control implementation, functional and

technical members of the implementation project group facilitate decisions related to how each control will be implemented and assign responsibility of activities to be performed within the process, to individuals with the appropriate skill level and knowledge of the system; including hardware, software, and associated configurations. Managers that assign responsibilities need to be mindful that the nature of the work required to implement a control varies considerably across management, operational, and technical controls. The implementation team member will not have expertise in all three control types inclusively. Therefore, careful planning and consideration must be made relative to the individuals performing each activity and the control type being implemented.

Part of the process of designing the security architecture for the ICT system is distinguishing among the different types of controls and identifying the resources available within the organization to provide adequate support. The activities performed during architectural design consider the system as a whole, the functions, and services it will perform in the context of the organization's enterprise architecture. By approaching design from this perspective, it is easier to identify existing business processes, services, technologies, and capabilities the system may be able to reuse and ensures that the system does not conflict with or duplicate functions or services already deployed in the organization. The architecture design process also produces detailed diagrams, at varying levels of abstraction, showing the different components making up the system and its operating environment, points at which it connects to other systems or environments (internally and externally), and the placement or integration of security controls.

The underlying outcome of security architecture is to specify which security controls apply to the various components of the ICT system and clearly establish the context by which common or hybrid controls are allocated to the system. In the case of common controls, the security architecture design process must analyze the descriptions in common control documentation to understand and fulfill specified requirements for the ICT system or to determine if any of the controls are better suited for hybrid or system-specific implementation.

Control Implementation through Security Engineering

It may be appropriate to begin by understanding the definition of security engineering. Unfortunately, a generally accepted definition does not exist. There are, however, activities that are generally included in security engineering. The Systems Security Engineering Capability Maturity Model suggests the following list of activities to be generally accepted (International Organization for Standardization, 2008a):

1. Identify the organizational security risks
2. Define the security needs to counter identified risks
3. Transform the security needs into activities

4. Establish confidence and trustworthiness in correctness and effectiveness in a system
5. Determine that operational impacts due to residual security vulnerabilities in a system or its operation are tolerable (acceptable risks)
6. Integrate the efforts of all engineering disciplines and specialties into a combined understanding of the trustworthiness of a system

Current international and federal guidelines on effective information resources management stipulate the integration of security in all phases of the SDLC, a notion that is often easier to accept in principle than to put into practice. Security engineering activities are generally performed throughout the design, development, and implementation of technical controls, although published guidelines emphasize the importance of considering management and operational controls such as policies and procedures when designing and implementing system security. Important to note: security engineering within the software development life cycle consists of security-focused design, software development, coding, and configuration, some or all of which may be relevant for a given ICT system and thus considered as part of the overarching SDLC.

The advantage of applying security engineering principles to control implementation is that they provide a plethora of general guidance and protocols that establish a basis for security control design and development. However, developers and other ICT personnel charged with implementing ICT system security controls often require more explicit development and implementation instruction. While many of the popular industry standards address secure coding and associated security-related development techniques applicable to ICT systems using custom-developed software, missing from those are prescribed development practices at a level of abstraction that would provide guidance toward custom development using specific technologies or programming languages. Rather, the standards and guidelines that are currently available focus on implementing and validating secure configuration for different types of system components and ICT products. To that end, the potential for a single ICT system to implement controls subject to different standard configuration specifications, development and implementation practices, and other published sources of secure engineering, makes it essential for professionals involved in security control implementation to provide detailed documentation describing the implementation and configuration of each security control.

Security Control Documentation

In the second of two major activities in the security control implementation process, organizations should update the system security plan to describe the details of the implementation activities already having taken place. The plan should be updated with details for system specific, hybrid, and common controls (taking into consideration the details related to working with common control providers where

appropriate), and to provide criteria to emphasize the intention of engaging in security control assessment.

In addition to updated control descriptions provided in the system security plan, the implementation of management and operational controls also results in the development of several other documents that either directly represent required security controls or describe security controls as implemented. Such documents typically include plans for configuration management, contingency operations, incident response, system maintenance and administration, continuous monitoring, and security awareness and training. Documentation for technical controls not only includes technical implementation details but also functional descriptions of the expected control behavior in addition to the inputs and outputs expected for each component in the ICT system. One of the difficult tasks that managers face is determining the amount of information and level of detail to provide for each required implemented control, considering factors such as the complexity, testing, audit, and impact level of the system while also balancing the effort required to produce adequate documentation other system development processes and security control formulation and development processes potentially competing for the same resources. Organizations should make it a priority to utilize existing sources of technical documentation whenever possible while developing security control documentation; this includes gaining access to functional and technical specifications from vendors responsible for IT products incorporated into the ICT system, policies, procedures, in addition to plans for management and operational controls from the organization functional units that implement them. Likewise, similar documentation should also be sought from common control providers.

Security Control Assessment

Similar to the approach we took in the last section, Chapter 8 will provide a complete presentation of security control activities related to validation and verification. In this chapter, however, we will prepare you for that discussion by putting the process of assessment into perspective in terms of the underlying security control formulation and development process.

The security control assessment process aims to gather and evaluate security control information and evidence produced by the ICT risk management program, common control providers, and individuals responsible for developing and deploying the ICT system. The security assessment process and the security control assessors who execute it normally have no prior responsibility in the development or enhancement of any security controls. The underlying basis from which assessment works on is to consider what has already been implemented or accomplished and produce a series of conclusions as to whether the security controls implemented for the system satisfy intended objectives. Figure 4.8 depicts the security control assessment process. You can see from the figure that the entire process relies on documentation and other critical artifacts developed during prior steps of the formulation

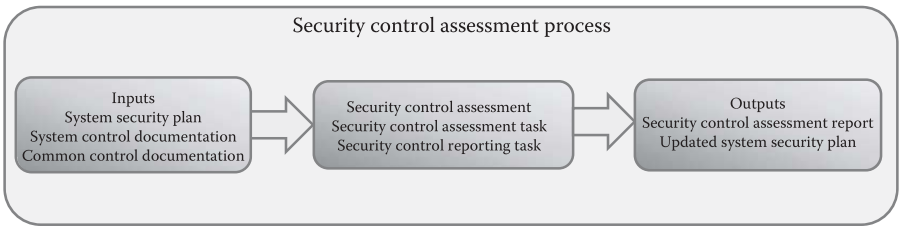

Figure 4.8 Security control assessment process.

and development process. Accordingly, it produces a separate set of documentation recording the assessment results, identifying any findings differing from expectations defined at the outset of the process, and makes recommendations for corrective actions to address any weaknesses or deficiencies found in the security posture of the ICT system.

The security control assessment and the security assessment report that gets produced during the assessment process provides vital information that can be used by management to make system-level decisions, but assessments support many other security, risk, and information resources management processes executed at a much higher level of abstraction than the processes associated with control formulation and development. "The information produced during control assessments can be used by an organization to:

- Identify potential problems or shortfalls in the organization's implementation of the Risk Management Framework
- Identify security- and privacy-related weaknesses and deficiencies in the information system and in the environment in which the system operates
- Prioritize risk mitigation decisions and associated risk mitigation activities
- Confirm that identified security- and privacy-related weaknesses and deficiencies in the information system and in the environment of operation have been addressed
- Support monitoring activities and information security and privacy situational awareness
- Facilitate security authorization decisions, privacy authorization decisions, and ongoing authorization decisions
- Inform budgetary decisions and the capital investment process" (National Institute of Standards and Technology, 2014a).

With regard to its role within the security control formulation and development process, it is important to note that security control assessment is both the main focus under discussion in this step of the process and additionally plays a key role in continuous monitoring and other operational security management activities in the subsequent step (which we discuss later in this chapter). Depending on individual

organization security objectives, security assessments can be performed at a variety of places within the SDLC, where control developers and implementers can work collaboratively on specific assessment procedures to support activities in the SDLC development and implementation phases such as design and code reviews; vulnerability scanning; functional validation; and unit, integration, and regression testing.

Since one of the primary objectives of security control assessment is the identification of weaknesses or deficiencies in implementation, organizations, and their common control providers also conduct security control assessments during the operations and maintenance phase of the SDLC to confirm the proper function and configuration of controls allocated to each ICT system. For federal agencies, periodic control assessments for operational systems help satisfy requirements specified in FISMA and provide compliancy with agency and system-specific continuous monitoring strategies developed later in the control formulation and development process.

It is not uncommon for organizations to also conduct security assessments during the disposal phase of the SDLC to help ensure that sensitive information or other assets are removed from the information system and its storage media prior to disposal.

Components of Security Control Assessment

Generally, organizations utilize security control assessment guidelines as a means for facilitating the activities of this process. For example, federal agencies are required to use NIST SP 800-53A. Private sector industries are also beginning to see the value of that publication and are beginning to implement regulations for its use. NIST SP 800-53A provides detailed assessment procedures presented in a standard format. Each assessment procedure includes one or more assessment objectives that state specifically what the assessment team is trying to determine in order to evaluate the effectiveness of each control. Every assessment objective is further, associated with assessment methods and assessment objects that define how the assessment team should evaluate the control and what the focus of evaluations using each method should be. According to the NIST SP 800-53A guideline, assessment methods include examine, interview, and test:

- The examine method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects that may include specifications, mechanisms, or activities.
- The interview method is the process of holding discussions with individuals or groups of individuals (the assessment objects) within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence regarding implemented security controls.
- The test method is the process of exercising one or more assessment (National Institute of Standards and Technology, 2014c).

The assessment team normally works closely with organizational management and other members of the security team during the security control assessment planning process to choose the appropriate methods and objects for each control and to determine the applicable scope of each assessment method. The degree to which each method is applied can vary from basic, focused, to comprehensive; resulting in a set of requirements for performing examination, interviewing, and testing with a scope and level of detail consistent with the minimum assurance requirements for the system. The guidelines that the organization uses to plan and perform the control and assessment process should describe expectations for each level defined for the examinations, interviews, and tests performed. Security control assessment teams and security teams use this guidance to plan the level of effort and amount and nature of evidence needed to perform the assessment of each control and to guide the level of detail needed for assessment information documented during the assessment process, within security assessment reports.

While the NIST SP 800 series of guidelines is quickly becoming the de facto tandard for security control formulation in addition to all other security-related policies and procedures within the public and private sector. Organizations have considerable flexibility to adapt security control assessment procedures to suit their ICT systems and the environments in which those systems operate. Much as the security control selection process allows organization to tailor minimum security baselines to reflect the requirements of each system, security personnel and security control assessment teams can tailor the recommended assessment procedures in Special Publication 800-53A or use industry-specific guidelines. In either case, the degree to which assessment protocols are presented is analogous to test plans within the system or software development life cycles. The motivation for developing such a guide is to have predefined xamination methods, interview topics, and test cases established in order to streamline the assessment process and to provide a presence of process repeatability.

The assessment cases defined in the NIST guidelines or developed proprietarily, explain specific steps the assessment team should follow to gather evidence and evaluate controls and control enhancements using each of the relevant assessment methods. Assessment cases are developed from a government or industry-wide perspective, so for organizations following procedures prescribed in industry guides, assessment cases may still need to be adjusted for organizational or system-specific requirements. Where available assessment cases must align well with organization and system-level needs. Their use can reduce the time and level of effort required to develop security assessment plans.

Conducting Security Control Assessment

Based on the criteria contained within a preapproved security control assessment plan, the process attempts to verify the implementation of security controls documented in the system security plan by examining evidence produced by control

implementers, interviewing personnel with knowledge of the system, and testing relevant controls to determine whether they function as expected. The assessment follows defined procedures included for each control in the plan, examining, interviewing, or testing relevant assessment objects and reviewing available evidence to make a determination for each assessment objective. For each determination statement included in selected assessment procedures, the evaluation of evidence by the assessment team results in a conclusion of "satisfied" or "other than satisfied." The assessment team realizes assessment objectives for each control by performing the prescribed assessment methods on appropriate assessment objects and documenting the evidence used to evaluate each determination statement. The assessment team will render a conclusion of satisfied if there is substantive evidence that the control meets the assessment objective. A finding of other than satisfied indicates that the evidence found, is insufficient to meet the assessment objective.

It is important to note that, while the discovery of weaknesses or deficiencies in a control's implementation may result in an other-than-satisfied conclusion, that same conclusion may be acceptable in other circumstances, such as cases where the assessment team cannot obtain enough information to evaluate control to the level of detail necessary. Security control assessment findings should be objective, evidence based, and indicative of the way the organization implements each security control. The assessments must be supported by documentation and observation as sources of evidence for each assessed controls and must be demonstrate completeness, correctness, and a high level of quality of evidence presented.

To justify each other-than-satisfied conclusion, the assessment team documents what aspects of the security control were deemed unsatisfactory or were unable to be assessed and describes how the control, as implemented, differs from what was planned or expected. It is important that the assessment team document security control assessment results at a level of detail appropriate for the type of assessment being performed and consistent with organizational policy and any requirements or expectations specified by the management and senior executives that will review the assessment results.

Authorizing Security Controls

The underlying focus of the authorization process is the process of

- Ensuring that managing risk from the operation and use of ICT systems is consistent with the organization's mission/business objectives and overall risk strategy previously established by senior management.
- Ensure that the information security requirements, including security controls, are properly integrated into the organization's enterprise architecture and SDLC process.

- Support consistent, well informed, and ongoing security authorization decision making through a process of continuous monitoring, while providing system transparency, and risk-related information.
- Achieve the desired level of secure information and information systems through the consistent use and reevaluation of risk mitigation strategies.

In general, security authorization is the process of assessing the overall security of an ICT system in order to identify risks and determine which of those risks have been adequately mitigated to the extent that the cost (in terms of schedule allocation, human resources, monetary expense, etc.) of exploiting them is greater than the gain for exploiting them. When risks cannot be sufficiently mitigated, the authorization process provides a vehicle for documenting those risks. Such documentation will, in turn, be used by senior management in determining whether that system can operate within the organization. A new system authorization is required with a system is initially deployed, and should be updated with each successive change to the system or the environment from which it operates. Figure 4.8 depicts the security control authorization process.

Authorization Process

Cloud-based systems have certainly changed the landscape in terms of how security strategies are formulated. However, staying within the scope of physical system, information resources are allocated to the system in order to define its boundary; selecting, implementing, assessing controls, in addition to making vital authorizing decisions. "One of the most challenging problems for information system owners, authorizing officials, chief information officers, senior information security officers, and information security architects is identifying appropriate boundaries for organizational information systems. Well-defined boundaries establish the scope of protection for organizational information systems (i.e., what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes. Information system boundaries are established in coordination with the security categorization process and before the development of security plans. Information system boundaries that are too expansive (i.e., too many system components and/or unnecessary architectural complexity) make the risk management process extremely unwieldy and complex. Boundaries that are too limited increase the number of information systems that must be separately managed and as a consequence, unnecessarily inflate the total information security costs for the organization. The following sections provide general guidelines to assist organizations in establishing appropriate system boundaries to achieve cost-effective solutions for managing information security-related risks from the operation and use of information systems" (National Institute of Standards and Technology, 2010).

The point is that even though ICT systems are decomposed into smaller subsystems, that can and should be assessed individually, the components (or subsystems) are defined upfront and authorization is applied to the ICT system as a whole. Each subsystem is composed of hardware, software, an operating system, and data stores. Selected and implemented security controls must be applied to each of these layers of the system. The previous steps of the formulation and development process we have discussed in this chapter can be interpreted as the criteria for security authorization testing, and are based on the view of systems as predefined collections of platforms, software applications, and data stores that are owned and operated by a single organization for the purpose of providing computerized resources to a select group of users.

Monitoring Security Controls

In the final phase of security control formulation and definition, the focus shifts from realizing adequate security to maintaining effective security going forward, by monitoring the system for any changes potentially impacting its security posture and adjusting the implemented security controls as necessary to keep information security risk within an acceptable level as defined in the organization's risk management plan. The objectives that an organization strives to achieve in this phase are analogues to the transition in the system or software development life cycles from the implementation phase to the operations and maintenance phase. Security monitoring is one of several operational and administrative functions implemented for each organization's ICT systems; other related processes include: configuration management, system maintenance, and system, environment, and network performance monitoring. Continuous system security management is motivated, in part, by the activities and timelines in the security plan, but also incorporates routine administrative and maintenance activities in addition to monitoring the system, its operating environment, and the possibility of the occurrence of security events or the emergence of new threats or vulnerabilities that introduce new sources of risk that must be considered as part of the organization's underlying risk management strategy. The security documentation developed during the previous phases of the security control formulation and definition process provide the basis for ongoing security management tasks, in combination with organizational risk management and continuous monitoring strategies and processes or services that help management and security teams identify threats and vulnerabilities or other factors impacting system security.

Throughout the security control monitoring phase, managers and security personnel perform many of the same tasks completed during earlier phases of the process through the activities associated with security testing, training, and the implementation of operational controls, and provide regular security status reports (as specified by the risk management plan) to senior executives. Together, this information represents key outputs of security control monitoring activities that enable

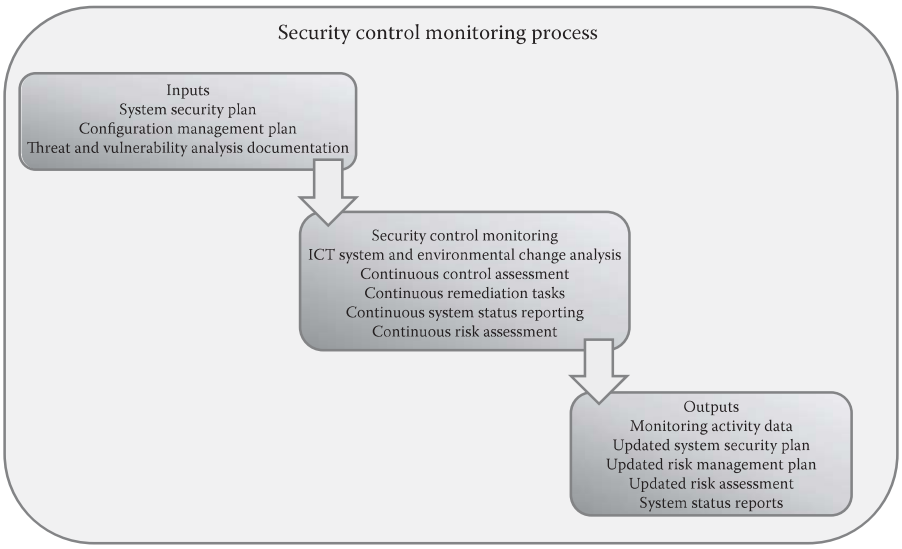

Figure 4.9 Security control monitoring process.

ongoing management of ICT security risk and help determine when more detailed reviews of system security are necessary. Figure 4.9 depicts the inputs, activities, and outputs of the security control monitoring phase.

With the exception of ICT system disposal, which only occurs after the operational and maintenance phase and the system or system component will no longer be used by the organization, the tasks of the security control monitoring phase of the formulation and development process fall within the context of continuous monitoring. These tasks include the following:

- Monitor the ICT system and environmental changes
- Conduct continuous security control assessments
- Conduct continuous remediation activities
- Continuously update security plan and risk management strategy
- Provide adequate security status reporting
- Conduct ongoing risk assessments

Monitor the System and Environmental Change

ICT systems and their associated security risk can and often do change dramatically over time. Such changes take place within system components and operating environments as well as internal or external nontechnical artifacts that pose additional threats and vulnerabilities to those systems. Monitoring for change is a key activity that emphasizes the importance of implementing a consistent, structured approach for

identifying, managing, documenting, and responding to changes that may impact the security of operational ICT systems. Continuous monitoring supports this process by identifying changes to systems and their operating environments, providing information that can be used in ongoing security control assessments. Typically, organizations implement formal configuration management and control processes to manage the tasks associated with making necessary changes to systems and their environments, using continuous monitoring to help identify internal **and** external security-related policies, procedures, and practices that require such change.

Through configuration management, ICT operations and maintenance teams should provide detailed information about system components identified as configuration items, including hardware specifications, software versions, configuration settings, and security control implementation descriptions. In combination with the details related to the environment in which the system operates, this information provides the basis for considering planned or unanticipated changes and assessing the potential security impact of those changes.

In the perfect world, organizations do not make changes to information systems without assessing the security impact in system changes. Through the task of performing impact analysis, organizations are able to determine the extent to which planned or already occurred changes to the ICT system or its operating environment affect the security posture of the system or the risk its operation poses to the organization.

Conduct Continuous Security Control Assessment

In an earlier section of this chapter, we stated that security control assessment addresses all security controls implemented for an ICT system. Its purpose is to assess the effectiveness of controls as implemented and identifying weaknesses or deficiencies that can be addressed by correcting control configurations or augmenting the implemented baseline with additional controls or control enhancements. It would be a mistake for an organization to assume that the effectiveness of security controls as assessed in the earlier phases of formulation and development will be consistent over time given the nature of changes that take place to internal and external environments in which their systems operate. New vulnerabilities often develop in operating systems, software applications, infrastructure components, external service providers, and external supply chain ICT systems, all of which may cause new sources of risk to be identified and require reevaluation of the extent to which the set of implement security controls adequately protect operational systems.

Continuous security assessments provide a mechanism for organizations to confirm the continued effectiveness of their security controls or evaluate the achievement of security objectives for changed or newly implemented controls, such as those implemented as corrective actions specified in the plan of action and milestones or in response to information system or environment changes identified through continuous monitoring.

Conduct Continuous Remediation Activities

Organizations must also have in place processes for determining appropriate remedies necessary to correct weaknesses and deficiencies discovered in ongoing assessments and documenting the actions taken. It is common practice that key individuals within the security and risk management function of an organization to receive the results of continuous monitoring activities and ongoing control assessments through routine security status reports, monitoring dashboards or other summary representations, or updated security assessment report documentation. This information is used to review recommendations for correcting weaknesses or deficiencies in their system security controls and to assess the risk, threats, and vulnerabilities that have been identified. When the appropriate course of action is risk mitigation, the organization begins the task of planning and initiating remediation activities. The plan developed for this purpose should include details related to corrective actions and the schedule for their completion to the plan and appropriate milestones.

Important to note, any security controls added, modified, or enhanced during the continuous monitoring process or as a result of ongoing security control assessments should be reassessed on a scheduled basis to ensure that the actions taken satisfactorily continue to rectify the identified weaknesses or deficiencies.

Continuously Update the Security Plan and Risk Management Strategy

In order to effectively achieve the continuous monitoring objectives of maintaining situational awareness of all operational information systems and enabling real-time risk management, organizations must establish the technical and procedural processes associated with the collection and communication of accurate security status information to affected users, senior executives, and affected third parties with established supply chain connections to the ICT system. A popular mechanism for organizations to provide this information is to implement automated monitoring tools and summarize the monitoring data they produce in a format and level of abstraction that provides adequate reporting and support for risk management implications.

Since the system security plan, risk management plan, and security assessment report collectively represent the main source of security information about an ICT system, it is imperative that organizations keep the information in these documents current, updating them as necessary to reflect changes effected as a result of continuous monitoring activities, ongoing assessments, or responses to risk associated with new threats or vulnerabilities.

Provide Adequate Security Status Reporting

The fundamental purpose of security status reporting is to summarize system security information collected through continuous monitoring and other

ongoing operational security activities and make that information available in the form of a report to operational management, senior executives, and third party suppliers whose own ICT systems are affected by the security activities performed.

Reporting occurs on an ongoing basis at a frequency and level of abstraction specified in organizational and system-specific monitoring strategies or as needed to comply with applicable regulatory requirements. The results of all ongoing security management and monitoring activities should be documented in the status reports to provide knowledge of changes or lack thereof to operational systems security, establish tracking and individual accountability for the completion of corrective actions and security-related administration and maintenance functions, and to identify trends in the organizational information security program.

Moreover, the information contained within security status reports provide current data related to the security state of each ICT system, including the effectiveness of implemented security controls where this data can be effectively collected through forms of automated monitoring. Security status reports also provide detail about the ongoing monitoring activities employed on each system. Such information contained within the reports helps management identify the types of controls or specific controls implemented, the various types of monitoring used, and indication of monitoring frequency. Another vital ingredient to the reports is that they also provide information related to the weaknesses, deficiencies, or vulnerabilities identified through security control assessments or control monitoring and report progress on resolving those issues.

Conduct Ongoing Risk Assessments

As management charged with oversight of organizational security regularly review the security status reports and updated system security documentation, their focus of attention is not only on the current changes to ICT system security changes, but also determine whether the current risk identified in the reports and documentation is acceptable to the organization. The use of automated continuous monitoring and security reporting tools can aide in the process of reassessing information security risk, although given the subjective nature of risk level assignment and the organization's determination of risk tolerance, the entire scope of risk assessment activities generally cannot be completely automated. Risk is dynamic; the sources and magnitude of risk faced by the organization change over time due to factors identified through continuous monitoring and ongoing security assessments and provided in security status reports. Management must constantly evaluate how changing circumstances affect the information security risk to the organization's underlying mission or business needs in an effort to determine the level of protection required to maintain an adequate level of security.

Chapter Summary

By definition, controls are a security mechanism, policy, or procedure that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization. The main focus of control formulation and development should be on the security of hardware, telecommunications, and software. Moreover, the level of control implementation chosen should protect sensitive information in one of the following three states: data at rest, data in transit, and data in process.

Security controls can be grouped in one of two categories: goal based and implementation. Goal-based controls are named based on the role they play in achieving adequate system security. These controls include: preventive controls that attempt to prevent an incident from occurring in the first place, detective controls that attempt to detect incidents after they have already occurred, corrective controls attempt to reverse the impact of an incident, deterrent controls that attempt to discourage individuals from causing an incident, compensating controls, which serve as alternatives used when a primary control is not feasible of sufficient, and common controls that are implemented across multiple ICT systems. Implementation-based controls are named based on the groups of individuals that implement the control and the amount of technology that control requires to adequately protect the system. These controls include: technical controls that use technology extensively, management controls use administrative or management methods, and operational controls are implemented by people in day-to-day operations.

Integrating information security into organizational infrastructure requires a carefully coordinated set of activities to ensure that fundamental requirements for information security are addressed and risk to the organization from information systems is managed efficiently and cost effectively. Security control formulation and development is a structured approach that can be used to determine the appropriate level of risk mitigation needed to protect the information systems, information, and infrastructure supporting organizational mission/business processes from security threats. The steps of this process guide organizations in developing good practices for securing its information and information systems by helping organizational leadership understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The guidelines discussed in this chapter provide a methodology that can be applied in an iterative manner to both new and legacy information systems within the context of the SDLC and the underlying enterprise architecture. The steps included within this methodology include: categorize—which considers the impact level associated with the loss of confidentiality, availability, and integrity of information and ICT system, select—in which an initial baseline of security controls is chosen supplemented as needed based on risk conditions, implementation—which are the activities associated

with the implement of security controls in the ICT system, control assessment—involves the assessment of effectiveness of the security controls implemented into the ICT system, control authorization—includes the official management decision to authorize operation of an information system and to explicitly accept the risk to organizational operations, organizational assets, individuals, other organizations based on the implementation of an agreed-upon set of security controls, and monitor—contains the activities associated with continuously monitoring and assessment of the security control implementation within the ICT system.

Key Concepts

- Regardless of the category of control, the underlying goal is to protect data at rest, data in transit, and data in process.
- One way of classifying controls is based on their goals in relationship to security incidents (preventive, deterrent, corrective, detective, and common).
- Implementation-based controls are based on how they are used and implemented within an organization. These controls consist of (technical, operational, and managerial.
- The driving force behind what and how security controls are chosen for implementation is based on enterprise IT governance and oversight, core missions and values, business processes, security requirements, and policy guidance.
- The security control formulation and development process that makes up the underlying risk management framework provide organizations a mechanism for approaching cybersecurity in a constant and organized manner.

Key Terms

Control baseline—the minimum set of security controls defined by an organization based on a predetermined level of impact.

Control formulation and development—process by which controls are categorized, selected, developed or implemented, assessed, and monitored.

Control remediation—the activities associated with resolving any issues and applying updates necessitated after discovery through control assessment and monitoring processes.

Enterprise architecture—is a conceptual blueprint that defines the structure and operation of an organization. From the perspective of this chapter and book, the intent is to determine how an organization can most effectively achieve its current and future security objectives.

Hybrid controls—a security control that is part common control and part system-specific control. A broader definition characterizes it as a customized common control.

Security posture—the approach an organization takes regarding security, from planning to implementation. It is comprised of technical and nontechnical policies, procedures and controls that provide protection from both internal and external threats.

System CONOPS—it describes systems characteristics for an ICT system from a user's perspective. Additionally, it provides the organization, mission, and objectives from an integrated systems point of view and is used to communicate quantitative and qualitative ICT system characteristics.

System-specific controls—the controls selected and implemented with the intention to be used by the ICT system for which they are designed.

References

International Organization for Standardization. (2008a). *Information Technology—Security Techniques—Systems Security Engineering—Capability Maturity Model® (SSE-CMM®): ISO/IEC 21827*. Geneva, Switzerland: ISO.

International Organization for Standardization. (2008b). *ISO/IEC 12207:2008 Systems and Software Engineering-Software Lifecycle Processes*. Geneva, Switzerland: ISO.

Loche, G. and Gallagher, P. (2011). *Managing Information Security Risk: Organization, Mission, and Information System View—NIST SP 800-39*. Gaithersburg, MD: National Institute of Standards and Technology.

National Institute of Standards and Technology. (2004). *FIPS PUB 199—Standards for Security Categorization of Federal Information Systems*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology. (2008). *Guide to Mapping Types of Information and Information Systems to Security Categories—SP 800-60*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology. (2010). *Guide for Applying the Risk Management Framework to Federal Information systems: NIST SP 800-37 Rev 1*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology. (2014a). *Assessing Security and Privacy Controls in Federal Information Systems and Organizations—Building Effective Assessment Plans: NIST SP 800-53Ar4*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology. (2014b). *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology. (2014c). *NIST SP 800-53 Rev 4: Security Controls for Federal Information Systems and Organizations*. Gaithersburg, MD: NIST.

Shoemaker, D. and Sigler, K. (2015). *Cybersecurity: Engineering a Secure Information Technology Organization*. Boston, MA: Cengage Learning.

Chapter 5

Implementing a Multitiered Governance and Control Framework in a Business

At the conclusion of this chapter, the reader will understand:

- The process for constructing formal control systems
- The practical elements of information governance
- What constitutes a control objective
- The principle domains of practical control
- The elements and steps of the control formulation process
- The general development and management of a control baseline
- The business aspects of control process formulation
- The elements of capability maturity in practical control systems

Constructing Practical Systems of Controls

The goal of this chapter is to demonstrate the practical tailoring of a standard framework into an explicit set of everyday controls. In particular, we see how a comprehensive and fully auditable cybersecurity control system (CCS) can be created and certified for compliance using a framework model. That includes the

creation of the process and mechanisms for the decomposition, risk-assessment, policy definition, discrete control creation, and maintenance of formal best-practice cybersecurity protection. In order to substantiate this, a real-world example of the implementation of this process will be provided at the end of this chapter.

In Chapter 2, we learned that a standard framework, such as ISO 27000, Control Objectives for Information and Related Technology (COBIT) or NIST SP 800-53 Rev. 4 can be adapted to serve as the template for defining a practical information governance infrastructure. And, we discovered that auditable proof of conformance to the best-practice recommendations of such a framework is an excellent means of demonstrating that the business is both trustworthy and secure. That trustworthiness can be assumed because the best practices that are embodied within such a standard model span the gamut of expert advice and consensus with respect to the correct way to ensure a given organizational application. Therefore, standard models such as 27000, COBIT, and NIST SP 800-53 can be considered to be authoritative points of reference from which an organization's across-the-board cybersecurity approach can be evaluated for adequacy and capability.

However, because they are intended to be generic, all of these models essentially serve as frameworks rather than the actual implementation of practical controls. So in that respect, they need to be viewed as comprehensive specifications of the functions required for instituting practical cybersecurity controls, rather than the controls themselves.

The creation of a functioning, real-world control system requires the performance of an individually planned and intentionally executed control formulation process within the specific setting where the controls will be operated. That process must be able to help the business deal more effectively with the many demands and requirements of cybersecurity across the organization. And, it should serve as the basis for getting that specific enterprise's information and IT-related assets under direct security control. In addition, in compliance situations, such as those imposed by FISMA, the approach should also embody some form of explicit audit mechanism that will allow the business to demonstrate both the effectiveness and also the compliance of its security controls.

Making Information Governance Tangible

As we saw in Chapter 2, the mandate of information governance is to add value to the business as well as to help it achieve its goals. Consequently, capable information governance will link technology processes, resources, and information to the overall purposes of the enterprise. And as we said earlier, since information is an asset, all organizations have the obligation to assure its uninterrupted confidentiality, integrity, and availability for use just it does for its other more common business elements such as finance.

Therefore, managers have the responsibility to establish a tangible internal control system, which will explicitly protect the everyday functioning of the information processing and retrieval processes of the particular business. In that respect, there are seven universally desirable characteristics, which an information governance infrastructure should embody:

- *Effectiveness*—that is, the organization's information must be ensured relevant and pertinent to the business process that it serves as well as delivered in a timely, correct, consistent, and usable manner.
- *Efficiency*—in the simplest terms information must be made readily available through the most optimal (productive and economical) means possible.
- *Confidentiality*—sensitive information must be protected from unauthorized disclosure or access as well as tampering.
- *Integrity*—the accuracy and completeness of information as well as its validity must be assured in accordance with the values and expectations of the business purpose.
- *Availability*—information must be accessible when required by the business process. This requirement applies to all present and future situations. It also applies to the safeguarding of the necessary resources and associated capabilities to carry this out.
- *Compliance*—all information and information processing must comply with those laws, regulations, and contractual arrangements to which the business process is subject, that is, externally imposed business criteria.
- *Reliability*—relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

These generic qualities are operationalized through an explicit set of control behaviors that are executed in a practical, day-to-day systematic fashion. In the light of defined business aims, those behaviors offer the capacity to directly mitigate and control the design, development, maintenance, and operation of the operational information and communications technology (ICT) systems of the business. Moreover, since there are never enough resources to realistically fulfill the mandate for complete trustworthiness, the overall control system formulation process should allow decision makers to perform a sort of triage in prioritizing each of these elements. Decision makers satisfy the requirement for prioritization by explicitly defining the precise level of control required for every one of the ICT functions that they are attempting to secure.

What is required to operationalize the practical intent of the generic model is for the organization to conduct a thorough security risk assessment and control formulation process. And then implement a validated set of real-world control behaviors. These control behaviors should be logically consistent in their interaction with each other. They should be fully auditable and documentable. And finally and most

importantly, they should ensure and satisfy the purpose and intent of the business operation.

Control Objectives

Since they are central to the ideas in this text, we need to stop here to define what a practical control objective is. By definition, a practical control objective is a precise account of the desired behavior. That includes the purpose to be achieved by implementing that given set of defined actions. As a consequence, a precise statement of expected behavior must accompany each control objective. The statement must explicitly justify and explain how that behavior will achieve the general requirement for effectiveness, efficiency, confidentially, integrity, availability, compliance, and reliability.

Control objectives establish a clear and distinct link between the anticipated security protection and the business purposes. In that respect, control objectives can be considered to be the specification of the exact set of activities that the ICT function proposes to carry out in order to achieve stated business goals. Control objectives provide a concrete description of the requisite outcome of an explicitly specified action.

Therefore, control objectives must be stated in an action-oriented way and they must directly accomplish some explicit business purpose that has been described by the business strategic planning function. Since the organization's control objectives have been traditionally "businessy" in nature, they have always tended to be focused on supporting the financial accounting aspects of the business. The large organizational control standards that we are discussing here simply adopt conventional security best practice into a specification of the same kind of mechanism for ensuring systematic cybersecurity functioning.

Given that intention, the models discussed in this chapter are all guidelines for the classification of control objectives in order to achieve the security purposes of an organization. They specify an explicit set of high-level control objectives for each of the security domains that make up the model. Then each of the detailed control objectives in the model is tied to a general business requirement for secure information. This applies to the various areas of need within the organization. In addition, each specific control objective behavior has to be directly traceable to the information resource it has been set to control.

Besides the control traceability requirement, the standard areas of organizational functioning addressed by the model should have at least one high-level control objective associated with it. In addition, a rationale must be provided for the inclusion of whatever behavior is specified as part of the actual security system. Besides rationalizing the inclusion of a control behavior, there should also be a specification of the presumed impact of not achieving a business goal. The latter feature will aid the real-world prioritization process.

Finally, there must be some form of tangible specification of the approach that will be employed to evaluate the effectiveness of each control objective. The performance of each control objective has to be capable of being tangibly assessed. Therefore, each specified objective must be stated in terms that will support the precise measurement of operational performance.

That assessment must be driven by assignment of the priority of the information elements that are most critical to the business process. As a consequence, the actual outcome of the specification of control performance assessment is an explicit evaluation based on the real-world measurement and prioritization criteria. That outcome gives the organization the practical means to determine if, or when, a process has been successfully completed. If there is also a compliance requirement, there has to be a specific definition of the approach that will be used to audit the controls.

The Process of Defining and Implementing Security Controls

The security controls that are implemented by an organization are always defined by a risk assessment. This risk evaluation is done first in order to identify the elements of the relevant model that are applicable to a particular business situation. Both ISO 27000 and COBIT touch on every aspect of IT security. They help the organization examine and categorize all of the risks and legal requirements associated with its information assets. Neither of these standards hammers the shape of the organization's security processes into a narrowly defined or rigid mold. Instead, the control objective categories force the organization to examine every aspect of the requisite security system.

The actual deployment of controls is driven by managerial decision making about the degree of security that is required within a particular setting. And the understanding that underlies this approach is that all situations are different. Thus the requirements of all of these standards force companies to undertake a step-by-step assessment of their security needs and appropriate responsibilities with respect to their information assets.

The actual control formulation process centers on defining and deploying a set of rational actions that are designed to ensure that a given aspect of the company's information resources is secured. The process starts with the formulation of explicit policies toward each of the protected artifacts and elements that will fall within the secured space. Then it ranges down to the more detailed implementation issues, which are identified by the risk assessment and managed by the control objectives.

The control models under discussion here are structured on one simple and pragmatic belief. That is, cybersecurity can be best understood and the actual assurance defined using a standard set of common categories of security functioning. The security itself is then implemented by the definition and deployment of

specifically designed control objective behaviors. Accordingly, all of these frameworks define an explicit set of high-level areas of control and an appropriate number of control objective requirements are specified within those domains. The complete set of these control objectives is assumed to describe and embody all aspects of security for the operation.

By developing concrete mitigation responses to the specification of control behavior requirements, the organization can ensure that a capable, real-world, control-based ICT security system is in place for any type of organization and at any level of security desired. The risk assessment that guides the implementation process is a necessary requirement for establishing that control. Management then uses the selected risk assessment approach to map where the organization is in relation to the best-practice requirements that are specified in the standard.

However, besides the ability to address identified risk, the practical realization of a security control framework also has to be periodically judged for effectiveness. Therefore, a defined set of critical success factors also has to accompany the security system plan. They are normally subjective rather than concrete. These factors include qualities like "reliable" or "easy to modify." And the terminology is expressed in ways that management can easily grasp and act on.

Since these factors are subjective, objective, or empirical, measures have to be defined to make these factors meaningful to managers. The aim is to let management understand whether a process has achieved its assurance objectives. Also critical success factors force the organization to address such vital management questions as: How far should we go to secure something and is the cost justified? What are the indicators of good security performance? What are risks of not achieving our objectives? What do others do? and How do we compare against best practice?

The standards we are discussing are meant to be generic. Or in simple terms, they are appropriate to almost any conceivable security requirement and situation worldwide. The security categories in these models are also proactive, in the sense that they prescribe a typical set of actions that should be taken in order to provide active working security assurance in a given area of organizational functioning. Thus, for the purposes of implementation, they require an organization to develop and document an explicit statement of the approach that will be taken to address the specific security risks that have been identified for each aspect of the operation. That includes executing a process to prioritize the complete set of organizational information resources in terms of the level of protection required. Once the prioritization is done, the organization can specify evidence that will indicate that the appropriate level of protection has been successfully reached.

Finally, the implementation of every one of these standards requires a complete specification of the threats, vulnerabilities, and weaknesses that are associated with each asset. This is necessary in order to insure proper defense in depth. Therefore,

there must also be a ranking of the relative priority and impact of each threat. Finally, these guidelines require that the organization itemize the measures that will be used to monitor and judge ongoing operational performance. If there are best-practice benchmarks involved in the actual determination of operational performance, those also have to be specified and their use clarified—for example, how they will be derived and used.

Establishing the Management System

As mentioned previously, the practical outcome of the implementation process is a tangible control-based system, which can be assumed to sufficiently protect ICT resource within the general security parameters of the organization. ISO 27000 dictates a specific process to develop that management framework, which it specifies in detail in ISO 27002. NIST 800-53 also has a process that is outlined in Federal Information Processing Standards (FIPS) 199. COBIT's implementation process is specified in the Information System Audit and Control Association's Management Guidelines. The documentation that is produced during the operation of this formal system of controls is what is referenced by the auditors in order to verify conformance to the principles of the given model. There are three different types of documentation artifacts involved in the process. The first of these are the documents that comprise the inputs to the implementation process itself. These inputs explicitly describe the various organizational context issues about which a policy decision must be made.

The initial documentation comes from the gap analysis. Using the recommended best practices as the point of reference, the organization identifies and prioritizes the threats it faces and the vulnerabilities that those represent. Essentially, any failure to comply with the recommendations of best practice represents a point of vulnerability. The organizations bases its decisions about the level of response to those identified vulnerabilities on its understanding of the harm that might come to its information and communication technology assets as a result of not responding to the threat.

Then, the substantive form of the response is structured based on the actual recommendations of the model. The response itself is operationalized through the standard procedures that the organization establishes as part of the implementation/tailoring of the generic practices of the model. The outcome of the tailoring amounts to the functioning security system with all of its controls and interactions in place. Finally, the documentation produced by the day to day operation of the controls drives the management of the overall security activity for the purposes of compliance oversight and audit.

The actual implementation of a standard is normally done in six practical phases, the first two of which involve the establishment of a formal security infrastructure that is based on the definition of comprehensive cybersecurity policy and

the setting of the boundaries of control. Factors that might enter into this activity include such issues as: what is the level of criticality for each of the information assets within the scope of the system, and what is the degree of assurance required for each?

This is often expressed in the form of a 10-point asset classification rating that (for example) can range from "not needed" on one end of the scale all the way up to "the business would close without this" on the other end. Some other infrastructure considerations may include any foreseen strategic initiatives as well as any market or regulatory influences. The boundary setting element of this is particularly important since there is an obvious direct relationship between the resources required to establish the security level specified and the extent of the territory that must be secured (Figure 5.1).

The organization performs a risk assessment following this. The risk assessment may be the most important element in the process, because it captures and categorizes the actual threats to the business's information assets. Since a particular threat may not necessarily have much impact within a given situation, all risk situations are evaluated once they have been identified in order to distinguish only those circumstances that would enable specific and undesirable vulnerabilities. Then the resulting vulnerability picture is carefully examined with respect to the detailed organizational situation. The aim is to precisely describe the form and function of the specific weaknesses that has been identified and which the security controls need to directly target. As we have said before, these weaknesses are then prioritized so that the ones with the most critical impacts are dealt with first.

The next step in the process implements the actual risk controls. These substantive controls must provably address the findings obtained by the risk assessment. The deployment of controls is done in the order established by the priorities defined in the prior step. Moreover, so that these procedures can be monitored and assessed the appropriate measurement criteria are identified, operationalized, and referenced to each procedure.

Finally, a statement of applicability is written and documented for each control that is deployed. This statement itemizes the target asset to be secured along with the reasons for the control's selection, the quantitative measure that will be used to determine whether that control's objective's has been met, and the resources necessary to achieve that desired result. This establishes a history for each control and it

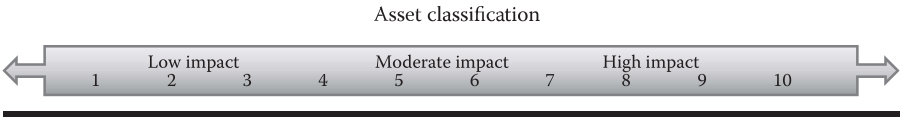

Figure 5.1 Asset classification continuum.

allows for rational modification as the organizational threat environment changes over time.

Standard Security Principles Derived from Standards

We have talked about these standards without discussing the various domains that comprise them. So in this section, we are going to factor out the common principles of security as represented by these models and then we examine each of these at some length. There are three influential control frameworks in the national and international space. These are the ISO 27000 model, which is a product of the International Organization for Standardization of Geneva, Switzerland. There is the FIPS 200 model that has been developed for federal information systems by the National Institute of Standards and Technology in Gaithersburg, Maryland. Finally, there is the COBIT model, which is a proprietary product of the Information Systems Audit and Control Association (ISACA) of Arlington Heights, Illinois. Each of these frameworks has an explicit set of security domains associated with it and each of those domains embodies a particular collection of underlying controls. Figure 5.2 provides a summary.

Please note that the much greater length of the third column (COBIT) in Figure 5.2 is due to the fact that the model is best represented by the high-level controls rather than the domains. There is considerable commonality between these three models. That allows us to tease out common principles of control coverage, which are shown in Figure 5.3 and specified in the following section.

Principle 1: Strategic planning-policy controls (FIPS 200–Planning–27000–Policy–COBIT–Planning and organization). Logically, the organization needs to develop a formal, comprehensive set of cybersecurity policies, which are promulgated organization wide in a customary policy stipulation document. In addition, there must be formal mechanisms in place to review, evaluate, and refine the policy set on a regular basis. This is the "big-picture" requirement that all frameworks enforce in order to prevent piecemeal solutions. The organization has to implement whatever management control it desires in a consistent, across the board manner. The aim is to ensure systematic deployment of procedure and operation of the security controls within the overall governance framework of the organization. Strategic planning and policy formulation is an intentional act. Therefore, it is sponsored and conducted at the top by the organization's policy decision makers. It is a future-oriented process that attempts to mitigate risk in the most cost efficient and effective manner possible. It is also a cyclical process, normally conducted on annual bases as all other forms of strategic plans are developed.

Principle 2: Operational security controls (FIPS 200–Accountability/integrity–27000–Process organization–COBIT–Delivery and support). The effect of this principle is to stipulate the need for day-to-day management of the controls that comprise the cybersecurity infrastructure that is created by the "Strategic Planning" principle (1). This includes the organization's commitment to formally organize

Security domains of three common standard models			
FIPS 200	**ISO 27002:2013**	**COBIT 5**	**COBIT 5 (continued)**
1. Access control (AC)	1. Information security policies	P01. Define a strategic IT plan	DS9. Manage the configuration
2. Awareness and training (AT)	2. Organization of information security	P02. Define the information architecture	DS10. Manage problems
3. Audit and accountability (AU)	3. Human resource security	P03. Determine technological direction	DS11. Manage data
4. Certification, accreditation, and security assessments (CA)	4. Asset management	P04. Define IT processes, organization, and relationships	DS12. Manage the physical environment
5. Configuration management (CM)	5. Access control	P05. Manage the IT investment	DS13. Manage operations
6. Contingency planning (CP)	6. Cryptography	P06. Communicate management aims and direction	ME1. Monitor and emulate IT performance
7. Identification and authentication (IA)	7. Physical and environmental security	P07. Manage IT human resources	ME2. Monitor and emulate internal control
8. Incident response (IR)	8. Operations security	P08. Manage quality	ME3. Ensure compliance with external requirements
9. Maintenance (MA)	9. Communications security	P09. Assess and manage IT risks	ME4. Provide IT governance
10. Media protection (MP)	10. System acquisition, development, and maintenance	P010. Manage projects	DS12. Manage the physical environment
11. Physical and environmental protection (PE)	11. Supplier relationships	AI1. Identify automated solutions	DS13. Manage operations
12. Planning (PL)	12. Information security incident management	AI2. Acquire and maintain application software	ME1. Monitor and emulate IT performance
13. Personnel security (PS)	13. Information security aspects of business continuity management	AI3. Acquire and maintain technology infrastructure	ME2. Monitor and emulate internal control
14. Risk assessment (RA)	14. Compliance	AI4. Enable operation and use	ME3. Ensure compliance with external requirements
15. System and services acquisition (SA)		AI5. Procure IT resources	ME4. Provide IT governance
16. System and communications protection (SC)		AI6. Manage changes	
17. System and information integrity		AI7. Install and accredit solutions and changes	
		DS1. Define and manage service levels	
		DS2. Manage third-party services	
		DS3. Manage performance and capacity	
		DS4. Ensure continuous service	
		DS5. Ensure systems security	
		DS6. Identify and allocate costs	
		DS7. Educate and train users	
		DS8. Manage service desk and incidents	

Figure 5.2 **Security domains of three common standard models.**

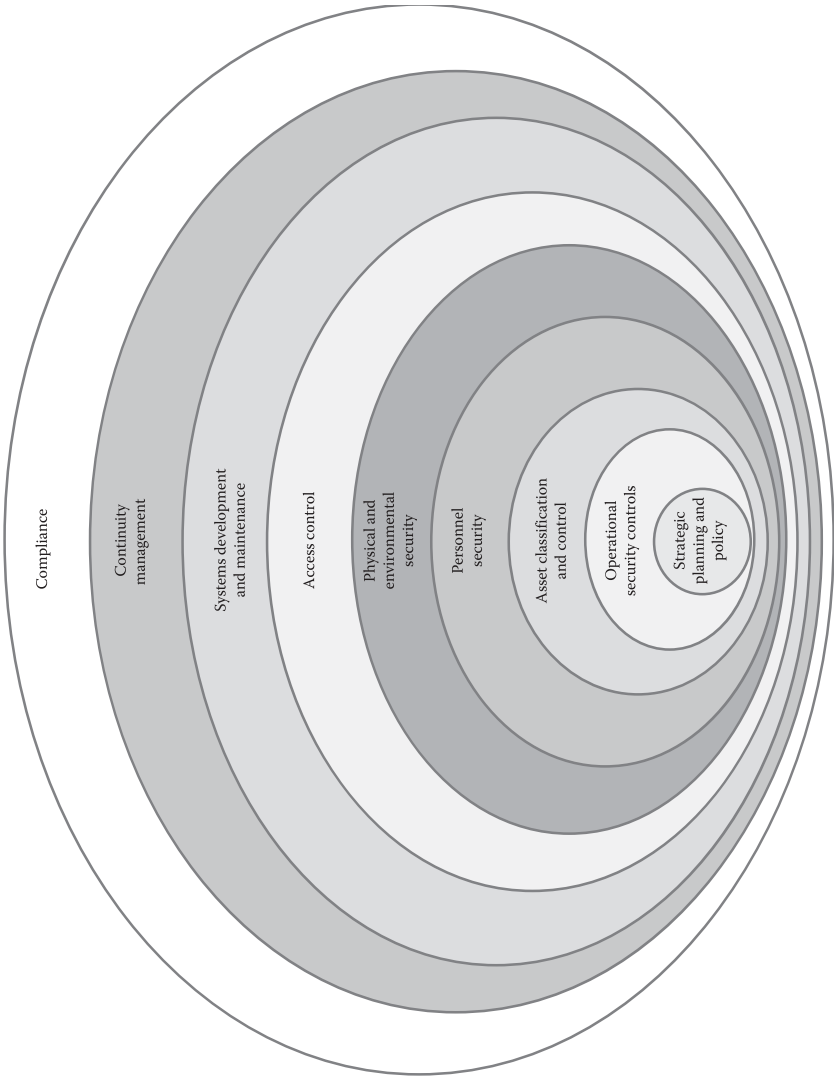

Figure 5.3 Nine common principles of control coverage.

and coordinate its security functions by explicitly allocating the accountability for cybersecurity among its management personnel and units and then following up with oversight activities such as reviews as audits. That includes assigning housekeeping details such as the detailing of the authority for control of information processing facilities and the specification of how and where to seek advice on security from experts (e.g., consultants) and specialists. Finally, external issues such as the procedures for inter-organization cooperation and third-party access, as well as independent review of these procedures need to be specified in the form of explicit behaviors. This includes the means that will be employed to identify the risks associated with third parties as well as the security requirements, specifically with respect to third-party contracts. Explicitly, the policy and the mechanism for assuring the security requirements of outsourced contracts must be specified.

There are five general control issues associated with the establishment of operational security. The first is the requirement to define operational procedures and responsibilities in unambiguous terms. These range through such diverse areas as the mechanisms for operational change control, incident management, and external facilities management. The second issue is the requirement to develop procedures for system management, including capacity planning and system assurance procedures. The third is the means that will be employed to protect against malicious actions against the system. That includes the need to explicitly define the controls against malicious software. The fourth is the need for secure operational procedures including how and when to utilize a procedure, how the procedure will be validated, and assurance and the rules for operator threat assessment and reporting. The fifth control is the requirement for explicit management policies that can be embedded in information and communication technology system operations. That includes at a minimum the explicit specification of the behavioral controls.

Principle 3: Asset classification and control (FIPS 200–Identification–27000–Asset management–COBIT–Define architecture and relationships). This principle has two simple but very essential elements associated with it. First, the organization must spell out the rules and procedures; it will employ to account for its assets. Then these assets must be inventoried, uniformly labeled and formulated into rational and coherent baselines, which (as they are developed) are placed under formal change management. Second, the same rigorous process must be applied to the classification and control operations for the control set for those assets. This includes preparing a policy and procedure that itemizes how present and future information and its associated controls will be classified and managed as well as spells out how information assets will be labeled and handled. The controls themselves are also baselined and placed under change control.

Principle 4: Personnel security (FIPS 200–Personnel security–27000–Personnel security–COBIT–Manage human resources). This domain requires careful and rigorous control since over a third of the cybersecurity incidents perpetrated each year relate to human behavior exploits such as insider theft. Therefore, the organization has a responsibility to prepare and document the procedures that are required

to insure the appropriate execution of the terms and conditions of employment for the organization. Much of the definition of the controls for this is embodied in the principles of Saltzer and Schroder (1975). That includes the necessary controls to ensure the effective definition of job responsibilities, effective screening of personnel and the arrangement of controls to protect sensitive material from unauthorized access, as well as the responsibility to undertake systematic cybersecurity education and training. This also involves the need to stipulate procedures that will ensure that personnel will respond appropriately to security incidents and malfunctions, report security incidents, and weaknesses that they encounter in their duties, report control, or system malfunctions and to develop lessons learned from incidents.

Along with all of these requirements, the organization must also formally define and publicize the disciplinary process that will apply to any personnel who breach those procedures. Of all of the issues embodied in personnel security, this is the one that might be the most important, since members of the organization have to be made to understand the consequences of security violations if the control system is to work at all. The aim of the enforcement process is to put consequences in place to ensure that violations of security are NOT the result of personnel simply ignoring correct procedure.

If security discipline is to be enforced, it will require a concomitant disciplinary process that details the exact consequences of violating controls over such humble day-to-day violations as not protecting passwords. In many cases, these violations can be attributed to sheer ignorance. But, since part of the purpose of a personnel security process is to ensure a proper level of security awareness among members of the workforce, something such as a defined and detailed disciplinary policy for security violations is a necessary adjunct, if nothing more than to get the staff's undivided attention.

Principle 5: Physical and environmental security (FIPS 200–Physical protection–27000–Physical security–COBIT–Manage facilities). This principle embodies the control objectives associated with traditional physical security. Since this area is often the only one that is actually allocated a set of tangible controls when an organization attempts to secure itself, this also serves to illustrate how necessary a complete specification of all of the elements of cybersecurity is. Although physical security is obviously important, it is only one of the aspects of complete cybersecurity. So, an organization that relies on securing just the physical elements of its operation might be considered to be unsecured.

The control objectives embraced by this area include the responsibility to define secure areas and the physical security perimeter, including the mechanisms for controlling physical entry, securing offices rooms and facilities, working in secure areas, securing isolated delivery and loading areas, and generally securing the equipment. This includes controls for properly protecting IT devices, as well as maintaining them, insuring uninterrupted power supplies, safeguarding the cabling, and protecting the equipment off site. Moreover, once the equipment has

reached the end of its useful life, there must be controls in place that will ensure secure disposal or reuse.

Finally, there are two humble but very critical and often overlooked controls that are invoked by this security principle. That is the requirement for good security hygiene as well as the requirement that a policy for removal of property be made explicit and understood organization wide. Borrowing a laptop for a weekend is a potentially serious security violation, particularly if it contains sensitive data. And it is something that organizations as powerful and allegedly secure as the Pentagon and the National Security Agency (NSA) have suffered from. Nevertheless, in the absence of appropriate policy, it might seem logical for a zealous employee to see that act as a sign of commitment to the job rather than a critical breach of the organization's security protection.

Principle 6: Access control (FIPS 200–Access control–27000–Access control–COBIT–Ensure system security). This principle ensures accurate identification and authorization of system access. It involves six general control areas. The first of these is the classic access control policy definition process. For instance, will the access control be role based or mandatory, how will authorizations be maintained, and so on. And following logically along behind that first step is the requirement, that these policies be clearly stated and the enforcement mechanism publicized throughout the organization. That includes a specification of how users will be registered, how privileges will be assigned and managed, how passwords will be assigned, and how user access rights will be reviewed. The third requirement is for tangible user access management controls to be established and assured to be working correctly as well as effectively.

Then there are a series of electronically focused control requirements. The fourth requirement is for electronic access control to be created. This includes many detailed technical elements, such as user authentication procedures and node authentication, but it also requires that the organization formulate a policy toward the operation of network services. The fifth requirement looks at operating system access control. This includes such highly technical elements as automatic terminal identification policies, and use of system utilities. The sixth requirement involves the traditional definition of procedures to control application access. This makes this principle very important to the general purposes of securing information assets. It includes a number of traditional control elements, such as how access to information will be restricted as well as controls to ensure that sensitive systems will be isolated from access by mainstream users.

Principle 7: Systems development and maintenance (FIPS 200–System and services acquisition–27000–Information systems life-cycle management–COBIT–Entire acquisition and implementation domain). This area encompasses all of the lifecycle process related to the development and acquisition of systems and software. The control requirements for securing systems and software throughout the lifecycle must be spelled out including such high-level things as the specification of the rules for software engineering practice as well as simple things like

procedures for data validation and message authentication. Because cryptography is an important aspect of electronic security that also includes the specification of cryptographic controls, this area includes all of the wonderfully elegant technical areas such as encryption, digital signing, and key management.

Another control element on the business side is the requirement that policies exist to assure the security of system files. That includes such things as how access to program and source code will be controlled and how system test data will be secured. However, there is also an implicit requirement for good software engineering management practice. So, there have to be process controls in place to ensure security in the development and sustainment activities of the organization including procedures for change control, technical reviews, and outsourced software development.

Principle 8: Continuity management (FIPS 200–Contingency planning–27000–Continuity–COBIT–Ensure continuous service). For the business side of the operation, this is an extremely important aspect of cybersecurity, since it requires that all aspects of business continuity management be considered and spelled out in the form of procedural controls. This includes the requirement that a business continuity management process, exist, ongoing business continuity, and impact analyses be performed and that continuity plans are written and implemented within a business continuity planning framework. This is another one of those frequently overlooked aspects of cybersecurity since it is not technical. Therefore, the continuity process is often conducted wholly on the business side of the strategic planning function. And, it takes place without reference to the technical issues that might be raised as part of the contingency planning. But, it is the backbone of insuring organizational survivability, which further serves to illustrate the practical importance of this principle.

Principle 9: Compliance (FIPS 200–Compliance–27000–Compliance–COBIT–Ensure compliance). Compliance is another business function, but it is also obviously a critical element of assuring information assets. Therefore, an integrated and effective set of controls are required. Compliance controls ensure that policies and procedures (primarily audit) exist that bring the organization into conformance with any and all external and internal legal requirements including intellectual property rights and privacy issues. The control set should also safeguard data and ensure technical compliance with regulatory standards.

The compliance principle is another example of why a comprehensive definition of security risks is a vital part of organizational survival. Since, generally speaking the people in the technical part of the business operation are neither aware of compliance concerns, nor do they consider it part of their responsibility. Nevertheless, failure to have controls in place to ensure due diligence in protecting the organization from violations in an applicable legal or regulatory area can lead to the sort of litigation that bankrupts businesses. Thus, a robust set of controls to ensure legal and regulatory compliance is an important part of any business's cybersecurity defenses.

Building the Security Control System

There is a standard generic process for implementing a control system. The form of this standard approach is dictated by the necessity to deploy a comprehensive set of systematic practices, not just address ad hoc problems. Because of the requirement to make the actual security solution complete and systematic there is an implicit order and logic to the implementation process based on the common goal, which is to ensure effective protection. Thus most real-world implementation processes follow the same general lines outlined here. Given the need to get to one common destination, most organizations implement the security control deployment process in nine stages (Figure 5.4).

Initial Setup and Tradeoffs

Information Gathering

The first stage understandably involves the gathering of all of the pertinent information necessary to define the form of the operational Cybersecurity Management System (CMS). That includes the identification, labeling, and valuation of all of the assets and the formulation of these into a comprehensive asset control baseline. This baseline is normally maintained under the dictates of rigorous, configuration management control.

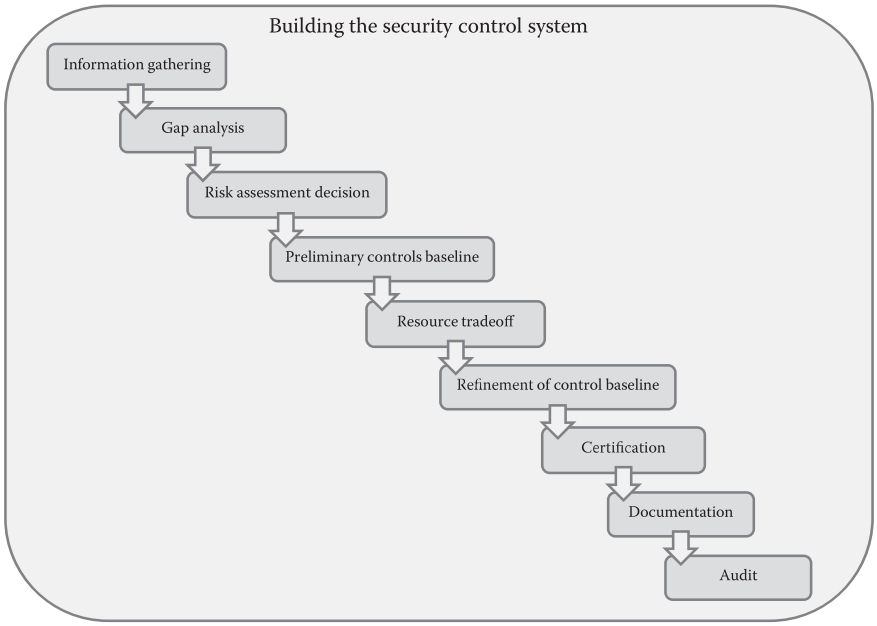

Figure 5.4 The security control deployment process.

Gap Analysis

Once all of the organization's information assets have been identified and baselined, the next step is to perform a security gap analysis. The purpose of this is to determine the exact status of the information protection safeguards that are already in place for each of the individual asset items in the baseline. This involves the identification of all of the direct threats, vulnerabilities, and weaknesses to the ICT base as well as any other contextual factors that might impact security, such as legal and contractual requirements and any current and projected business requirements.

Risk-Assessment Decision

This step requires the organization to make a considered decision about the findings of the gap analysis. As we said, this is not a simple matter of plugging holes, since it is likely that a comprehensive gap analysis will identify more existing vulnerabilities than the organization would ever have the resources to address. Consequently, a formally designated set of managers needs to perform a triage activity in order to prioritize and address the existing security concerns in such a way that the organization's critical functions will be adequately protected.

Preliminary Control Baseline

Once the management team feels as though it has gotten a handle on the security issues for their particular areas of responsibility, they will select a suitable set of control objectives from the reference model that they have adopted. Again, it needs to be stressed that there are a number of models for doing this. Nonetheless, there is an obligation to fully implement the recommendations of the one that is selected. This includes the development of a complete specification of all of the appropriate controls to address all of the threats and vulnerabilities identified in the gap analysis for any given area of best practice. In addition to the identified gaps, the controls must also satisfy any other legal, contractual, or business requirement that might have been identified.

Resource Tradeoff

Once the entire set of controls has been identified, the organization's decision makers undertake a rational and explicit tradeoff process that weighs the inherent impact of the threat against the resources required to address each item on the priority list. In simple terms, this means that the estimated cost of implementing the necessary controls is traded off against the potential business impacts of the threat.

This process is applied to the identified threats and vulnerabilities as well as any other identified legal, contractual, and/or business vulnerabilities. The rule

that applies here is that the probability of the risk actually occurring must be balanced against the resources that would be required to eliminate it. The eventual outcome is a sliding scale set of recommendations called a risk reduction decision, which outlines the consequences of the range of viable responses to the problem, for example, a partial solution, against the estimated business cost should the expected impact materialize. This set of recommendations will range between not dealing with the threat at all, all the way up to deploying all of the resources required to completely eliminate it.

Selection of Final Control Set

Refinement of the Control Baseline

The next three steps are really aspects of the same activity. Once all of the elements of risk and resources are understood, it is time to refine the initial baseline of controls. As the title of this section implies that amounts to an iterative validation and enhancement process. The initial control deployment—the one for which the resource tradeoff was carried out—is a beta version of the operational control set. It is put in place as a sounding board for the evaluation of the selected controls over time. Over the initial setup period, the organization will decide on and fine-tune the eventual operational control set. These are the day-to-day behaviors that the organization's decision makers feel are the most effective steps for the assurance of its ICT assets.

Alterations to the operational set of controls are based on the feedback that is obtained from the users and stakeholders in the organization. Normally, the evaluation period will involve a significant period of time. During this time, changes are permitted based on the tenets of good configuration management practice. However, the long-term goal is still the finalization of the control set for long-term use. Once that final set is assessed and appears to be working properly, they are placed under a baseline configuration control, which is maintained under formal configuration management best practice. This is often the final stage in the assurance process unless the organization elects to move to the certification phase outlined next.

Certification

This stage is not necessarily the goal of the process in the sense that the purposes of the standards, we are discussing, are fulfilled by the completion of the prior stages. However, many organizations elect to pursue formal certification of their systems either to gain business advantage, as would be the case with ISO 27000 assessments, or because of compliance mandates such as those that are associated with NIST 800-53. If that is the case, it is necessary to prepare formal, written statements of applicability for every one of the control objectives that are selected and implemented in the operational systems as well as an explanation as to why all other standard controls have not been chosen.

Like threat assessment and control formulation processes, the justification process is also iterative. The organization examines all of its embedded controls and relates each of them to threat issues that substantiate their operation. One of the more important adjuncts to this process is the preparation of the justification for the controls that have *not* been selected. It is sometimes more important and difficult from an audit standpoint to be able to understand the lack of the presence of a control that has been recommended by the standard model. Therefore, the aim of the justification for *not* implementing the control has to provide the impact, likelihood, or economic justification for why the control was not included in the operational security system.

Properly done the documentation of the included controls along with the explanation for why a control has been omitted should provide a clear and unambiguous statement about the strategic security goals that underlies the implementation and operation of a particular cybersecurity system. This statement should serve as the lynchpin for the ongoing operation and sustainment of the security state that has been chosen by the organization, and it should also provide an authoritative road map for future security system development.

Once the organization is confident that it has its operational security system well in hand and functioning as intended a third-party auditor is contacted to perform the actual assessment for the purposes of certification. This assessment is normally carried out in the same fashion as any other compliance audit and it involves the presentation and evaluation of all forms of documentation relevant to and supporting the correctness of the operation.

There are currently a number of national bodies capable of granting certification depending on the standard. Generally, ISO certifies ISO 27000 implementation through agencies such as the United Kingdom Accreditation Service (UKAS), which is the national accrediting body of the United Kingdom. UKAS maintains that status through IRCA under EA-7-03 Accreditation Guidelines for Info Security Systems and ISO/IEC Guide 61:1996.

ISACA does not offer certification accreditation to COBIT. However, COBIT does provide the best practice basis for Sarbanes–Oxley (SOX) compliance under the SOX Act of 2002. The Public Company Accounting Oversight Board (PCAOB) defines the criteria for SOX compliance. And by convention the control objectives within the COBIT model are considered to be sufficient to demonstrate that those criteria have been satisfied. The audit is normally conducted by a licensed CPA firm against the stipulations of the COBIT controls and the certification of adequate control over financial reporting is based on the presence of any material weakness in control implementation.

The NIST 800-53 standard controls are the basis for the satisfaction of the legal requirements of the Federal Information Security Management Act (2002). The certification of system security as defined by those controls is required as part of the granting of an approval to operate any federal information system. That process is slightly different from the other two certifications in that there must first be an

assessment of sensitivity of the information for classification purposes as defined by FIPS 199. Once the sensitivity has been defined, the baseline control formulation using the recommendations of FIPS 200/NIST 800-53 is undertaken using the appropriate control set.

Practical Implementation: How to Establish a Real, Working Control Framework

As we just said, the process of implementing a comprehensive set of controls entails the identification, prioritization, assurance, and sustainment of an effective response to every plausible threat. This control deployment function is not a one-shot "front-end" to setting up a static security solution. It is a constant and organized probing of the environment to sense the presence of and respond appropriately to any potential sources of harm to the organization's information assets (Figure 5.5).

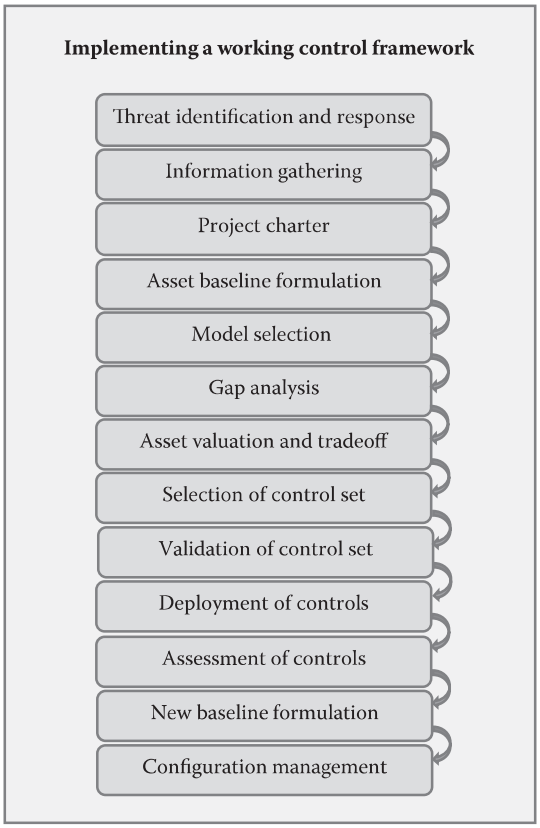

Figure 5.5 Implementing a working control framework.

Logically, the first step in formulating a correct security response is threat identification. That amounts to the systematic identification of **any** threats in the organization's technical or operating base that might lead to the loss of **any** information, of **any** value. And then the deployment of an effective set of controls to alleviate each vulnerability identified. There are two types of activities. The first type involves the steps to obtain corporate buy-in, the actual identification and labeling of the assets, the selection of an appropriate model of best practice and the subsequent strategic deployment of the controls based on resources available are the essential subfunctions of this phase. This part of the process drives the resource allocation decisions as well as the development and refinement of the optimum set of controls. It is termed the "threat identification and response" phase.

The second phase is aimed at the definition of the tangible cybersecurity system. We are going to discuss each of these phases in turn in detail. The threat identification and response phase is composed of the following four elements:

1. Information gathering and chartering
2. Asset baseline formulation
3. Model selection and gap analysis
4. Asset valuation and tradeoff

The aim of these four activities is to achieve an understanding of the security response that is appropriate to the precise situation. And which fits within the constraints of the organization. Properly executed, it is conducted in the background of day-to-day organizational functioning.

In practice, this activity employs methods and tools to identify, analyze, plan for, and control any potentially harmful or undesirable event. It should be noted that while the overall aim of the threat identification process is to prevent or minimize the impact of threats at the business level of the organization. Technical risks are also managed since they often constitute the root cause for business breaches or losses.

Threat understanding approaches must establish a disciplined environment for proactive decision making. They should regularly assess what could go wrong and then determine the approach and timing by which each potential threat will be countered. This all takes place within the constraints of practical business considerations such as resources available and time. Business constraints are an important consideration for a realistic solution since it is highly likely that more risks will be identified than can possibly be responded to. So, it is important to at least address the ones that pose the most potential harm to the corporation.

Finally, we want to stress that the form of the process as well as the scope of the solution is dictated by the type of control desired. Consequently, the substance of the identification, analysis, planning and control elements, and activities required is going to vary. It is also important to keep in mind that the actual business

considerations vary with the focus and intent of the organization. Thus a project chartering prestep might be required. Charters are a form of contract. The drawing up of a charter often proceeds major engineering activities, that is because the creation of a comprehensive control system is expensive and can often be disruptive to the general flow of business. Therefore, the project requires up-front commitment. Operationally, the right set of representatives formulates the requirements for the control system into a statement of need. This is then documented and authorized by the appropriate executive decision makers and distributed to the business at-large.

The only purpose of this phase is to serve as a launch pad for the decision making with respect to the specific control model that will be utilized. So logically, the charter should generally define both the scope and extent of the desired control. In practice, this stage is probably the least substantive aspect in the sense that it does not really touch on any of the details of the requisite control scheme. Nonetheless, it might be the single likeliest point of failure. That is because everything that will happen downstream originates from this one point. As a consequence, it is important for everybody who will have anything to do with the control system understand and agree on the type and degree of protection at the beginning of the process.

In effect, a charter should accomplish two critical purposes. From a functional governance standpoint, it has to ensure that the project is properly targeted. More importantly, it should also support the education and buy-in of the people who are going to be actively involved in formulating the actual system. That is, because it is well documented that the long-term success of any solution is directly dependent on the level of support for the process. Comprehensive organizational control deployment is not an inconsequential exercise and it can be resource intensive. The execution of this process is generally based on generic business analysis approaches. So, there are numerous recognized ways of actually conducting this. However, there is only one absolute requirement, which is that the eventual outcome has to be sponsored at the highest levels of the company.

There have been a number of studies to support the idea that the ownership should be at the level of the board of directors or CEO. Notwithstanding that, the literature is unanimous in stressing that effective control solutions have to be thoroughly embedded in the everyday functioning of the organization. That requires across-the-board acceptance, which can only be enforced through executive sponsorship. One final point also must be stressed, which is that the information-gathering function should not degenerate into a detailed technical problem solving process. The only objective of this first stage is to define the general form of the problem for the purpose of determining an explicit strategic direction. There are many reasons why a complete framework solution may not be appropriate, ranging from a lack of resources all the way to knowledge of a specific targeted need. These must all be identified, brought forward, and agreed on in order to choose a proper

scope and appropriate model for the eventual response. Since the decision makers are conventional executives, they are never interested in the details only in the assurance that the correct target will be hit. Consequently, the first phase has to be conducted with that single goal in mind.

Once the direction is chosen, the form of the rest of the process is dependent on the model selected and that activity constitutes the rest of this stage. The selection of an appropriate model is crucial, because the only way that the control scheme will work is if the model it is based on fits the organization's control needs. The only rule is that whatever is eventually developed should fit the particular requirements of the situation. This is both an intelligent design process as well as a political one. As such the findings of the information-gathering process must be rigorously adhered to in order to guide that decision-making process. And the eventual model selected should always meet the requirements that have been "bought into" by the whole organization through the chartering process. Since the next phase of the process starts the tactical implementation of the control solution, this initial stage is the point where the strategy is set.

This second stage is probably the least commonly understood of the control system implementation steps in that for most assurance tasks the substantive form of the assets to be controlled is known. In the case of information and communication technology, the asset base is an abstract construct, which could legitimately have many forms. Therefore, before control schemes can be devised, the boundaries and material form of the asset must be characterized. That involves gathering all of the pertinent information necessary to define the complete form of the assets that will be protected. This involves the meticulous identification and labeling of every item under control of the control system. It is a prerequisite for subsequent assessment of risk because it establishes the "day one" state of the organization's total set of information assets.

In practice, the aggregate set of assets is termed a "baseline." The individual components that constitute this baseline must be explicitly identified and labeled as part of the asset identification process. A precisely defined information asset baseline is an absolute prerequisite for the conduct of the rest of the process, since it is this explicit configuration that is maintained by the control system. And because it is a tangible structure, the classification and tagging of the asset elements that constitute it is usually based on their logical interrelationships with each other.

This is maintained as a top-down hierarchy of elements that ranges from a view of the ICT asset as a single entity down to the explicit items that constitute that resource at its basic functional level. The baseline scheme that emerges at the lowest level of decomposition represents the concrete architecture of the target information asset. It must be noted that the decisions that determine what this asset base looks like are normally made using the input of a number of different participants. That could range from the technical staff all the way up to executive owners of a

given information item. The items defined at any level in the hierarchy are then given unique and appropriate labels that are explicitly associated with the overall organization of the information asset itself.

Once the asset baseline is established the next step is to do a gap analysis against the strategic model to be utilized. We have highlighted the three that are arguably the most popular, but there are a wide range of applicable models. The only condition is that one framework should be utilized, not a combination. That is because the specifications of the model are used to perform the gap analysis. The requirement for a gap analysis is common to most threat analysis situations. The gap analysis is always applied uniformly across the organization. That is, because the point of the gap analysis is to identify **risks** created by gaps in operating procedures. The gap analysis is arguably the most important element in any control implementation, because it identifies the places of potential weakness, assesses the harm that might ensue from each, and analyzes and categorizes options for response.

Operationally, this process is carried out by comparing the form of the current operation against the comprehensive set of control objectives specified in the selected control framework model. This is done to identify the gaps that exist. These gaps represent the deficiencies and material weaknesses that must be addressed by new procedures if the threat is to be mitigated. Since a particular gap may not have much impact for a given situation, it is important to only focus on priority gaps. Thus, once all of the gaps are identified, they are assessed to distinguish only those that would create specific and undesirable weaknesses.

Next, these weaknesses are carefully analyzed with respect to the particular organizational situation. The analysis is aimed at identifying the specific elements of the weaknesses that the control system needs to target directly. The weaknesses are prioritized so that the ones with the most critical impacts are dealt with first. The process can best be described by looking at it from the standpoint of the documentation that is utilized to carry it out. In fact, the tangible documentation set is so important that it is generally the only thing that an auditor uses to verify that a selected model has been implemented properly. This documentation will drive the activity in subsequent stages where the organization will make decisions about the actions that must be taken to address each identified weakness as well as how it will document the control system for the purposes of management oversight and audit.

The next subphase is the asset valuation and tradeoff process. The product of this phase is a concrete governance strategy. The input is derived from the outcomes of the prior three stages. The boundary setting element is particularly important to this consideration since there is a direct relationship between resources required to establish a control level specified and the extent of the territory that must be secured. Operational factors that enter into the development of this strategy include: what is the level of criticality of each particular information asset that falls into the asset baseline? What is the specific degree of resource commitment required to control it? Thus the most important aspect of this might lie in the simple valuation of the assets themselves.

This is the case because in the real-world, there are never enough resources to absolutely control every element of the information asset baseline. And since that baseline is overwhelmingly composed of abstract entities, the value of that asset base is also abstract, meaning not known. Therefore, it is essential for each organization to undertake a formal approach to systematically value and prioritize its information assets in a way that the most important assets are targeted first. Since, this is a resource decision the assumption is that the critical success factors are defined at the business level. And any form of operational asset valuation must be rooted in and reflect the vision, strategies, and purposes of that part of the organization.

The tradeoff process is a political one; however, it is necessary because the actual tradeoff is the fundamental element of strategic planning for control. This is not a scientific activity though. Nevertheless, with precisely targeted information decision makers can move ahead with some assurance that they are basing their strategies on the realities of the situation. The assumption is that the actual deployment of the control functions will meet the requirements of the project charter, which was drawn up at the front of the process. That decision making is based on knowledge of the financial equipment and personnel resources available to implement the desired level of control, and the pressing business concerns and the relative value of the asset. The point is to get a clear fix on the asset base so that the particulars of the deployment can be planned with precision. This should be both tangibly documented and publicized to the organization at large. This also effectively concludes the threat identification and response phase of the formal control system implementation process.

The next step in this process is the actual selection and validation of the control set. This phase involves tailoring, deploying, and validating an appropriate set of technical and behavioral controls. This is 99.999% of the time the same model employed to do the gap analysis, although not absolutely required. The only rule is that the control set has to address the priority requirements for control. The implementation is unique in the sense that the deployment is determined by the situation. However, there are three elements that must be carried out no matter which model is selected:

1. Assignment of controls to a control baseline
2. Assessment of the effectiveness of those controls
3. The formulation of the final control set into a control system

The necessary controls are deployed once the information asset baseline has been established and prioritized. This requires an item-by-item assessment of the information and communication technology resource baseline in order to design and formalize the appropriate control set. Nonetheless, in order to devise the appropriate and correct set of control procedures, it is necessary to return to the risk analysis to better understand the nature of the threat.

Basically threats can be characterized as physical or logical, from internal or external sources. Thus, the analysis considers the controls that are necessary to suitably address any and all anticipated threats from every given source. That includes steps to detect a threat as close to the time that it occurs (threat response). And a procedure to ensure that it will be either attended to by subsequent corrective action or that the loss that may arise from it will be effectively contained. Since adverse impacts of threats also inevitably fall into the financial arena, it is important to consider the applicable ROI issues.

One obvious example is that it ought to be a certainty that the cost of the control would be less than any anticipated dollar losses. Another consideration is the frequency with which the threat occurs. If the historical rate of occurrence is high than even a low ROI item could prove to be a good investment. The other issue is the *probability* that a threat might occur. Probability should never be confused with frequency. In essence, the question that has to be asked is, "What is the probability that harm might ensue if a threat occurs?" And, the answer would be how likely it is that a given occurrence will produce adverse results.

Finally, it must be recognized that there is always an uncertainty in all of these cases that dictates that baseline control formulation should always be an iterative function. Basically, uncertainty can be estimated as a level of confidence, from 0% to 100% on any control. What this expresses is the necessity or usefulness of the associated control. It should be noted that the failure to integrate uncertainty factors will reduce the overall level of trust in the effectiveness of the resultant control baseline.

It is necessary to validate the selected control set in order to assure the effectiveness as well as confirm the accuracy of the defensive scheme. This always takes place after it is operationally deployed. That is, it is formulated into an active baseline and placed under effective baseline control. From a control deployment standpoint, this activity is a standard beta-test function in the sense that the essence of the process is the ongoing comparison of expected performance with the actual result of executing the process.

The assessment process is planned, implemented, and monitored in the same fashion as any other testing activity. It normally embodies the criteria and factors considered during the threat analysis and baseline formulation process, but operational issues can be added at this point as well. The intention is to be able to say with assurance that the aggregate control set is effective within the aims of the control scheme. Operationally, this should be done within a specified time frame as well as a defined reporting and decision making structure. Because the overall purpose of this step is to produce a finalized baseline, the organization must treat it exactly like a project in the sense that the outcome of the process is a fully functioning control set for everyday use.

Once the project purposes and timelines are set, generally speaking each control must have a set of performance assessment criteria assigned. The purpose of this is to underwrite precise monitoring of the effectiveness of each component of the control baseline. Therefore, these criteria must be both measurable and able to be

recorded. Then on execution of the process, the outcome data associated with each control is recorded. The organization uses the ongoing outcomes of the operational use of the control to assess its effectiveness.

This assessment is based on the performance criteria set for that particular control as well as the assumptions about cost and occurrence that were part of the baseline formulation process. Then, once the testing step is complete the aggregate set of results for the control baseline is assessed for the purposes of formalizing a finalized set of control objectives. These controls represent the operational realization of the control system. And their baseline representation is maintained under strict change control by the configuration management process. The released version of the information and communication technology asset baseline and its associated control baseline is managed by configuration management in the same manner as a software release. That is, no changes are allowed without authorization and subsequent verification of the correctness and effectiveness of the change.

Ensuring Long-Term Control Capability

The ISACA (COBIT), ISO, and NIST frameworks outline controls for a comprehensive set of logical domains within the IT environment. Each of these areas is intended to control some specific aspect of cybersecurity operation. In order to implement that control, there are high-level control statements for each domain and a variable number of explicit detailed control behaviors specified that operationalize the intent of each domain. However, given the number and complexity of the control procedures that might be developed and implemented to embody the desired level of control, there is a requirement that these procedures be evaluated for effectiveness. Or in simple terms, the fact that a control has been defined and documented does not de facto mean that it can be relied on. So, given the importance of organizational controls in each area of operational function, a mechanism to rate their effectiveness can be a useful tool, which is true both for reasons of assurance and also for the purpose of insuring continuous improvement of the security function. That is what we are discussing here.

It is possible to assess the effectiveness of each security control using a maturity rating scale. Logically, this is based on simple principles of best practice laid out in several similar capability models. The assumption is that capability is directly tied to the level of definition and execution of the process. Every one of the currently existing capability maturity frameworks assumes that a capable process is one that embodies the following five common elements:

1. Defined and documented policies and processes
2. Clear lines of accountability
3. Strong support and commitment from management
4. Complete and appropriate communication mechanisms
5. Consistent measurement practices

The levels of capability are normally expressed in terms of the performance of the practices associated with the control. Those practical performance levels are as follows:

1. Absent—not found or no response
2. Low—process is ad hoc and disorganized
3. Moderate—process follows a regular pattern but not documented
4. Contained—best practices documented and understood
5. Managed—process is monitored and measured
6. Optimized—change management is employed

These levels build on each other. For instance, the activities installed at the managed level are carried out in addition to the performance of the already existing best practices from the prior level.

The business can benchmark itself along this maturity rating scale both in terms of the effectiveness of individual control objectives and as a total entity. And it can aim to achieve higher levels of maturity by increasing the effort that it commits to the formulation and documentation of its controls. This can be supported by any explicit audit or review process that might be selected to augment performance. The advantage of a maturity framework in the implementation of effective organization-wide controls is that it provides a direction for the development of the overall cybersecurity governance function. This approach should be familiar to most IT organizations in that they do not build anything complex in a single pass. Instead they approach problems in an iterative fashion, continually refining their understanding and the relative quality of what they are creating. Implementing control through a defined maturity path provides the motivation for an organization to both start the process as well as continuously enhance its control systems. In that practical respect, a maturity framework could be as important to successful security protection as the control objectives themselves.

Chapter Summary

Standard frameworks, such as ISO 27000, COBIT, or NIST 800-53(4) can be adapted to serve as the template for defining a practical information governance infrastructure. And we discovered that auditable proof of conformance to the best-practice recommendations of such a framework is an excellent means of demonstrating that the business is both trustworthy and secure. That trustworthiness can be assumed, because the best practices that are embodied within such a standard model span the gamut of expert advice and consensus with respect to the correct way to ensure a given organizational application. Therefore, standard models such as 27000, COBIT, and 800-53 can be considered to be authoritative points of reference from which an organization's across the board cybersecurity approach can be evaluated for adequacy and capability.

The creation of a functioning, real-world control system requires the performance of an individually planned and intentionally executed control formulation process within the specific setting where the controls will be operated. That process must be able to help the business deal more effectively with the many demands and requirements of cybersecurity across the organization. And it should serve as the basis for getting that specific enterprise's information and IT-related assets under direct security control.

Managers have the responsibility to establish a tangible internal control system, which will explicitly protect the everyday functioning of the information processing and retrieval processes of the particular business. In that respect, there are seven universally desirable characteristics, which an information governance infrastructure should embody.

These generic qualities are operationalized through an explicit set of control behaviors that are executed in a practical, day-to-day systematic fashion. In the light of defined business aims, those behaviors offer the capacity to directly mitigate and control the design, development, maintenance, and operation of the operational ICT systems of the business. Moreover, since there are never enough resources to realistically fulfill the mandate for complete trustworthiness, the overall control system formulation process should allow decision makers to perform a sort of triage in prioritizing each of these elements. Decision makers satisfy the requirement for prioritization by explicitly defining the precise level of control required for every one of the ICT functions that they are attempting to secure.

The actual deployment of controls is driven by managerial decision making about the degree of control that is required within a particular setting. And the understanding that underlies this approach is that all situations are different. Thus, the requirements of all of these standards force companies to undertake a step-by-step assessment of their security needs and appropriate responsibilities with respect to their information assets.

The actual control formulation process centers on defining and deploying a set of rational actions that are designed to ensure that a given aspect of the company's information resources is secured. The process starts with the formulation of explicit policies toward each of the protected artifacts and elements that will fall within the secured space. Then it ranges down to the more detailed implementation issues, which are identified by the risk assessment and managed by the control objectives.

By developing concrete mitigation responses to the specification of control behavior requirements, the organization can ensure that a capable, real-world, control-based ICT security system is in place for any type of organization and at any level of security desired. The risk assessment that guides the implementation process is a necessary requirement for establishing that control. Management then uses the selected risk assessment approach to map where the organization is in relation to the best-practice requirements that are specified in the standard.

The documentation that is produced during the operation of this formal system of controls is what is referenced by the auditors in order to verify conformance to

the principles of the given model. There are three different types of documentation artifacts involved in the process. The first of these are the documents that comprise the inputs to the implementation process itself. These inputs explicitly describe the various organizational context issues about which a policy decision must be made.

The initial documentation comes from the gap analysis. Using the recommended best practices as the point of reference, the organization identifies and prioritizes the threats it faces and the vulnerabilities that those represent. Essentially, any failure to comply with the recommendations of best practice represents a point of vulnerability. The organizations bases its decisions about the level of response to those identified vulnerabilities on its understanding of the harm that might come to its information and communication technology assets as a result of not responding to the threat.

Then the substantive form of the response is structured based on the actual recommendations of the model. The response itself is operationalized through the standard procedures that the organization establishes as part of the implementation/tailoring of the generic practices of the model. The outcome of the tailoring amounts to the functioning security system with all of its controls and interactions in place. Finally, the documentation produced by the day to day operation of the controls drives the management of the overall security activity for the purposes of compliance oversight and audit.

There is a standard generic process for implementing a control system. The form of this standard approach is dictated by the necessity to deploy a comprehensive set of systematic practices, not just address ad hoc problems. Because of the requirement to make the actual security solution complete and systematic, there is an implicit order and logic to the implementation process based on the common goal, which is to ensure effective protection. Thus, most real-world implementation processes follow the same general lines outlined here. Given the need to get to one common destination, most organizations implement the security control deployment process in nine stages.

This process is applied to the identified threats and vulnerabilities as well as any other identified legal, contractual, and/or business vulnerabilities. The rule that applies here is that the probability of the risk actually occurring must be balanced against the resources that would be required to eliminate it. The eventual outcome is a sliding scale set of recommendations called a risk reduction decision—which outlines the consequences of the range of viable responses to the problem, for example, a partial solution—against the estimated business cost should the expected impact materialize. This set of recommendations will range between not dealing with the threat at all, all the way up to deploying all of the resources required to completely eliminate it.

Alterations to the operational set of controls are based on the feedback that is obtained from the users and stakeholders in the organization. Normally, the evaluation period will involve a significant period of time. During this time, changes are permitted based on the tenets of good configuration management practice. However, the long-term goal is still the finalization of the control set for long-term

use. Once that final set is assessed and appears to be working properly, they are placed under a baseline configuration control, which is maintained under formal, configuration management best practice. This is often the final stage in the assurance process unless the organization elects to move to the certification phase.

Like threat assessment and control formulation processes, the justification process is also iterative. The organization examines all of its embedded controls and relates each of them to threat issues that substantiate their operation. One of the more important adjunct to this process is the preparation of the justification for the controls that have **not** been selected. It is sometimes more important and difficult from an audit standpoint to be able to understand the lack of the presence of a control that has been recommended by the standard model. Therefore, the aim of the justification for **not** implementing the control has to provide the impact, likelihood, or economic justification for why the control was not included in the operational security system.

Given the number and complexity of the control procedures that might be developed and implemented to embody the desired level of control, there is a requirement that these procedures be evaluated for effectiveness. Or in simple terms, the fact that a control has been defined and documented does not de facto mean that it can be relied on. So, given the importance of organizational controls in each area of operational function, a mechanism to rate their effectiveness can be a useful tool. That is true both for reasons of assurance and also for the purpose of insuring continuous improvement of the security function. That is what we are discussing here.

It is possible to assess the effectiveness of each security control using a maturity rating scale. Logically, this is based on simple principles of best practice laid out in several similar capability models. The assumption is that capability is directly tied to the level of definition and execution of the process. Every one of the currently existing capability maturity frameworks assumes that a capable process is one that embodies common elements.

The business can benchmark itself along this maturity rating scale both in terms of the effectiveness of individual control objectives and as a total entity. And it can aim to achieve higher levels of maturity by increasing the effort that it commits to the formulation and documentation of its controls. This can be supported by any explicit audit or review process that might be selected to augment performance.

The advantage of a maturity framework in the implementation of effective organization-wide controls is that it provides a direction for the development of the overall cybersecurity governance function. This approach should be familiar to most IT organizations in that they do not build anything complex in a single pass. Instead they approach problems in an iterative fashion, continually refining their understanding and the relative quality of what they are creating. Implementing control through a defined maturity path provides the motivation for an organization to both start the process as well as continuously enhance its control systems. In that practical respect, a maturity framework could be as important to successful security protection as the control objectives themselves.

Key Concepts

- Controls are deployed to address substantively documented threats.
- Controls enforce governance.
- Controls are explicitly observable behaviors expressed as objectives.
- Strategic governance is enabled by a comprehensive set of controls.
- There is a generic process for applying all large control models.
- Every control deployment is tailored to every situation.
- The aim of practical tailoring is to create an everyday control set.
- Controls are implemented through gap analysis.
- Resource tradeoffs are necessary because all threats cannot be addressed.
- Control needs to be a living process updated by reviews and audits.
- Controls ensure a number of basic principles of security.
- Controls are arrayed in a baseline and managed under change management.
- The aim of capability maturity is to increase the effectiveness of organizational control models.

Key Terms

Control behavior—the actual operation of the control in real-world application.
Control framework—the specific array of controls utilized in the particular application.
Control model—a set of best practices arrayed in a commonly accepted general framework.
Control objective—a formally defined desirable outcome from the implementation and execution of an explicit control behavior.
Compliance—a state of agreement or alignment with formally expressed criteria.
Gap (gap analysis)—the process of estimating the presence of a threat based on the absence of a considered best practice.
Governance control—a strategic state where organizational actions are stated as explicitly auditable behavior.
Maturity model—a staged series of increasingly effective best practices arrayed for common application in a real-world setting.
Operational security—a predictable state of security enforced by an explicit set of controls.
Resource tradeoff—the process of decision making with respect to the cost and effectiveness of a given approach to control.
Risk analysis—an estimation of the level of harm that will result from the actions of a known threat.
Strategic planning—actions taken to ensure complete and comprehensive long-term deployment of a control set.

References

Information Systems Audit and Control Association. (2013). *Control Objectives for IT (COBIT) v5*. Arlington Heights, IL: ISACA.

International Organization for Standardization. (2012). *ISO 27000, Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*. Geneva, Switzerland: ISO.

National Institute of Standards and Technology. (2006). *NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*. Computer Security Division, Information Technology Laboratory, NIST. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf, Accessed July, 2015.

Privacy Rights Clearinghouse. (2014). *Chronology of Data Breaches Security Breaches 2005—Present*. San Diego, CA: PRC.

Saltzer, J.H. and Schroeder, M.D. (1975). The protection of information in computer systems. *Proceedings of the IEEE* 63,9, 1278–1308.