chapter 4

Planning for Security

Begin with the end in mind.
STEPHEN COVEY, AUTHOR OF *SEVEN HABITS OF HIGHLY EFFECTIVE PEOPLE*

Charlie Moody flipped up his jacket collar to cover his ears. The spray blowing over him from the fire hoses was icing the cars along the street where he stood watching his office building burn. The warehouse and shipping dock were not gone, but were severely damaged by smoke and water. He tried to hide his dismay by turning to speak to Fred Chin.

"Look at the bright side," said Charlie. "At least we can get the new servers that we've been putting off."

Fred shook his head. "Charlie, you must be dreaming. We don't have enough insurance for a full replacement of everything we've lost."

Charlie was stunned. The offices were gone, all the computer systems, servers, and desktops were melted slag, and he would have to try to rebuild without the resources he needed. At least he had good backups, or so he hoped. He thought hard, trying to remember the last time the off-site backup tapes had been tested.

He wondered where all the network design diagrams were. He knew he could call his network provider to order new circuits as soon as Fred found some new office space. But where were all the circuit specs? The only copy had been in a drawer in his office, which wasn't there

anymore. This was not going to be fun. He would have to call directory assistance just to get the phone number for his boss, Gladys Williams, the chief information officer (CIO).

Charlie heard a buzzing noise to his left. He turned to see the flashing numbers of his alarm clock. Relief flooded him as he realized it was just a nightmare; Sequential Label and Supply (SLS) had not burned down. He turned on the light and started making notes for reviewing with his staff later that morning. Charlie would make some changes to the company contingency plans *today*.

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Describe management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
- Explain what an information security blueprint is, identify its major components, and explain how it supports the information security program
- Discuss how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs
- Describe what contingency planning is and how it relates to incident response planning, disaster recovery planning, and business continuity plans

Introduction

An organization's information security effort succeeds only when it operates in conjunction with the organization's information security policy. An information security program begins with policy, standards, and practices, which are the foundation for the information security architecture and blueprint. The creation and maintenance of these elements require coordinated planning. The role of planning in modern organizations is hard to overemphasize. All but the smallest organizations engage in some planning: strategic planning to manage the allocation of resources and contingency planning to prepare for the uncertainties of the business environment.

Information Security Planning and Governance

Key Terms

goals Sometimes used synonymously with *objectives*; the desired end of a planning cycle.

objectives Sometimes used synonymously with *goals*; the intermediate states obtained to achieve progress toward a goal or goals.

strategic plan The documented product of strategic planning; a plan for the organization's intended strategic efforts over the next several years.

strategic planning The process of defining and specifying the long-term direction (strategy) to be taken by an organization, and the allocation and acquisition of resources needed to pursue this effort.

Strategic planning sets the long-term direction to be taken by the organization and each of its component parts. Strategic planning should guide organizational efforts and focus resources toward specific, clearly defined **goals**. After an organization develops a general strategy, it generates an overall **strategic plan** by extending that general strategy into plans for major divisions. Each level of each division then translates those plan **objectives** into more specific objectives for the level below. To execute this broad strategy, the executive team must first define individual responsibilities. (The executive team is sometimes called the organization's C-level, as in CEO, COO, CFO, CIO, and so on.)

› Planning Levels

Key Terms

operational plan The documented product of operational planning; a plan for the organization's intended operational efforts on a day-to-day basis for the next several months.

operational planning The actions taken by management to specify the short-term goals and objectives of the organization in order to obtain specified tactical goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.

tactical plan The documented product of tactical planning; a plan for the organization's intended tactical efforts over the next few years.

tactical planning The actions taken by management to specify the intermediate goals and objectives of the organization in order to obtain specified strategic goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.

Once the organization's overall strategic plan is translated into strategic plans for each major division or operation, the next step is to translate these plans into tactical objectives that move toward reaching specific, measurable, achievable, and time-bound accomplishments. The process of strategic planning seeks to transform broad, general, sweeping statements into more specific and applied objectives. Strategic plans are used to create **tactical plans**, which in turn are used to develop **operational plans**.

Tactical planning focuses on short-term undertakings that will be completed within one or two years. The process of tactical planning breaks each strategic goal into a series of incremental objectives. Each objective in a tactical plan should be specific and should have a delivery date within a year of the plan's start. Budgeting, resource allocation, and personnel are critical components of the tactical plan. Tactical plans often include project plans and resource acquisition planning documents (such as product specifications), project budgets, project reviews, and monthly and annual reports. The chief information security officer (CISO) and security managers use the tactical plan to organize, prioritize, and acquire resources necessary for major projects and to provide support for the overall strategic plan.

Managers and employees use **operational planning** derived from tactical planning to organize the ongoing, day-to-day performance of tasks. An operational plan includes the necessary tasks for all relevant departments as well as communication and reporting requirements, which might include weekly meetings, progress reports, and other associated tasks. These plans must reflect the organizational structure, with each subunit, department, or project

team conducting its own operational planning and reporting. Frequent communication and feedback from the teams to the project managers and/or team leaders, and then up to the various management levels, will make the planning process more manageable and successful.

Planning and the CISO

The first priority of the CISO and the information security management team is the creation of a strategic plan to accomplish the organization's information security objectives. While each organization may have its own format for the design and distribution of a strategic plan, the fundamental elements of planning share characteristics across all types of enterprises. The plan is an evolving statement of how the CISO and various elements of the organization will implement the objectives of the information security charter, which is expressed in the enterprise information security policy (EISP). You will learn about EISPs later in this chapter.

As a clearly directed strategy flows from top to bottom, a systematic approach is required to translate it into a program that can inform and lead all members of the organization. Strategic plans formed at the highest levels of the organization are used to create an overall corporate strategy. As lower levels of the organizational hierarchy are involved (moving down the hierarchy), the plans from higher levels are evolved into more detailed, more concrete planning. So, higher-level plans are translated into more specific plans for intermediate layers of management. That layer of strategic planning by function (such as financial, IT, and operations strategies) is then converted into tactical planning for supervisory managers and eventually provides direction for the operational plans undertaken by non-management members of the organization. This multi-layered approach encompasses two key objectives: general strategy and overall strategic planning. First, general strategy is translated into specific strategy; second, overall strategic planning is translated into lower-level tactical and operational planning.

Information security, like information technology, must support more than its own functions. All organizational units will use information, not just IT-based information, so the Information Security group must understand and support the strategic plans (a.k.a. strategies) of all business units. This role may sometimes conflict with that of the IT department, as IT's role is the efficient and effective delivery of information and information resources, while the role of information security is the protection of all information assets.

For more information on information security planning, read NIST Special Publication (SP) 800-18, Rev. 1, which is available from the NIST SP Web site at http://csrc.nist.gov/publications/PubsSPs.html.

Information Security Governance

Key Terms

corporate governance Executive management's responsibility to provide strategic direction, ensure the accomplishment of objectives, oversee that risks are appropriately managed, and validate responsible resource use.

governance "The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."[1]

information security governance The application of the principles of corporate governance to the information security function.

Governance describes the entire function of controlling, or governing, the processes used by a group to accomplish some objective. It represents the strategic controlling function of an organization's senior management, which is designed to ensure informed, prudent strategic decisions made in the best interest of the organization.

Just like governments, corporations and other organizations have guiding documents—corporate charters or partnership agreements—as well as appointed or elected leaders or officers, and planning and operating procedures. These elements in combination provide **corporate governance**. Each operating unit within an organization also has controlling customs, processes, committees, and practices. The information security group's leadership monitors and manages all of the organizational structures and processes that safeguard information. **Information security governance** then applies these principles and management structures to the information security function.

The governance of information security is a strategic planning responsibility whose importance has grown in recent years. To secure information assets, management must integrate information security practices into the fabric of the organization, expanding corporate governance policies and controls to encompass the objectives of the information security process. Information security objectives must be addressed at the highest levels of an organization's management team in order to be effective and sustainable. A broader view of information security encompasses all of an organization's information assets, including the knowledge managed by those IT assets.

According to the Information Technology Governance Institute (ITGI), information security governance includes all of the accountabilities and methods undertaken by the board of directors and executive management to provide:

- Strategic direction
- Establishment of objectives
- Measurement of progress toward those objectives
- Verification that risk management practices are appropriate
- Validation that the organization's assets are used properly

Figure 4-1 illustrates the responsibilities of various people within an organization for information security governance.

› Information Security Governance Outcomes

Effective communication among stakeholders is critical to the structures and processes used in governance at every level, especially in information security governance. This requires the

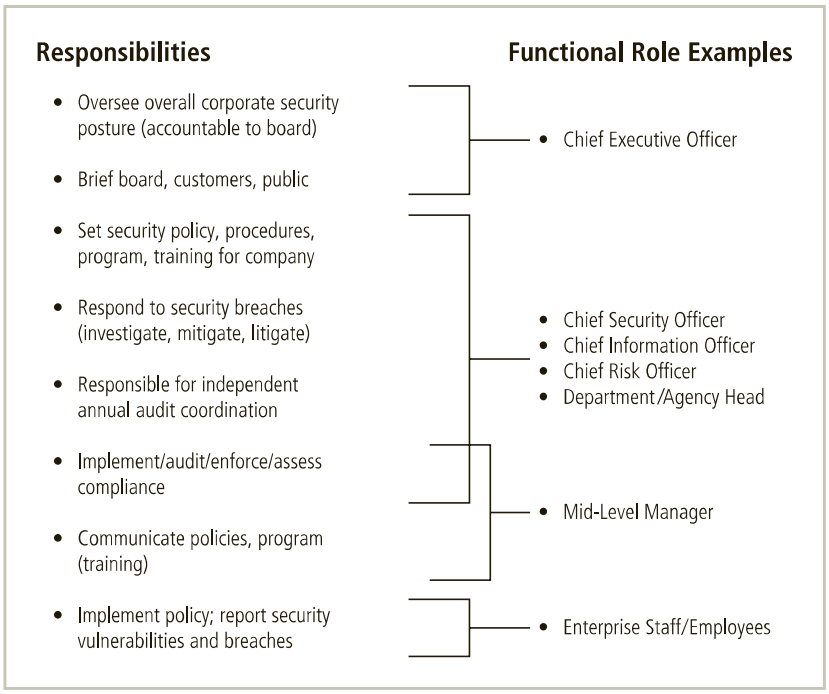


Figure 4-1 Information security governance roles and responsibilities

Source: This information is derived from the Corporate Governance Task Force Report, "Information Security Governance: A Call to Action," April 2004, National Cyber Security Task Force.

development of constructive relationships, a common language, and a commitment to the objectives of the organization.

The five goals of information security governance are:

1. *Strategic alignment of information security with business strategy to support organizational objectives*
2. *Risk management by executing appropriate measures to manage and mitigate threats to information resources*
3. *Resource management by using information security knowledge and infrastructure efficiently and effectively*
4. *Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved*
5. *Value delivery by optimizing information security investments in support of organizational objectives*[2]

For a library of documents on information security governance and recommended frameworks, visit the US-CERT Web site hosted by the Software Engineering Institute at www.cert.org/governance/ges.html. A list of related documents is also included in the Selected Readings section at the end of this chapter.

Information Security Policy, Standards, and Practices

Management from all communities of interest, including general staff, information technology, and information security, must make policies the basis for all information security planning, design, and deployment. Policies direct how issues should be addressed and how technologies should be used. Policies do not specify the proper operation of equipment or software—this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation. In addition, *policy should never contradict law; policy must be able to stand up in court, if challenged; and policy must be properly administered through dissemination and documented acceptance*. Otherwise, an organization leaves itself exposed to significant liability. For a discussion of this issue, see the Offline feature on Arthur Andersen.

Good security programs begin and end with policy.[3] Information security is primarily a management problem, not a technical one, and policy is a management tool that obliges personnel to function in a manner that preserves the security of information assets. Security policies are the least expensive control to execute, but the most difficult to implement *properly*. They have the lowest cost in that their creation and dissemination require only the time and effort of the management team. Even if the management team hires an outside consultant to help develop policy, the costs are minimal compared to those of technical controls.

› Policy as the Foundation for Planning

Key Terms

de facto standard A standard that has been widely adopted or accepted by a public group rather than a formal standards organization. Contrast with a *de jure standard*.

de jure standard A standard that has been formally evaluated, approved, and ratified by a formal standards organization. Contrast with a *de facto standard*.

guidelines Nonmandatory recommendations the employee may use as a reference in complying with a policy. If the policy states to "use strong passwords, frequently changed," the guidelines might advise that "we recommend you don't use family or pet names, or parts of your Social Security number, employee number, or phone number in your password."

information security policy Written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets.

practices Examples of actions that illustrate compliance with policies. If the policy states to "use strong passwords, frequently changed," the practices might advise that "according to X, most organizations require employees to change passwords at least semi-annually."

procedures Step-by-step instructions designed to assist employees in following policies, standards, and guidelines. If the policy states to "use strong passwords, frequently changed," the procedure might advise that "in order to change your password, first click the Windows Start button, then…."

standard A detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance. If the policy states that employees must "use strong passwords, frequently changed," the standard might specify that the password "must be at least 8 characters, with at least one number, one letter, and one special character."

OFFLINE

Arthur Andersen and Enron

"I obstructed justice," testified David B. Duncan, the former chief outside auditor of Enron Corporation, an American energy company. He told a federal jury that he knew he had committed a crime when he instructed his colleagues at Arthur Andersen LLP to destroy documents as their energy client collapsed. "I instructed people on the engagement team to follow a document-retention policy which I knew would result in the destruction of documents." Duncan was fired by Andersen in January 2002 after an internal probe revealed that the world-renowned accounting company had shredded tons of financial documents and deleted Enron-related e-mail messages. He pleaded guilty to a single count of obstruction of justice.[4]

Enron Corporation was found to have lied about its financial records, specifically its reported profits. Enron was also accused of many dubious business practices, including concealing financial losses and debts. The depth and breadth of the fraud was so great that at least one executive committed suicide rather than face criminal charges. One of the company's accounting firms, Andersen, contributed to the fraud by shredding documents in an attempt to hide the problem. Andersen claimed this was its policy.

Policy that conflicts with law is by definition illegal; therefore, following such a policy is a criminal act. In the Enron/Arthur Andersen scandal, people went to jail claiming they had simply followed policy, although they might have gotten away with it if the policy had been enforced for legitimate and lawful purposes.

The Andersen policy for document retention stated that staff must keep work papers for six years before destroying them, but client-related files, such as correspondence or other records, were only kept "until not useful." Managers and individual partners who kept such material in client folders or other files should "purge" the documents, the policy stated. But, in cases of threatened litigation, Andersen staff were not supposed to destroy "related information."[5] A subsequent update to the policy was interpreted as a mandate to shred all but the most basic working papers as soon as possible unless precluded by an order for legal discovery.

So the shredding party began. A big part of the problem was that the policy was not followed consistently—that is, the shredding began right *after* Andersen found out that Enron was to be investigated for fraudulent business practices, which indicated that the consulting firm had decided to cover its tracks and those of its business partner.

In the end, people went to jail, one person is dead, and thousands of people's lives were disrupted because they lost their jobs, investments, or retirement accounts. A company with a tradition of integrity and trustworthiness is gone, and many claimed they were just following policy.

Policies function like laws in an organization because they dictate acceptable and unacceptable behavior there, as well as the penalties for failure to comply. Like laws, policies define what is right and wrong, the penalties for violating policy, and the appeal process. **Standards**, on the other hand, are more detailed statements of what must be done to comply with policy. They have the same requirements for compliance as policies. Standards may be informal or part of an organizational culture, as in **de facto standards**. Or, standards may be published, scrutinized, and ratified by a group, as in formal or **de jure standards**. Practices, procedures, and guidelines effectively explain how to comply with policy. Figure 4-2 shows the relationships among policies, standards, **guidelines**, **procedures**, and **practices**. This relationship is further examined in the nearby Offline feature.

The meaning of the term *security policy* depends on the context in which it is used. Governmental agencies view security policy in terms of national security and national policies to deal with foreign states. A security policy can also communicate a credit card agency's method for processing credit card numbers. In general, a security policy is a set of rules that protects an organization's assets. An **information security policy** provides rules for protection of the organization's information assets.

Management must define three types of security policy, according to Special Publication (SP) 800-14 of the National Institute of Standards and Technology (NIST):

1. Enterprise information security policies
2. Issue-specific security policies
3. Systems-specific security policies

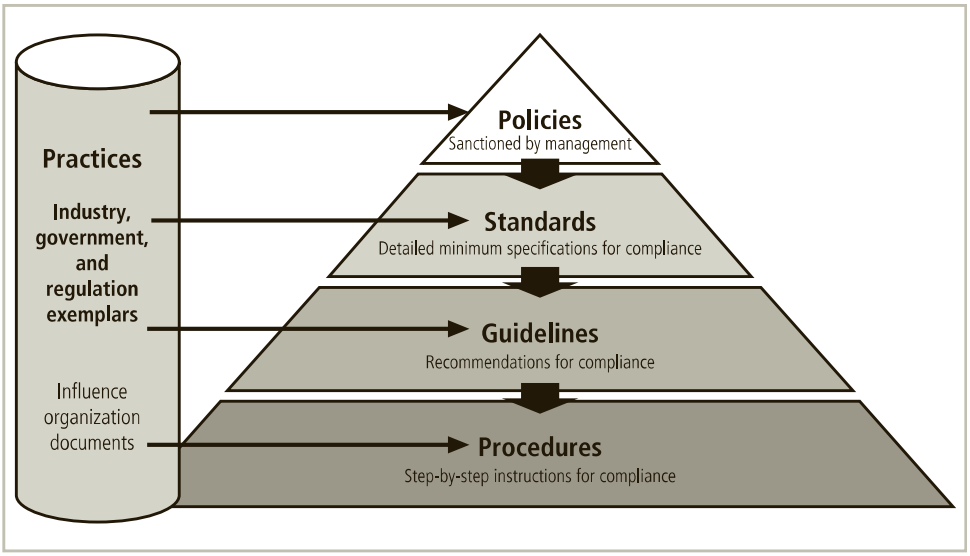


Figure 4-2 Policies, standards, guidelines, and procedures

OFFLINE

Policies, Practices, Standards, Guidelines, and Procedures

The relationships among these terms, even when carefully defined, sometimes confuse the reader. The following examples are provided for assistance. Note that many organizations may use the terms differently and publish documents they identify as policy, which may be a combination of what this text defines as policy, standards, or procedures.

The initial statement of intent is the policy.

Policy: Employees must use strong passwords on their accounts. Passwords must be changed regularly and protected against disclosure.

The standard provides specifics to help employees comply with the policy.

Standard: Passwords must be at least 10 characters long and incorporate at least one lowercase letter, one uppercase letter, one numerical digit (0–9), and one special character permitted by our system (&%$#@!). Passwords must be changed every 90 days, and must not be written down or stored on insecure media.

The practice identifies other reputable organizations and agencies that offer recommendations the organization may have adopted or adapted.

Practice: US-CERT recommends the following:

- *Use a minimum password length of 15 characters for administrator accounts.*
- *Require the use of alphanumeric passwords and symbols.*
- *Enable password history limits to prevent the reuse of previous passwords.*
- *Prevent the use of personal information as passwords, such as phone numbers and dates of birth.*
- *Use a minimum password length of 8 characters for standard users.*
- *Disable local machine credential caching if not required through the use of a Group Policy Object (GPO).*
- *Deploy a secure password storage policy that provides password encryption.*[6]

Guidelines provide examples and recommendations to assist users in complying with the new policy.

Guidelines: In order to create strong yet easy-to-remember passwords, consider the following recommendations from NIST SP 800-118: Guide to Enterprise Password Management (Draft), April 2009:

- *Mnemonic Method. A user selects a phrase and extracts a letter of each word in the phrase (such as the first letter or second letter of each word), adding numbers or special characters or both.*
  - *Example: "May the force be with you always, young Jedi" becomes Mtfbwya-yJ*

- *Altered Passphrases. A user selects a phrase and alters it to form a derivation of that phrase. This method supports the creation of long, complex passwords. Passphrases can be easy to remember due to the structure of the password: it is usually easier for the human mind to comprehend and remember phrases within a coherent structure than a string of random letters, numbers, and special characters.*
  - *Example: Never Give Up! Never Surrender! becomes Nv.G.Up!-Nv.Surr!*
- *Combining and Altering Words. A user can combine two or three unrelated words and change some of the letters to numbers or special characters.*
  - *Example: Jedi Tribble becomes J3d13bbl*

Finally, procedures are step-by-step instructions for accomplishing the task specified in the policy.

Procedures: To change your log-in password on our system, perform the following steps:

1) *Log in using your current (old) password.*
2) *On your organizational portal home page, click the [Tools] Menu option.*
3) *Select [Change Password].*
4) *Enter your old password in the first field and your new password in the second. The system will ask you to confirm your new password to prevent you from mistyping it.*
5) *The system will then report that your password has been updated, and ask you to log out and log back in with your new password.*

   Do not write your new password down. If you own a smartphone, you may request that your department purchase an approved password management application like eWallet for storing passwords.

As stated earlier, many organizations combine their policy and standards in the same document, and then provide directions or a Web link to a page with guidelines and procedures.

SP 800-14 will be discussed in greater detail later in this chapter.

As introduced in Chapter 3, a policy must meet the following criteria to be effective and thus legally enforceable:

- Dissemination (distribution): The organization must be able to demonstrate that the policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.
- Review (reading): The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for employees who are

illiterate, reading-impaired, and unable to read English. Common techniques include recording the policy in English and other languages.

- Comprehension (understanding): The organization must be able to demonstrate that the employee understands the requirements and content of the policy. Common techniques include quizzes and other assessments.
- Compliance (agreement): The organization must be able to demonstrate that the employee agrees to comply with the policy through act or affirmation. Common techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.
- Uniform enforcement (fairness in application): The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

› Enterprise Information Security Policy

Key Term

enterprise information security policy (EISP) The high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts. An EISP is also known as a security program policy, general security policy, IT security policy, high-level InfoSec policy, or simply an InfoSec policy.

An **enterprise information security policy (EISP)** is also known as a general security policy, organizational security policy, IT security policy, or information security policy. The EISP is an executive-level document, usually drafted by or in cooperation with the organization's chief information officer. This policy is usually 2 to 10 pages long and shapes the philosophy of security in the IT environment. The EISP usually needs to be modified only when there is a change in the strategic direction of the organization.

The EISP guides the development, implementation, and management of the security program. It sets out the requirements that must be met by the information security blueprint or framework. It defines the purpose, scope, constraints, and applicability of the security program. It also assigns responsibilities for the various areas of security, including systems administration, maintenance of the information security policies, and the practices and responsibilities of users. Finally, it addresses legal compliance. According to NIST, the EISP typically addresses compliance in two areas:

1. General compliance to ensure that an organization meets the requirements for establishing a program and assigning responsibilities therein to various organizational components
2. The use of specified penalties and disciplinary action[7]

When the EISP has been developed, the CISO begins forming the security team and initiating necessary changes to the information security program.

EISP Elements Although the specifics of EISPs vary among organizations, most EISP documents should include the following elements:

- An overview of the corporate philosophy on security
- Information on the structure of the information security organization and people who fulfill the information security role
- Fully articulated responsibilities for security that are shared by all members of the organization (employees, contractors, consultants, partners, and visitors)
- Fully articulated responsibilities for security that are unique to each role within the organization

The components of a good EISP are shown in Table 4-1. For examples of EISP documents and recommendations for how to prepare them, we recommend using *Information Security Policies Made Easy* by Charles Cresson Wood, published by Information Shield. While the current version is relatively expensive, prior editions are widely available as used books and in libraries around the world.

Component	Description
Statement of Purpose	Answers the question "What is this policy for?" Provides a framework that helps the reader understand the intent of the document. Can include text such as the following: "This document will: • Identify the elements of a good security policy • Explain the need for information security • Specify the various categories of information security • Identify the information security responsibilities and roles • Identify appropriate levels of security through standards and guidelines This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs."[8]
Information Security Elements	Defines information security. For example: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology …" This section can also lay out security definitions or philosophies to clarify the policy.
Need for Information Security	Provides information on the importance of information security in the organization and the legal and ethical obligation to protect critical information about customers, employees, and markets.
Information Security Responsibilities and Roles	Defines the organizational structure designed to support information security within the organization. Identifies categories of people with responsibility for information security (IT department, management, users) and those responsibilities, including maintenance of this document.
Reference to Other Information Standards and Guidelines	Lists other standards that influence this policy document and are influenced by it, perhaps including relevant federal laws, state laws, and other policies.

Table 4-1 Components of the EISP[9]

Issue-Specific Security Policy

Key Term

issue-specific security policy (ISSP) An organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resource, such as one of its processes or technologies.

As an organization supports routine operations by executing various technologies and processes, it must instruct employees on their proper use. In general, the **issue-specific security policy**, or **ISSP**, (1) addresses specific areas of technology as listed below, (2) requires frequent updates, and (3) contains a statement about the organization's position on a specific issue.[10] An ISSP may cover the following topics, among others:

- E-mail
- Use of the Internet and World Wide Web
- Specific minimum configurations of computers to defend against worms and viruses
- Prohibitions against hacking or testing organization security controls
- Home use of company-owned computer equipment
- Use of personal equipment on company networks (BYOD: bring your own device)
- Use of telecommunications technologies, such as fax and phone
- Use of photocopy equipment
- Use of portable storage devices such as USB memory sticks, backpack drives, game players, music players, and any other device capable of storing digital files
- Use of cloud-based storage services that are not self-hosted by the organization or engaged under contract; such services include Google Drive, Dropbox, and Microsoft Live

For examples of ISSP policies and recommendations for how to prepare them, we recommend using *Information Security Policies Made Easy* by Charles Cresson Wood, published by Information Shield. The book includes a wide variety of working policy documents and can assist in defining which are needed and how to create them.

Several approaches are used to create and manage ISSPs within an organization. Three of the most common are:

1. Independent ISSP documents, each tailored to a specific issue
2. A single comprehensive ISSP document that covers all issues
3. A modular ISSP document that unifies policy creation and administration while maintaining each specific issue's requirements

The independent ISSP document typically has a scattershot effect. Each department responsible for a particular application of technology creates a policy governing its use, management, and control. This approach may fail to cover all of the necessary issues and can lead to poor policy distribution, management, and enforcement.

The single comprehensive ISSP is centrally managed and controlled. With formal procedures for the management of ISSPs in place, the comprehensive policy approach establishes guidelines for overall coverage of necessary issues and clearly identifies processes for the dissemination, enforcement, and review of these guidelines. Usually, these policies are developed by the people responsible for managing the information technology resources. Unfortunately, these policies tend to overgeneralize the issues and skip over vulnerabilities.

The optimal balance between the independent and comprehensive ISSP is the modular ISSP. It is also centrally managed and controlled, but it is tailored to individual technology issues. The modular approach provides a balance between issue orientation and policy management. The policies created with this approach comprise individual modules, each created and updated by people responsible for the issues addressed. These people report to a central policy administration group that incorporates specific issues into an overall comprehensive policy.

Table 4-2 is an outline of a sample ISSP, which can be used as a model. An organization should start with this structure and add specific details that dictate security procedures not covered by these general guidelines.

The components of each major category presented in the sample ISSP in Table 4-2 are discussed after the table. Even though the details may vary from policy to policy and some sections of a modular policy may be combined, it is essential for management to address and complete each section.

Statement of Policy The policy should begin with a clear statement of purpose—in other words, what exactly is this policy supposed to accomplish? Consider a policy that covers the issue of fair and responsible Internet use. The introductory section of this policy should address the following questions: What is the scope of this policy? Who is responsible and accountable for policy implementation? What technologies and issues does it address?

Authorized Access and Usage of Equipment This section of the policy statement addresses *who* can use the technology governed by the policy, and *what* it can be used for. Remember that an organization's information systems are its exclusive property, and users have no particular rights of use. Each technology and process is provided for business operations. Use for any other purpose constitutes misuse of equipment. This section defines "fair and responsible use" of equipment and other organizational assets and should address key legal issues, such as protection of personal information and privacy.

Prohibited Use of Equipment Unless a particular use is clearly prohibited, the organization cannot penalize its employees for misuse. For example, the following can be prohibited: personal use, disruptive use or misuse, criminal use, offensive or harassing materials, and infringement of copyrighted, licensed, or other intellectual property. As an alternative approach, categories 2 and 3 of Table 4-2 can be collapsed into a single category called "Appropriate Use." Many organizations use such an ISSP section to cover both categories.

Systems Management The systems management section of the ISSP policy statement focuses on the users' relationship to systems management. Specific rules from management

Components of an ISSP
1. Statement of policy a. Scope and applicability b. Definition of technology addressed c. Responsibilities
2. Authorized access and usage of equipment a. User access b. Fair and responsible use c. Protection of privacy
3. Prohibited use of equipment a. Disruptive use or misuse b. Criminal use c. Offensive or harassing materials d. Copyrighted, licensed, or other intellectual property e. Other restrictions
4. Systems management a. Management of stored materials b. Employee monitoring c. Virus protection d. Physical security e. Encryption
5. Violations of policy a. Procedures for reporting violations b. Penalties for violations
6. Policy review and modification a. Scheduled review of policy procedures for modification b. Legal disclaimers
7. Limitations of liability a. Statements of liability b. Other disclaimers as needed

Table 4-2 Components of an ISSP[11]

Source: Whitman, Townsend, and Aalberts, Communications of the ACM.

include regulating the use of e-mail, the storage of materials, the authorized monitoring of employees, and the physical and electronic scrutiny of e-mail and other electronic documents. It is important that all such responsibilities are assigned either to the systems administrator or the users; otherwise, both parties may infer that the responsibility belongs to the other.

Violations of Policy The people to whom the policy applies must understand the penalties and repercussions of violating it. Violations of policy should carry penalties that are appropriate—neither draconian nor overly lenient. This section of the policy statement should contain not only specific penalties for each category of violation, but instructions for how people in the organization can report observed or suspected violations. Many

people think that powerful employees in an organization can retaliate against someone who reports violations. Allowing anonymous submissions is often the only way to convince users to report the unauthorized activities of more influential employees.

Policy Review and Modification Because any document is only useful if it is up to date, each policy should contain procedures and a timetable for periodic review. As the organization's needs and technologies change, so must the policies that govern their use. This section should specify a methodology for reviewing and modifying the policy to ensure that users do not begin circumventing it as it grows obsolete.

Limitations of Liability If an employee is caught conducting illegal activities with the organization's equipment or assets, management does not want the organization held liable. The policy should state that if employees violate a company policy or any law using company technologies, the company will not protect them, and the company is not liable for their actions. In fact, many organizations assist in the prosecution of employees who violate laws when their actions violate policies. It is assumed that such violations occur without knowledge or authorization by the organization.

› Systems-Specific Security Policy (SysSP)

Key Terms

access control list (ACL) Specifications of authorization that govern the rights and privileges of users to a particular information asset. ACLs include user access lists, matrices, and capabilities tables.

access control matrix An integration of access control lists (focusing on assets) and capability tables (focusing on users) that results in a matrix with organizational assets listed in the column headings and users listed in the row headings. The matrix contains ACLs in columns for a particular device or asset and capability tables in rows for a particular user.

capabilities table A lattice-based access control with rows of attributes associated with a particular subject (such as a user).

configuration rules The instructions a system administrator codes into a server, networking device, or security device to specify how it operates.

managerial guidance SysSP A systems-specific security policy that expresses management's intent for the acquisition, implementation, configuration, and management of a particular technology, written from a business perspective.

systems-specific security policies (SysSPs) Organizational policies that often function as standards or procedures to be used when configuring or maintaining systems. SysSPs can be separated into two general groups—managerial guidance and technical specifications—but may be written as a single unified SysSP document.

technical specifications SysSP A type of systems-specific security policy that expresses technical details for the acquisition, implementation, configuration, and management of a particular technology, written from a technical perspective. Typically the policy includes details on configuration rules, systems policies, and access control.

While issue-specific policies are formalized as written documents readily identifiable as policy, **systems-specific security policies** (**SysSPs**) sometimes have a different look. SysSPs often

function as standards or procedures to be used when configuring or maintaining systems. For example, a SysSP might describe the configuration and operation of a network firewall. This document could include a statement of managerial intent; guidance to network engineers on the selection, configuration, and operation of firewalls; and an access control list that defines levels of access for each authorized user. SysSPs can be separated into two general groups, **managerial guidance SysSPs** and **technical specifications SysSPs**, or they can be combined into a single policy document that contains elements of both.

Managerial Guidance SysSPs A managerial guidance SysSP document is created by management to guide the implementation and configuration of technology and to address the behavior of employees in ways that support information security. For example, while the method for implementing a firewall belongs in the technical specifications SysSP, the firewall's configuration must follow guidelines established by management. An organization might not want its employees to access the Internet via the organization's network, for instance; in that case, the firewall should be implemented accordingly.

Firewalls are not the only technology that may require systems-specific policies. Any system that affects the confidentiality, integrity, or availability of information must be assessed to evaluate the trade-off between improved security and restrictions.

Systems-specific policies can be developed at the same time as ISSPs, or they can be prepared in advance of their related ISSPs. Before management can craft a policy informing users what they can do with certain technology and how to do it, system administrators might have to configure and operate the system. Some organizations may prefer to develop ISSPs and SysSPs in tandem so that operational procedures and user guidelines are created simultaneously.

Technical Specifications SysSPs While a manager can work with a systems administrator to create managerial policy, as described in the preceding section, the systems administrator in turn might need to create a policy to implement the managerial policy. Each type of equipment requires its own set of policies, which are used to translate management's intent for the technical control into an enforceable technical approach. For example, an ISSP may require that user passwords be changed quarterly; a systems administrator can implement a technical control within a specific application to enforce this policy. There are two general methods of implementing such technical controls: access control lists and configuration rules.

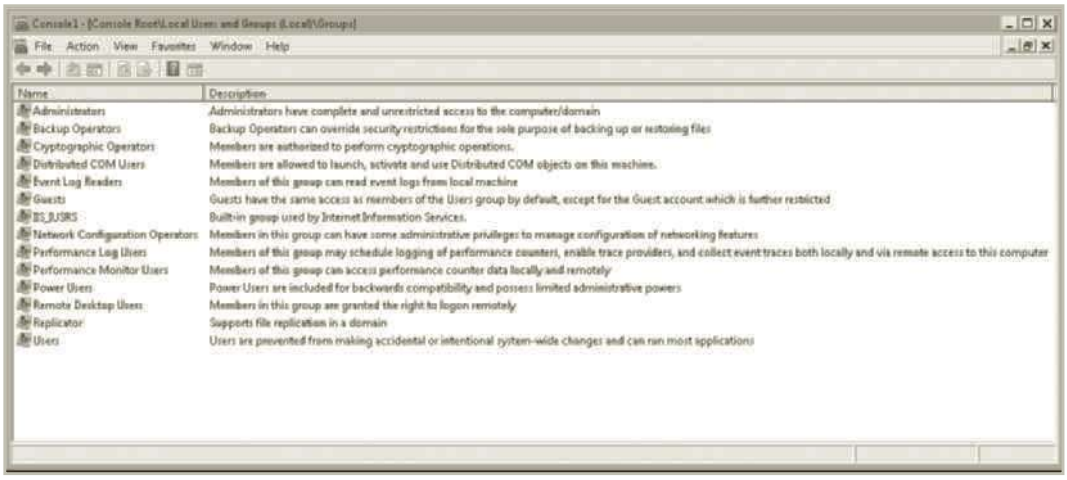
Access Control Lists An **access control list** (**ACL**) consists of details about user access and use permissions and privileges for an organizational asset or resource, such as a file storage system, software component, or network communications device. ACLs focus on assets and the users who can access and use them. A **capabilities table** is similar to an ACL, but it focuses on users, the assets they can access, and what they can do with those assets. In some systems, capability tables are called user profiles or user policies.

These specifications frequently take the form of complex matrices rather than simple lists or tables, resulting in an **access control matrix** that combines the information in ACLs and capability tables.

As illustrated in Figures 4-3 and 4-4, both Microsoft Windows and Linux systems translate ACLs into sets of configurations that administrators use to control access to their systems.

The level of detail may differ from system to system, but in general ACLs can restrict access for a particular user, computer, time, or duration—even a particular file. This specificity provides powerful control to the administrator. In general, ACLs regulate the following:

- *Who* can use the system
- *What* authorized users can access
- *When* authorized users can access the system
- *Where* authorized users can access the system



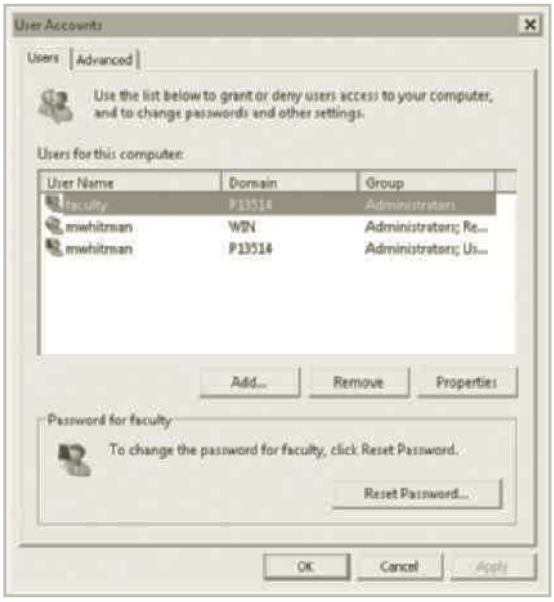


Figure 4-3 Microsoft Windows use of ACLs

Source: Microsoft.

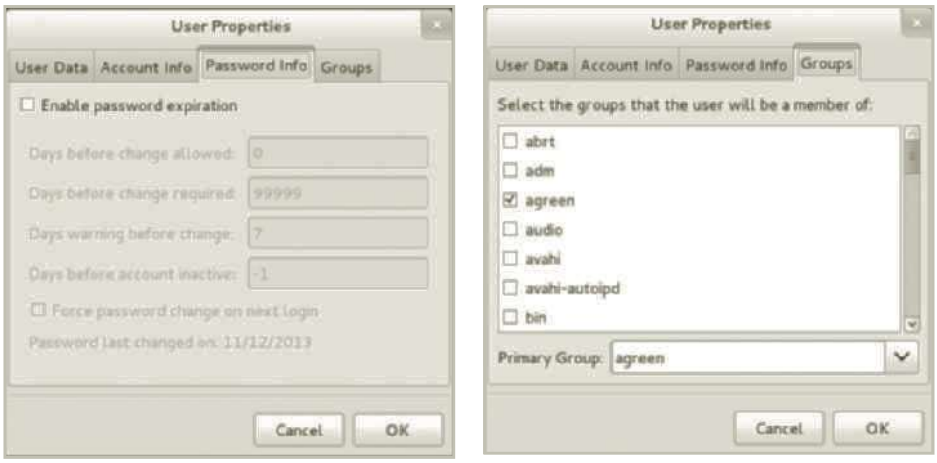


Figure 4-4 Linux use of ACLs

Source: Ubuntu Linux.

The *who* of ACL access may be determined by a person's identity or membership in a group. Restricting *what* authorized users are permitted to access—whether by type (printers, files, communication devices, or applications), name, or location—is achieved by adjusting the resource privileges for a person or group to Read, Write, Create, Modify, Delete, Compare, or Copy. To control *when* access is allowed, some organizations implement time-of-day and day-of-week restrictions for certain network or system resources. To control *where* resources can be accessed, many network-connected assets block remote usage and have some levels of access that are restricted to locally connected users, such as restrictions by computer MAC address or network IP address. When these various ACL options are applied concurrently, the organization can govern how its resources can be used.

Configuration Rule Policies **Configuration rules** (or policies) govern how a security system reacts to the data it receives. Rule-based policies are more specific to the operation of a system than ACLs, and they may or may not deal with users directly. Many security systems—for example, firewalls, intrusion detection and prevention systems (IDPSs), and proxy servers—use specific configuration scripts that represent the configuration rule policy to determine how the system handles each data element they process. The examples in Figures 4-5 and 4-6 show how network security policy has been implemented by a Check Point firewall's rule set and by Ionx Verisys (File Integrity Monitoring) in a host-based IDPS rule set.

Combination SysSPs Many organizations create a single document that combines the managerial guidance SysSP and the technical specifications SysSP. While this document can be somewhat confusing to casual users, it is practical to have the guidance from managerial and technical perspectives in a single place. If this approach is used, care should be taken to clearly articulate the required actions. Some might consider this type of policy document a

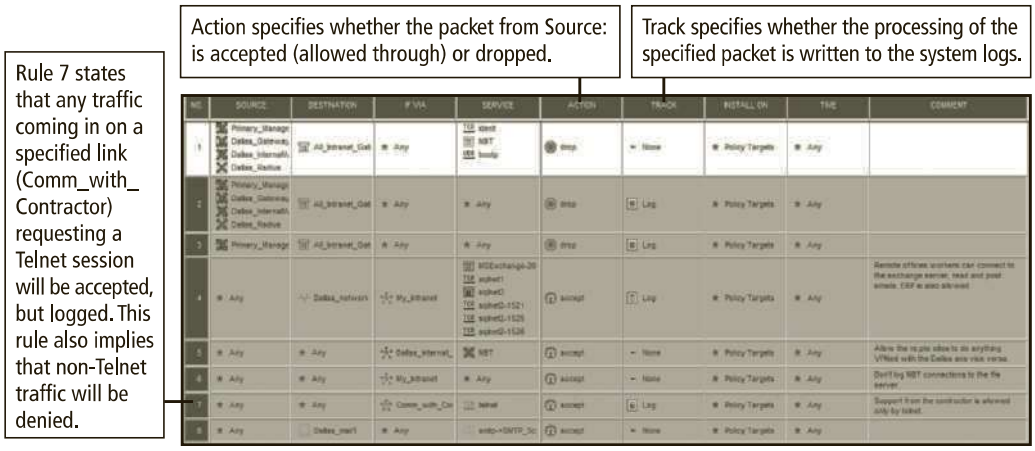


Figure 4-5 Check Point VPN-1/Firewall-1 Policy Editor

Source: Check Point.

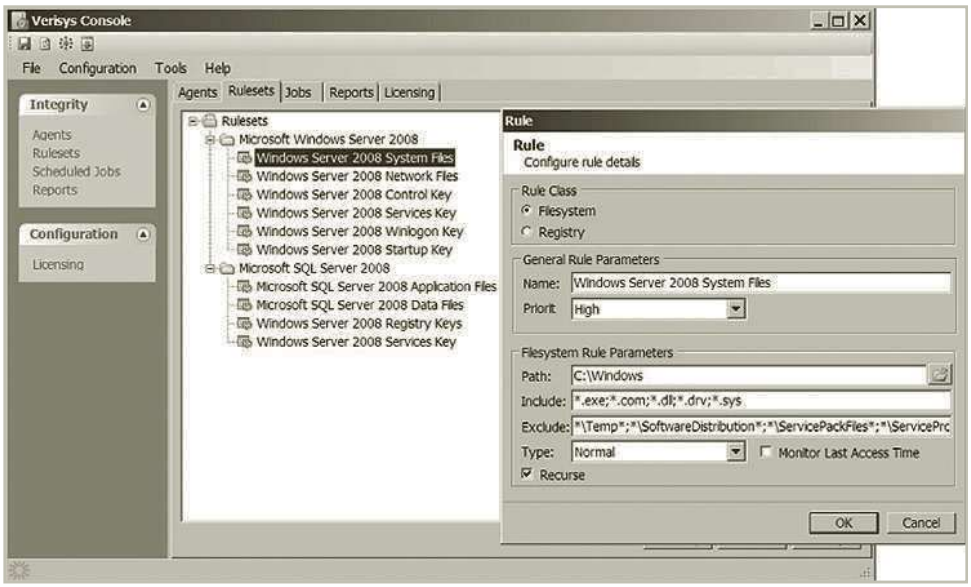


Figure 4-6 Ionx Verisys (File Integrity Monitoring) use of rules

Source: Ionx.

procedure, but it is actually a hybrid that combines policy with procedural guidance to assist implementers of the system being managed. This approach is best used by organizations that have multiple technical control systems of different types, and by smaller organizations that want to document policy and procedure in a compact format.

Policy Management

Key Terms

policy administrator An employee responsible for the creation, revision, distribution, and storage of a policy in an organization.
sunset clause A component of policy or law that defines an expected end date for its applicability.

Policies are living documents that must be managed. It is unacceptable to create such an important set of documents and then shelve them. These documents must be properly distributed, read, understood, agreed to, uniformly applied, and managed. How they are managed should be specified in the policy management section of the issue-specific policy described earlier. Good management practices for policy development and maintenance make for a more resilient organization. For example, all policies, including security policies, undergo tremendous stress when corporate mergers and divestitures occur. In such situations, employees are faced with uncertainty and many distractions. System vulnerabilities can arise, for instance, if incongruent security policies are implemented in different parts of a newly merged organization. When two companies merge but retain separate policies, the difficulty of implementing security controls increases. Likewise, when one company with unified policies splits in two, each new company may require different policies.

To remain viable, security policies must have a responsible manager, a schedule of reviews, a method for making recommendations for reviews, and a policy issuance and revision date.

Responsible Manager Just as information systems and information security projects must have champions and managers, so must policies. The policy manager is often called the **policy administrator**. Note that the policy administrator does not necessarily have to be proficient in the relevant technology. While practicing information security professionals require extensive technical knowledge, policy management and policy administration require only a moderate technical background. It is good practice, however, for policy administrators to solicit input both from technically adept information security experts and from business-focused managers in each community of interest when making revisions to security policies. The administrator should also notify all affected members of the organization when the policy is modified.

It is disheartening when a policy that required hundreds of staff-hours to develop and document is ignored. Thus, someone must be responsible for placing the policy and all subsequent revisions into the hands of people who are accountable for its implementation. The policy administrator must be clearly identified in the policy document as the primary point of contact for additional information or suggested revisions to the policy.

Schedule of Reviews Policies can only retain their effectiveness in a changing environment if they are periodically reviewed for currency and accuracy and then modified

accordingly. Policies that are not kept current can become liabilities as outdated rules are enforced (or not) and new requirements are ignored. To demonstrate due diligence, an organization must actively seek to meet the requirements of the market in which it operates. This applies to government, academic, and nonprofit organizations as well as private, for-profit organizations. A properly organized schedule of reviews should be defined and published as part of the document. Typically, a policy should be reviewed at least annually to ensure that it is still an effective control.

Review Procedures and Practices To facilitate policy reviews, the policy manager should implement a mechanism by which people can comfortably make recommendations for revisions, whether via e-mail, office mail, or an anonymous drop box. If the policy is controversial, anonymous submission of recommendations may be the best way to encourage staff opinions. Many employees are intimidated by management and hesitate to voice honest opinions about a policy unless they can do so anonymously. Once the policy has come up for review, all comments should be examined and management-approved improvements should be implemented. In reality, most policies are drafted by a single responsible employee and then reviewed by a higher-level manager. But, even this method does not preclude the collection and review of employee input.

Policy and Revision Date The simple action of dating the policy is often omitted. When policies are drafted and published without dates, confusion can arise. If policies are not reviewed and kept current, or if members of the organization are following undated versions, disastrous results and legal headaches can ensue. Such problems are particularly common in a high-turnover environment. Therefore, the policy must contain the date of origin and the date(s) of any revisions. Some policies may also need a **sunset clause** that indicates their expiration date, particularly if the policies govern information use in short-term business associations. Establishing a policy end date prevents a temporary policy from mistakenly becoming permanent, and it also enables an organization to gain experience with a given policy before adopting it permanently.

Automated Policy Management In recent years, a new category of software has emerged for the management of information security policies. This type of software was developed in response to the needs of information security practitioners. While many software products can meet the need for a specific technical control, software now can automate some of the busywork of policy management. Automation can streamline the repetitive steps of writing policy, tracking the workflow of policy approvals, publishing policy once it is written and approved, and tracking when employees have read the policy. Using techniques from computer-based training and testing, an organization can train staff members and improve its awareness program. To quote the VigilEnt Policy Center (VPC) user's guide from NetIQ Corporation:

> *Effective security policies are the cornerstone of any security effort. This effort includes writing policies, as well as communicating them to everyone who has access to and uses company information. Once you communicate the policies, you should measure how well the policies are communicated and understood by*

each employee. VigilEnt Policy Center (VPC) helps automate this entire process of security policy management.

Keeping policies up to date and making sure employees are aware of these changes is a complex but necessary procedure. As businesses grow and expand to include new companies, products, and regions, each with their own set of policies and standards, information security officers often ask themselves serious questions.

- *VigilEnt Policy Center helps educate employees about current policies and tests their knowledge through customized policy quizzes.*
- *You can easily update any existing policy document or create new policies as technology and regulations change throughout your company's life.*
- *Using a company's intranet, you can instantly send news items and alert users of sudden events.*
- *VPC lets you easily distribute policies around the world and verify that your users have received, read, and understood the current documents.*

VigilEnt Policy Center is the first product to address these issues with a comprehensive security management solution.[12]

The Information Security Blueprint

Key Terms

information security blueprint In information security, a framework or security model customized to an organization, including implementation details.

information security framework In information security, a specification of a model to be followed during the design, selection, and initial and ongoing implementation of all subsequent security controls, including information security policies, security education and training programs, and technological controls. Also known as a security model.

information security model See *information security framework*.

Once an organization has developed its information security policies and standards, the information security community can begin developing the blueprint for the information security program. If any policies, standards, or practices have not been completed, management must determine whether to proceed nonetheless with the development of the blueprint.

After the information security team has inventoried the organization's information assets and then assessed and prioritized threats to those assets, it must conduct a series of risk assessments using quantitative or qualitative analyses, feasibility studies, and cost-benefit analyses. These assessments, which include determining each asset's current protection level, are used to decide whether to proceed with any given control. Armed with a general idea of vulnerabilities in the organization's information technology systems, the security team develops a design blueprint that is used to implement the security program.

This **information security blueprint** is the basis for the design, selection, and implementation of all security program elements, including policy implementation, ongoing policy management, risk management programs, education and training programs, technological controls, and program maintenance. The security blueprint builds on top of the organization's information security policies. It is a detailed implementation of an **information security framework**. The blueprint specifies tasks and the order in which they are to be accomplished, just as an architect's blueprint serves as the design template for the construction of a building. The framework (also known as an information security model) is the philosophical foundation from which the blueprint is designed, like the style or methodology in which an architect was trained.

In choosing a methodology you might use to develop an information security blueprint, you should adapt or adopt a recognized or widely accepted **information security model** backed or promoted by an established security organization or agency. This exemplar framework can outline steps for designing and implementing information security in the organization. Several published information security frameworks from government agencies and other sources are presented later in this chapter. Because each information security environment is unique, the security team may need to modify or adapt pieces from several frameworks. Experience teaches that what works well for one organization may not precisely fit another.

The ISO 27000 Series

One of the most widely referenced security models is the *Information Technology—Code of Practice for Information Security Management*, which was originally published as British Standard BS7799. In 2000, this code of practice was adopted as ISO/IEC 17799, an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The document was revised in 2005 to become ISO 17799:2005, and then it was renamed as ISO 27002 in 2007 to align it with ISO 27001, which is discussed later in this chapter. While the details of ISO/IEC 27002 are available only to those who purchase the standard, its structure and general organization are well known and are becoming increasingly significant for all who work in the area of information security. For a summary description of the structure of ISO 27002:2013, see Table 4-3.

The stated purpose of ISO/IEC 27002, as derived from its ISO/IEC 17799 origins, is to:

> *offer guidelines and voluntary directions for information security management. It is meant to provide a high level, general description of the areas currently considered important when initiating, implementing or maintaining information security in an organization.... The document specifically identifies itself as "a starting point for developing organization specific guidance." It states that not all of the guidance and controls it contains may be applicable and that additional controls not contained may be required. It is not intended to give definitive details or "how-to's."*[13]

ISO/IEC 27002:2013 is focused on a broad overview of the various areas of security. It provides information on 14 security control clauses and addresses 35 control objectives and more than 110 individual controls. Its companion document, ISO/IEC 27001:2013, provides information for how to implement ISO/IEC 27002 and set up an information security

ISO 27002:2013 Contents
Foreword
0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Structure of this standard
5. Information security policies
6. Organization of information security
7. Human resource security
8. Asset management
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
13. Communication security
14. System acquisition, development, and maintenance
15. Supplier relationships
16. Information security incident management
17. Information security aspects of business continuity management
18. Compliance
Bibliography

Table 4-3 The Sections of ISO/IEC 27002:2013[14]

Source: Compiled from various sources.

management system (ISMS). ISO/IEC 27001's primary purpose is to be used as a standard so organizations can adopt it to obtain certification and build an information security program; ISO 27001 serves better as an assessment tool than as an implementation framework. ISO 27002 is for organizations that want information about implementing security controls; it is not a standard used for certification. As shown in Figure 4-7, ISO 27001 has moved from its previous Plan-Do-Check-Act format to a more formal and comprehensive approach to implementing the ISO 27002 control structure.

In the United Kingdom, correct implementation of both volumes of these standards had to be determined by a BS7799 certified evaluator before organizations could obtain ISMS certification and accreditation. When the standard first came out, several countries, including the United States, Germany, and Japan, refused to adopt it, claiming that it had fundamental problems:

- The global information security community had not defined any justification for a code of practice identified in ISO/IEC 17799.

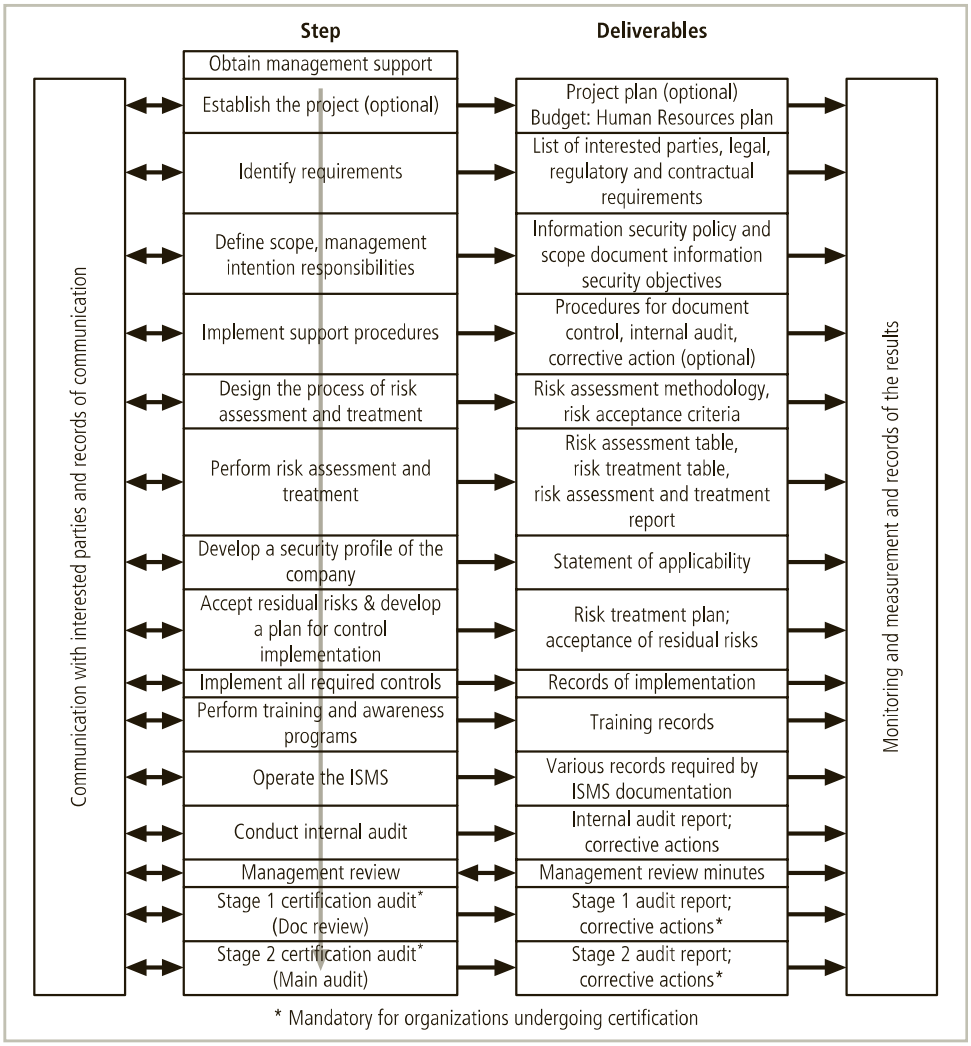


Figure 4-7 ISO/IEC 27001:2013 major process steps

Source: 27001 Academy: ISO 27001 and ISO 22301 Online Consultation Center[15]

- The standard lacked the measurement precision associated with a technical standard.
- There was no reason to believe that ISO/IEC 17799 was more useful than any other approach.
- It was not as complete as other frameworks.
- The standard was hurriedly prepared given the tremendous impact its adoption could have on industry information security controls.[16]

The ISO/IEC 27000 series is becoming increasingly important in the field, especially among global organizations. Many certification bodies and corporate organizations are complying with it or will someday be expected to comply with it.

For more details on ISO/IEC 27001 sections, see www.praxiom.com/iso-27001.htm or www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/.

The ISO has a roadmap for planned standards in the 27000 series related to information security issues and topics. Table 4-4 provides a list of ISO 27000 documents that are currently issued or were planned as of mid-2016.

ISO 27000 Series Standard	Title or Topic	Comment
27000	Series Overview and Terminology	Defines terminology and vocabulary for the standard series
27001:2013	Information Security Management System Specification	Drawn from BS7799:2
27002:2013	Code of Practice for Information Security Management	Renamed from ISO/IEC 17799; drawn from BS7799:1
27003:2010	Information Security Management Systems Implementation Guidelines	Guidelines for project planning requirements for implementing an ISMS
27004:2009	Information Security Measurements and Metrics	Performance measures and metrics for information security management decisions
27005:2011	ISMS Risk Management	Supports 27001, but doesn't recommend any specific risk method
27006:2011	Requirements for Bodies Providing Audit and Certification of an ISMS	Largely intended to support the accreditation of certification bodies providing ISMS certification
27007:2011	Guideline for ISMS Auditing	Focuses on management systems
27008:2011	Guideline for Information Security Auditing	Focuses on security controls
27009:Draft	Sector-specific application of ISO/IEC 27001	Guidance for those who develop "sector-specific" standards based on or relating to ISO/IEC 27001
27010:2015	Information security management for inter-sector and inter-organizational communications	Guidance for inter-sector and inter-organizational communications
27011:2008	Information security management guidelines for telecommunications organizations	Guidance in the application of ISO/IEC 27002 in telecommunications organizations
27013:2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Support for implementing an integrated dual management system
27014:2013	Governance of information security	ISO's approach to security governance—guidance on evaluating, directing, monitoring, and communicating information security
27015:2012	Information Security Management Guidelines for Financial Services	Guidance for financial services organizations
27016:2014	Information security management – Organizational economics	Guidance for understanding the economical consequences of information protection decisions

Table 4-4 ISO 27000 Series Current and Planned Standards

ISO 27000 Series Standard	Title or Topic	Comment
27017:2015	Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Guidance for practice in applying 27002 standards to cloud services
27018:2014	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	Guidance for practice in applying 27002 standards to PII processed in cloud services
27019:2013	Information security management guidelines for process control systems specific to the energy industry	Focused on helping organizations in the energy industry implement ISO standards
27023:2015	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	Guidance on the revised editions of ISO/IEC 27001 and ISO/IEC 27002
27031:2011	Guidelines for information and communication technology readiness for business continuity	Application of ISO/IEC 27002 to information and communication technology readiness for business continuity
27032:2012	Guidelines for cybersecurity	Guidance to achieve cybersecurity
27033-1:2015	Network security – Part 1: Overview and concepts	Overview and concepts of network security
27033-2:2012	Network security – Part 2: Design and implementation of network security	Guidance for the design and implementation of network security
27033-3:2010	Network security – Part 3: Reference networking scenarios – Threats, design techniques, and control issues	Networking scenarios
27033-4:2014	Network security – Part 4: Securing communications between networks using security gateways	Securing communications between networks using security gateways
27033-5:2013	Network security – Part 5: Securing communications across networks using virtual private networks (VPNs)	Securing communications across networks using VPNs
27034-1:2011	Application security – Part 1: Overview and concepts	Overview and concepts of application security
27034-2:2015	Application security – Part 2: Organization normative framework for application security	A framework for application security
27035:2011	Information security incident management	Guidance for information security incident management
27036-1:2014	Information security for supplier relationships – Part 1: Overview and concepts	Overview of information security for supplier relationships
27036-2:2014	Information security for supplier relationships – Part 2: Requirements	Requirements for information security for supplier relationships
27036-3:2013	Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security	Guidelines for information security for supplier relationships

Table 4-4 ISO 27000 Series Current and Planned Standards *(continues)*

ISO 27000 Series Standard	Title or Topic	Comment
27038:2014	Specification for digital redaction	Digital redaction specification
27039:2015	Selection, deployment, and operations of intrusion detection systems (IDPSs)	Guidance for IDPS selection, deployment, and operations
27040:2015	Storage security	Guidance on storage security
27041:2015	Guidance on assuring suitability and adequacy of incident investigative methods	Guidance on incident investigative methods
27042:2015	Guidelines for the analysis and interpretation of digital evidence	Guidelines for the analysis and interpretation of digital evidence
27043:2015	Incident investigation principles and processes	Incident investigation principles and processes
27799:2008	Health informatics – Information security management in health using ISO/IEC 27002	Provides guidance to health organizations and other holders of personal health information on how to protect such information via implementation of ISO/IEC 27002
Identified Future 27000 Series Standards (In Draft)		
27033-6	Network security – Part 6: Securing wireless IP network access	
27034-3	Application security – Part 3: Application security management process	
27034-5	Application security – Part 5: Protocols and application security controls data structure – XML schemas	
27034-7	Application security – Part 7: Application security assurance prediction	
27035-2	Information security incident management – Part 2: Guidelines to plan and prepare for incident response	
27035-3	Information security incident management – Part 3: Guidelines for CSIRT operations	
27036-4	Information security for supplier relationships – Part 4: Guidelines for security of cloud services	

Table 4-4 ISO 27000 Series Current and Planned Standards[17] *(continued)*

Note: Additional 27000 series documents are in preparation and are not included here.

Source: www.iso27001security.com/html/iso27000.html.

NIST Security Models

Other approaches are described in the many documents available from the NIST Computer Security Resource Center (*http://csrc.nist.gov*). Because the NIST documents are publicly available at no charge and have been for some time, they have been broadly reviewed by government and industry professionals, and were among the references cited by the U.S. government when it decided not to select the ISO/IEC 17799 (now 27000 series) standards. The following NIST documents can assist in the design of a security framework:

- SP 800-12: *An Introduction to Computer Security: The NIST Handbook*
- SP 800-14: *Generally Accepted Principles and Practices for Securing Information Technology Systems*
- SP 800-18 Rev. 1: *Guide for Developing Security Plans for Federal Information Systems*

- SP 800-30 Rev. 1: *Guide for Conducting Risk Assessments*
- SP 800-37 Rev. 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- SP 800-39: *Managing Information Security Risk: Organization, Mission, and Information System View*
- SP 800-50: *Building an Information Technology Security Awareness and Training Program*
- SP 800-55 Rev. 1: *Performance Measurement Guide for Information Security*
- SP 800-100: *Information Security Handbook: A Guide for Managers*

Many of these documents have been referenced earlier in this book as sources of information for the management of security. The following sections examine these documents as they apply to the blueprint for information security.

NIST SP 800-12 SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, is an excellent reference and guide for the security manager or administrator in the routine management of information security. It provides little guidance, however, for the design and implementation of new security systems, and therefore should be used only as a precursor to understanding an information security blueprint.

NIST SP 800-14 SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, provides best practices and security principles that can direct the security team in the development of a security blueprint. In addition to detailing security best practices across the spectrum of security areas, it provides philosophical principles that the security team should integrate into the entire information security process. The document can guide the development of the security framework and should be combined with other NIST publications to provide the necessary structure for the entire security process. While the document itself is a bit aged, many of the principles and approaches to information security are timeless.

The scope of NIST SP 800-14 is broad, so you should consider each of the security principles it presents. The following sections examine some of its significant points in more detail.

- *2.1 Security supports the mission of the organization*: Failure to develop an information security system based on the organization's mission, vision, and culture guarantees the failure of the information security program.
- *2.2 Security is an integral element of sound management*: Effective management includes planning, organizing, leading, and controlling. Security enhances management functions by providing input during the planning process for organizational initiatives. Information security controls support sound management via the enforcement of managerial and security policies.
- *2.3 Security should be cost-effective*: The costs of information security should be considered part of the cost of doing business, much like the costs of computers, networks, and voice communications systems. Security is not a profit-generating area of the organization and may not lead to competitive advantages. Information security should justify its own costs. The use of security measures that do not justify their cost must have a strong business justification, such as a legal requirement.

- *2.4 Systems owners have security responsibilities outside their own organizations*: Whenever systems store and use information from customers, patients, clients, partners, or others, the security of this information becomes the responsibility of the systems' owners. These owners are expected to diligently work with each other to assure the confidentiality, integrity, and availability of the entire value chain of their interconnected systems.
- *2.5 Security responsibilities and accountability should be made explicit*: Policy documents should clearly identify the security responsibilities of users, administrators, and managers. To be legally binding, the policies must be documented, disseminated, read, understood, and agreed to by all involved members of the organization. As noted in Chapter 3, ignorance of the law is no excuse, but ignorance of policy is. Organizations should also provide information about relevant laws in issue-specific security policies.
- *2.6 Security requires a comprehensive and integrated approach*: Security personnel alone cannot effectively implement security. As emphasized throughout this textbook, *security is everyone's responsibility*. The three communities of interest—information technology management and professionals, information security management and professionals, and users, managers, administrators, and other stakeholders—should participate in the process of developing a comprehensive information security program.
- *2.7 Security should be periodically reassessed*: Information security that is implemented and then ignored is considered negligent because the organization has not demonstrated due diligence. Security is an ongoing process. To be effective against a constantly shifting set of threats and a changing user base, the security process must be periodically repeated. Continuous analyses of threats, assets, and controls must be conducted and new blueprints developed. Only thorough preparation, design, implementation, vigilance, and ongoing maintenance can secure the organization's information assets.
- *2.8 Security is constrained by societal factors*: Several factors influence the implementation and maintenance of security controls and safeguards, including legal demands, shareholder requirements, and even business practices. For example, security professionals generally prefer to isolate information assets from the Internet, which is the leading avenue of threats to the assets, but the business requirements of the organization may preclude this control measure.

Table 4-5 lists the principles for securing information technology systems, which is part of NIST SP 800-14. You can use this document to make sure the needed key elements of a successful effort are factored into the design of an information security program and to produce a blueprint for an effective security architecture.

NIST SP 800-18 Rev. 1 SP 800-18 Rev. 1, The *Guide for Developing Security Plans for Federal Information Systems*, can be used as the foundation for a comprehensive security blueprint and framework. This publication provides detailed methods for assessing, designing, and implementing controls and plans for applications of varying size. SP 800-18 Rev. 1 can serve as a useful guide to the activities described in this chapter and as an aid in the planning process. It also includes templates for major application security plans. As with any publication of this scope and magnitude, SP 800-18 Rev. 1 must be customized to fit the particular needs of an organization.

Principles and Practices for Securing IT Systems	
1.	Establish a sound security policy as the foundation for design.
2.	Treat security as an integral part of the overall system design.
3.	Clearly delineate the physical and logical security boundaries governed by associated security policies.
4.	Reduce risk to an acceptable level.
5.	Assume that external systems are insecure.
6.	Identify potential trade-offs among reducing risk, increased costs, and decreases in other aspects of operational effectiveness.
7.	Implement layered security to ensure there is no single point of vulnerability.
8.	Implement tailored system security measures to meet the organization's security goals.
9.	Strive for simplicity.
10.	Design and operate an IT system to limit vulnerability and to be resilient in response.
11.	Minimize the system elements to be trusted.
12.	Implement security through a combination of measures distributed physically and logically.
13.	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
14.	Limit or contain vulnerabilities.
15.	Formulate security measures to address multiple overlapping information domains.
16.	Isolate public access systems from mission-critical resources, such as data and processes.
17.	Use boundary mechanisms to separate computing systems and network infrastructures.
18.	Where possible, base security on open standards for portability and interoperability.
19.	Use common language in developing security requirements.
20.	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
21.	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
22.	Authenticate users and processes to ensure appropriate access control within and across domains.
23.	Use unique system identities that are tied to people who have defined relationships to the organization and are linked to specific data ownership and usage roles to ensure accountability.
24.	Implement least privilege.
25.	Do not implement unnecessary security mechanisms.
26.	Protect information while it is being processed, in transit, and in storage.
27.	Strive for operational ease of use.
28.	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
29.	Consider custom products to achieve adequate security.
30.	Ensure proper security in the shutdown or disposal of a system.
31.	Protect against all likely classes of attacks.
32.	Identify and prevent common errors and vulnerabilities.
33.	Ensure that developers are trained in how to develop secure software.

Table 4-5 Principles for Securing Information Technology Systems[18]

Source: NIST SP 800-14.

NIST and the Risk Management Framework NIST's approach to managing risk in the organization, titled the Risk Management Framework (RMF), emphasizes the following:

- *Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls*
- *Maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes*
- *Providing essential information to help senior leaders make decisions about accepting risk to an organization's operations and assets, individuals, and other organizations arising from the use of information systems*

The RMF has the following characteristics:

- *Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring*
- *Encourages the use of automation to provide senior leaders with necessary information to make cost-effective, risk-based decisions about information systems that support an organization's core missions and business functions*
- *Integrates information security into the enterprise architecture and system development life cycle*
- *Emphasizes the selection, implementation, assessment, and monitoring of security controls and the authorization of information systems*
- *Links risk management processes at the information system level to risk management processes at the organization level through a risk executive function*
- *Establishes responsibility and accountability for security controls deployed within an organization's information systems and inherited by those systems (i.e., common controls).*[19]

The NIST Risk Management Framework is discussed in detail in Chapter 5, "Risk Management."

The NIST Cybersecurity Framework In early 2014, NIST published a new Cybersecurity Framework in response to Executive Order 13636 from President Obama. NIST's mandate was to create a voluntary framework that provides an effective approach to "manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services."[20] The resulting framework, which is designed specifically to be vendor-neutral, closely resembles the other approaches described in this textbook, but it provides additional structure to the process, if not detail. The NIST Framework builds on and works closely with the RMF described in the previous section. The Framework document represents the integration of previously discussed special publications from NIST, in a form that makes the Framework easier to understand and enables organizations to implement an information security improvement program.

The intent of the Framework is to allow organizations to: "1) Describe their current cybersecurity posture; 2) Describe their target state for cybersecurity; 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; 4) Assess progress toward the target state; and 5) Communicate among internal and external stakeholders about cybersecurity risk."[21]

The NIST Framework consists of three fundamental components:

- The Framework core: This is a set of information security activities an organization is expected to perform, as well as their desired results. These core activities are:
  - "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."[22]
- The Framework tiers: The Framework then provides a self-defined set of tiers so organizations can relate the maturity of their security programs and implement corresponding measures and functions. The four tiers include:
  - Tier 1: Partial: In this category, an organization does not have formal risk management practices, and security activities are relatively informal and ad hoc.
  - Tier 2: Risk Informed: Organizations in this category have developed but not fully implemented risk management practices, and have just begun their formal security programs, so security is not fully established across the organization.
  - Tier 3: Repeatable: Organizations in this category not only have risk management practices formally established, they also have documented policy implemented. The organization has begun a repeatable security program to improve its approach to information protection and proactively manage risk to information assets.
  - Tier 4: Adaptive: The most mature organization falls into this tier. The organization not only has well-established risk management and security programs, it can quickly adapt to new environments and threats. The organization is experienced at managing risk and responding to threats and has integrated security completely into its culture.
- The Framework profile: Organizations are expected to identify which tier their security programs most closely match and then use corresponding recommendations within the Framework to improve their programs. This Framework profile is then used to

perform a gap analysis—comparing the current state of information security and risk management to a desired state, identifying the difference, and developing a plan to move the organization toward the desired state. This approach is identical to the approaches outlined elsewhere in this text.

Using the materials provided in the NIST Framework, organizations are encouraged to follow a seven-step approach to implementing or improving their risk management and information security programs:

- "Step 1: Prioritize and scope: The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process.
- Step 2: Orient: Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.
- Step 3: Create a current profile: The organization develops a current profile by indicating which category and subcategory outcomes from the Framework core are currently being achieved.
- Step 4: Conduct a risk assessment: This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization.
- Step 5: Create a target profile: The organization creates a target profile that focuses on the assessment of the Framework categories and subcategories describing the organization's desired cybersecurity outcomes.
- Step 6: Determine, analyze, and prioritize gaps: The organization compares the current profile and the target profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost-benefit analysis, and understanding of risk to achieve the outcomes in the target profile. The organization then determines resources necessary to address the gaps.
- Step 7: Implement action plan: The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the target profile."[23]

As you learned in Chapter 1 while studying the SecSDLC waterfall methodology, the preceding steps are designed to be an iterative process that gradually moves the organization closer to a Tier 4 security level and results in a better approach to risk management and information protection.

NIST also provides a "Roadmap for Improving Critical Infrastructure Cybersecurity,"[24] which provides supplemental guidance for the Framework and insights into its future development and refinement as an evolutionary, living document.

For more information on the NIST Cybersecurity Framework, visit the NIST Web site at www.nist.gov/cyberframework.

Other Sources of Security Frameworks

Many public and private organizations promote solid best security practices. A variety of public and semipublic institutions provide information on best practices—one is the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University (*www.cert.org*). CERT/CC provides detailed and specific assistance for how to implement a sound security methodology.

Professional societies often provide information on best practices for their members. The Technology Manager's Forum (*www.techforum.com*) has an annual best practice award in several areas, including information security. The Information Security Forum (*www.securityforum.org*) has a free publication titled "Standard of Good Practice for Information Security," which outlines information security best practices.

Many organizations hold seminars and classes on best practices for implementing security; in particular, the Information Systems Audit and Control Association (*www.isaca.org*) hosts regular seminars. The International Association of Professional Security Consultants (*www.iapsc.org*) has a listing of best practices. At a minimum, information security professionals can peruse Web portals for posted security best practices. Several free portals dedicated to security have collections of best practices, such as SearchSecurity.com and NIST's Computer Resources Center.

Design of Security Architecture

Key Terms

defense in depth A strategy for the protection of information assets that uses multiple layers and different types of controls (managerial, operational, and technical) to provide optimal protection.

managerial controls Information security safeguards that focus on administrative planning, organizing, leading, and controlling, and that are designed by strategic planners and implemented by the organization's security administration. These safeguards include governance and risk management.

operational controls Information security safeguards focusing on lower-level planning that deals with the functionality of the organization's security. These safeguards include disaster recovery and incident response planning.

redundancy The use of multiple types and instances of technology that prevent the failure of one system from compromising the security of information.

security domain An area of trust within which information assets share the same level of protection. Each trusted network within an organization is a security domain. Communication between security domains requires evaluation of communications traffic.

security perimeter The boundary in the network within which an organization attempts to maintain security controls for securing information from threats from untrusted network areas. The advent of mobile and cloud information technologies makes the security perimeter increasingly difficult to define and secure.

technical controls Information security safeguards that focus on the application of modern technologies, systems, and processes to protect information assets. These safeguards include firewalls, virtual private networks, and IDPSs.

To inform the discussion of information security program architecture and to illustrate industry best practices, the following sections outline a few key components of security

architecture. Many of these components are examined in detail in later chapters of the book, but this overview can help you assess whether a framework and blueprint are on target to meet an organization's needs.

Spheres of Security The spheres of security, shown in Figure 4-8, are the foundation of the security framework. Generally speaking, the spheres of security illustrate how information is under attack from a variety of sources. The sphere of use, on the left side of Figure 4-8, illustrates the ways in which people access information. For example, people read hard copies of documents and access information through systems. Information, as the most important asset in this model, is at the center of the sphere. Information is always at risk from attacks whenever it is accessible by people or computer systems. Networks and the Internet are indirect threats, as exemplified by the fact that a person attempting to access information from the Internet must traverse local networks.

The sphere of protection, as shown by the shaded bands on the right side of Figure 4-8, illustrates that a layer of protection must exist between each layer of the sphere of use. For example, "Policy and law" and "Education and training" are protections placed between people and the information. Controls are also implemented between systems and the information, between networks and the computer systems, and between the Internet and internal networks. This reinforces the concept of defense in depth. A variety of controls can be used to protect the information. The items of control shown in the figure are not intended to be comprehensive, but they illustrate some of the safeguards that can protect the systems closer to the center of the sphere. Because people can directly access each ring as well as the information at the core of the model, the side of the sphere of protection that attempts to control

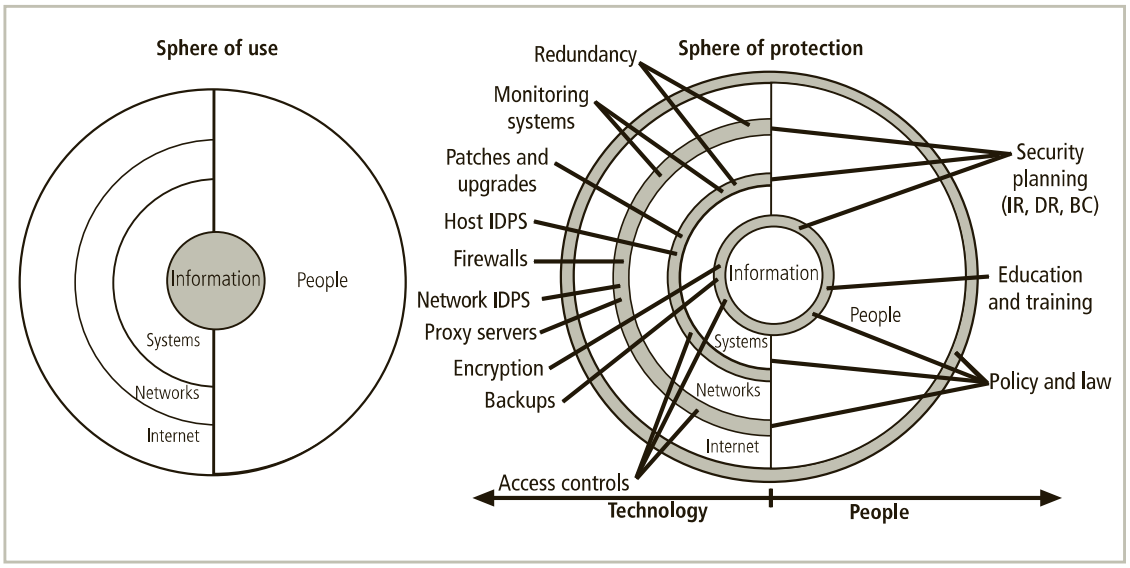


Figure 4-8 Spheres of security

access by relying on people requires a different approach to security than the side that uses technology. The members of the organization must become a safeguard that is effectively trained, implemented, and maintained, or they too will present a threat to the information.

Information security is designed and implemented in three layers: policies, people (education, training, and awareness programs), and technology. These layers are commonly referred to as PPT. Each layer contains controls and safeguards to protect the information and information system assets that the organization values. But, before any technical controls or other safeguards can be implemented, the policies that define the management philosophies behind the security process must be in place.

Levels of Controls Information security safeguards provide three levels of control: managerial, operational, and technical. **Managerial controls** set the direction and scope of the security process and provide detailed instructions for its conduct. In addition, these controls address the design and implementation of the security planning process and security program management. They also address risk management and security control reviews (as described in Chapter 5), describe the necessity and scope of legal compliance, and set guidelines for the maintenance of the entire security life cycle.

Operational controls address personnel security, physical security, and the protection of production inputs and outputs. In addition, operational controls guide the development of education, training, and awareness programs for users, administrators, and management. Finally, they address hardware and software systems maintenance and the integrity of data.

Technical controls are the tactical and technical implementations of security in the organization. While operational controls address specific operating issues, such as developing and integrating controls into the business functions, technical controls include logical access controls, such as identification, authentication, authorization, accountability (including audit trails), cryptography, and the classification of assets and users.

Defense in Depth A basic tenet of security architectures is the layered implementation of security. To achieve **defense in depth**, an organization must establish multiple layers of security controls and safeguards, which can be organized into policy, training and education, and technology, as shown in the CNSS model presented in Chapter 1. While policy itself may not prevent attacks, it certainly prepares the organization to handle them; when coupled with other layers, policy can deter attacks. For example, the layer of training and education can help defend against attacks enabled by employee ignorance and social engineering. Technology is also implemented in layers, with detection equipment working in tandem with reaction technology behind access control mechanisms. **Redundancy** can be implemented at several points throughout the security architecture, such as in firewalls, proxy servers, and access controls. Figure 4-9 illustrates the concept of building controls in multiple and sometimes redundant layers. The figure shows firewalls and prevention IDPSs that use both packet-level rules (shown as the packet header in the diagram) and content analysis (shown as a database icon with the caption 0100101011). More information on firewalls and intrusion detection systems is presented in Chapters 6 and 7, respectively.

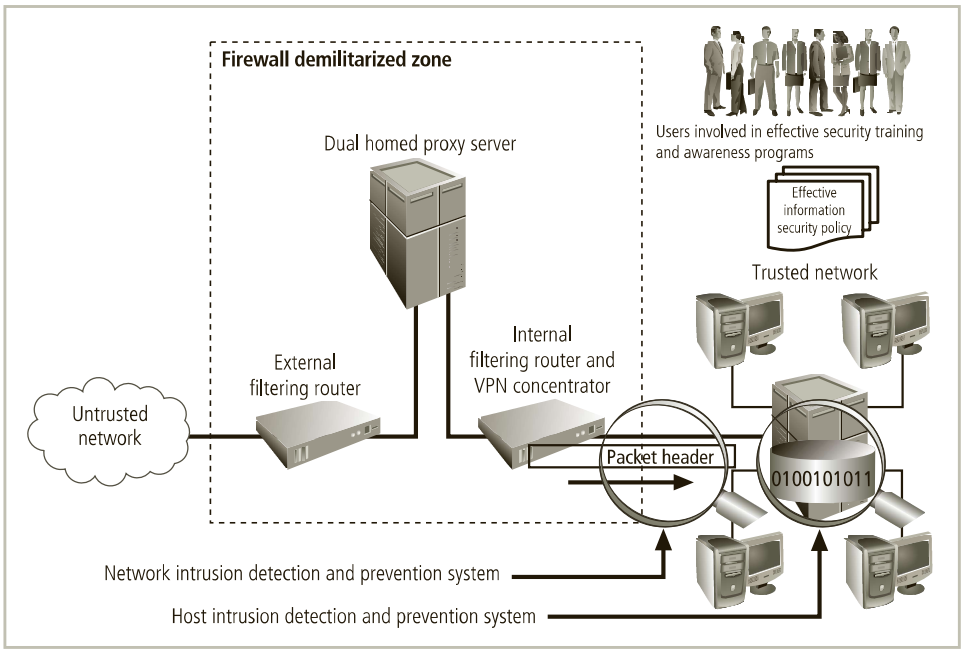


Figure 4-9 Defense in depth

Security Perimeter A perimeter is a boundary of an area. A **security perimeter** is the border of security that protects all internal systems from outside threats, as pictured in Figure 4-10. Unfortunately, the perimeter does not protect against internal attacks from employee threats or onsite physical threats. In addition, the emergence of mobile computing devices, telecommuting, and cloud-based functionality has made the definition and defense of the perimeter increasingly more difficult. This has led some security experts to declare the security perimeter extinct and call for an increased focus on improved system-level security and active policing of networked assets. An organization can have both an electronic security perimeter, usually at the exterior network or Internet connection, and a physical security perimeter, usually at the entrance to the organization's offices. Both require perimeter security. Security perimeters can effectively be implemented as multiple technologies that segregate the protected information from potential attackers. Within security perimeters the organization can establish **security domains**, each with differing levels of security, between which traffic must be screened. The assumption is that if people have access to one system within a security domain, they have authorized access to all systems within that domain. The security perimeter is an essential element of the overall security framework, and its implementation details are the core of the completed security blueprint. The key components of the security perimeter are firewalls, DMZs (demilitarized zones), proxy servers, and IDPSs. You will learn more about information security technologies in Chapters 6, 7, and 8.

Many security experts argue that the security perimeter is dead. With the dramatic growth in popularity of cloud-based computing and data storage, and the continued use of mobile

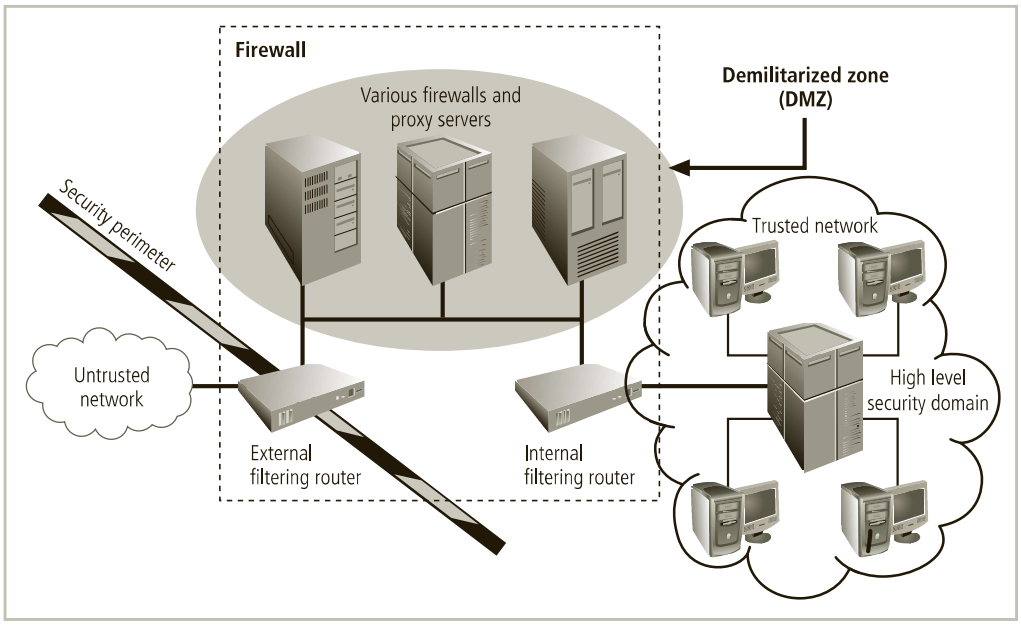


Figure 4-10 Security perimeters and domains

computing devices, they argue that there is no "inside" or "outside" to organizations' networks anymore. Whether this is true is the subject of much debate. With the extensive use of cloud-based services to deliver key systems capability, including security-related functions, there is a growing movement toward realizing that a security perimeter is the entirety of an organization's network presence, anywhere and everywhere the company's data is, and that the use of defense in depth is still a valid approach to protecting it. Whether you subscribe to the "perimeter is dead" philosophy or not, the responsibility for protecting the organization's data using every available resource is still alive and well.

Security Education, Training, and Awareness Program

Key Term

security education, training, and awareness (SETA) A managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance for an organization's employees.

Once your organization has defined the policies that will guide its security program and selected an overall security model by creating or adapting a security framework and a corresponding detailed implementation blueprint, it is time to implement a **security education, training, and awareness** (SETA) program. The SETA program is the responsibility of the

CISO and is a control measure designed to reduce incidents of accidental security breaches by employees. Employee errors are among the top threats to information assets, so it is well worth developing programs to combat this threat. SETA programs are designed to supplement the general education and training programs that many organizations use to educate staff about information security. For example, if an organization detects that many employees are opening questionable e-mail attachments, those employees must be retrained. As a matter of good practice, systems development life cycles must include user training during the implementation phase. Practices used to take control of the security and privacy of online data are sometimes called *cyber hygiene*.

The SETA program consists of three elements: security education, security training, and security awareness. An organization may not be able or willing to undertake all three of these elements, and it may outsource elements to local educational institutions. The purpose of SETA is to enhance security by doing the following:

- Improving awareness of the need to protect system resources
- Developing skills and knowledge so computer users can perform their jobs more securely
- Building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems[25]

Table 4-6 compares the features of security education, training, and awareness within the organization.

Security Education

Everyone in an organization needs to be trained and made aware of information security, but not everyone needs a formal degree or certificate in information security. When management

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction • Discussion seminar • Background reading • Hands-on practice	Practical instruction • Lecture • Case study workshop • Posters	Media • Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

Table 4-6 Comparative Framework of SETA[26]

Source: NIST SP 800-12.

agrees that formal education is appropriate, an employee can investigate courses in continuing education from local institutions of higher learning. Several universities have formal coursework in information security. For people who are interested in researching formal information security programs, resources are available, such as the DHS/NSA-identified National Centers of Academic Excellence program (see *www.iad.gov/NIETP/index.cfm*). This program identifies universities that offer coursework in information security and an integrated view of information security in the institution itself. Other local resources can also provide information on security education, such as Kennesaw State's Center for Information Security Education (*http://infosec.kennesaw.edu)*.

Security Training

Security training provides employees with detailed information and hands-on instruction to prepare them to perform their duties securely. Management of information security can develop customized in-house training or outsource the training program.

Alternatives to formal training programs are industry training conferences and programs offered through professional agencies such as SANS (*www.sans.org*), $(ISC)^2$ (*www.isc2.org*), and ISSA (*www.issa.org*). All of these agencies have been described in previous chapters. Many of these programs are too technical for the average employee, but they may be ideal for the continuing education requirements of information security professionals.

Several resources for conducting SETA programs offer assistance in the form of sample topics and structures for security classes. For organizations, the Computer Security Resource Center at NIST provides several useful documents free of charge in its special publications area *(http://csrc.nist.gov)*.

Security Awareness

A security awareness program is one of the least frequently implemented but most beneficial programs in an organization. A security awareness program is designed to keep information security at the forefront of users' minds. These programs don't have to be complicated or expensive. Good programs can include newsletters, security posters (see Figure 4-11 for an example), videos, bulletin boards, flyers, and trinkets. Trinkets can include security slogans printed on mouse pads, coffee cups, T-shirts, pens, or any object frequently used during the workday that reminds employees of security. In addition, a good security awareness program requires a dedicated person who is willing to invest time and effort to promoting the program, and a champion willing to provide the needed financial support.

The security newsletter is the most cost-effective method of disseminating security information and news to employees. Newsletters can be distributed via hard copy, e-mail, or intranet. Topics can include new threats to the organization's information assets, the schedule for upcoming security classes, and the addition of new security personnel. The goal is to keep the idea of information security in users' minds and to stimulate users to care about security. If a security awareness program is not actively implemented, employees may begin to neglect security matters and the risk of employee accidents and failures is likely to increase.

Figure 4-11 Information security awareness at Kennesaw State University

Continuity Strategies

Key Terms

adverse event An event with negative consequences that could threaten the organization's information assets or operations. Sometimes referred to as an incident candidate.

business continuity plan (BC plan) The documented product of business continuity planning; a plan that shows the organization's intended efforts to continue critical functions when operations at the primary site are not feasible.

business continuity planning (BCP) The actions taken by senior management to develop and implement the BC policy, plan, and continuity teams.

business resumption planning (BRP) The actions taken by senior management to develop and implement a combined DR and BC policy, plan, and set of recovery teams.

contingency plan The documented product of contingency planning; a plan that shows the organization's intended efforts in reaction to adverse events.

contingency planning (CP) The actions taken by senior management to specify the organization's efforts and actions if an adverse event becomes an incident or disaster. This planning includes incident response, disaster recovery, and business continuity efforts, as well as preparatory business impact analysis.

contingency planning management team (CPMT) The group of senior managers and project members organized to conduct and lead all CP efforts.

disaster An adverse event that could threaten the viability of the entire organization. A disaster may either escalate from an incident or be initially classified as a disaster.

disaster recovery plan (DR plan) The documented product of disaster recovery planning; a plan that shows the organization's intended efforts in the event of a disaster.

disaster recovery planning (DRP) The actions taken by senior management to specify the organization's efforts in preparation for and recovery from a disaster.

incident An adverse event that could result in loss of an information asset or assets, but does not currently threaten the viability of the entire organization.

incident response plan (IR plan) The documented product of incident response planning; a plan that shows the organization's intended efforts in the event of an incident.

incident response planning (IRP) The actions taken by senior management to develop and implement the IR policy, plan, and computer security incident response team.

A key role for all managers is **contingency planning** (CP). Managers in the IT and information security communities are usually called on to provide strategic planning to assure the continuous availability of information systems.[27] Unfortunately for managers, however, the probability that some form of attack will occur—from inside or outside, intentional or accidental, human or nonhuman, annoying or catastrophic—is very high. Thus, managers from each community of interest must be ready to act when a successful attack occurs.

Various types of contingency plans are available to respond to **adverse events**, including incident response plans, disaster recovery plans, and business continuity plans. In some organizations, these might be handled as a single integrated plan. In large, complex organizations, each of these plans may cover separate but related planning functions that differ in scope, applicability, and design. In a small organization, the security administrator or systems administrator may have one simple plan that consists of a straightforward set of media backup and recovery strategies and service agreements from the company's service providers. However, the sad reality is that many organizations have a level of planning that is woefully deficient.

Plans for incident response, disaster recovery, and business continuity are components of contingency planning, as shown in Figure 4-12. A **contingency plan** is prepared by the organization to anticipate, react to, and recover from events that threaten the security of information

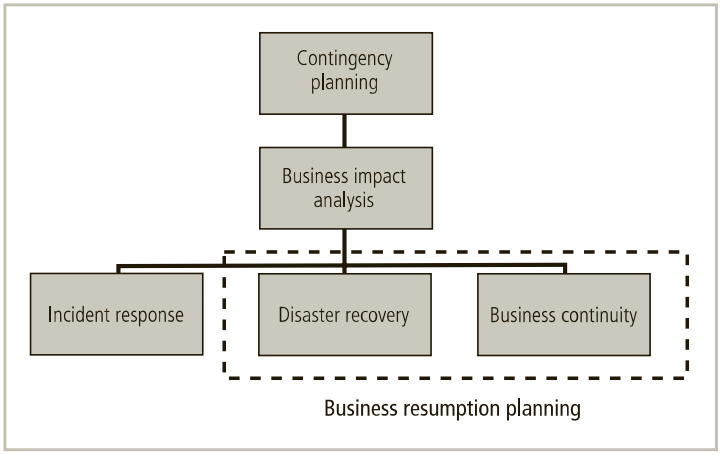


Figure 4-12 Components of contingency planning

and information assets in the organization. This plan also helps restore the organization to normal modes of business operations after an event. The discussion of contingency planning begins by explaining the differences among its various elements and examining the points at which each element is brought into play.

CP includes **incident response planning** (**IRP**), **disaster recovery planning** (**DRP**), and **business continuity planning** (**BCP**), in preparation for adverse events that become **incidents** or **disasters**. The primary functions of these three types of planning are as follows:

- The **incident response plan** (**IR plan**) focuses on immediate response, but if the attack escalates or is disastrous (for example, a fire, flood, earthquake, or total blackout), the process moves on to disaster recovery and the BC plan.
- The **disaster recovery plan** (**DR plan**) typically focuses on restoring systems at the original site after disasters occur, and so is closely associated with the BC plan.
- The **business continuity plan** (**BC plan**) occurs concurrently with the DR plan when the damage is major or ongoing, and requires more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site.

Some experts argue that the DR and BC plans are so closely linked that they are indistinguishable (a.k.a. **business resumption planning, or BRP**). However, each has a distinct role and planning requirement. The following sections detail the tasks necessary for each of the three types of plans. You can also further distinguish among these types of planning by examining when each comes into play during the life of an incident. Figure 4-13 shows a sample

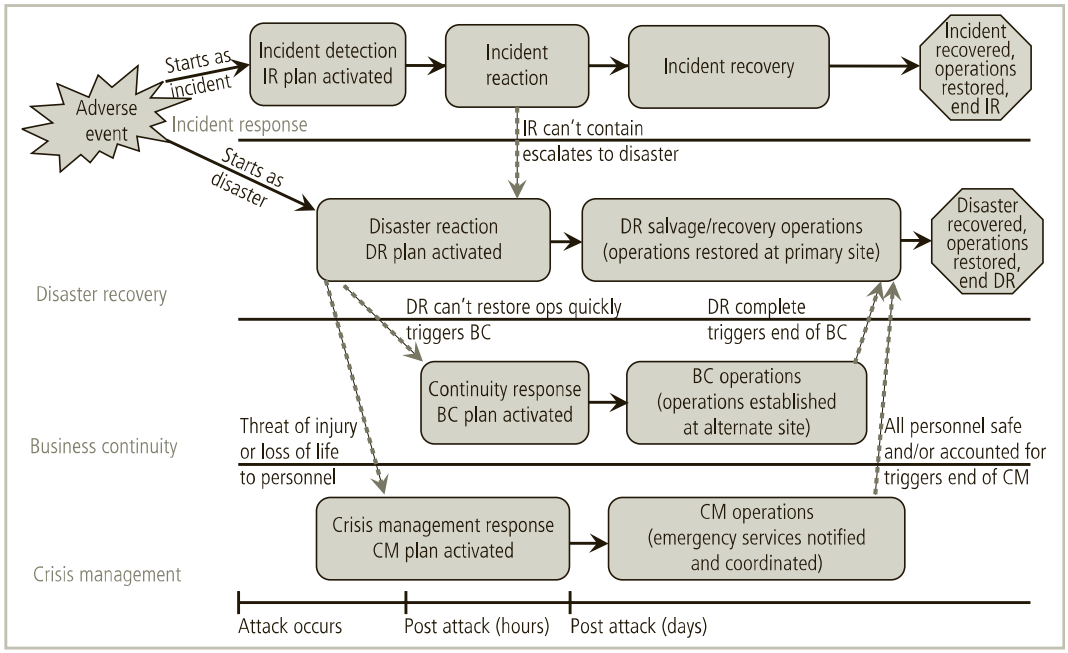


Figure 4-13 Contingency planning timeline

sequence of events and the overlap between when each plan comes into play. Disaster recovery activities typically continue even after the organization has resumed operations at the original site.

Before any planning can begin, an assigned person or a planning team has to get the process started. In the usual case, a **contingency planning management team (CPMT)** is assembled for that purpose. A roster for this team may consist of the following members:

- Champion: As with any strategic function, the contingency planning project must have a high-level manager to support, promote, and endorse the findings of the project. This could be the CIO or ideally the CEO.
- Project manager: A mid-level manager or even the CISO must lead the project and make sure a sound planning process is used, a complete and useful project plan is developed, and resources are prudently managed to reach the goals of the project.
- Team members: The team members should be managers or their representatives from the various communities of interest: business, information technology, and information security.

The CPMT is responsible for obtaining commitment and support from senior management, writing the contingency plan document, conducting the business impact analysis (BIA), and organizing the subordinate teams.

The overall CP process, which should integrate the BIA, IRP, and DRP efforts, includes the following steps, once the CPMT (and other subordinate teams) have been formed:

1. *Develop the CP policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.*
2. *Conduct the BIA. The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes. A template for developing the BIA is provided to assist the user.*
3. *Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.*
4. *Create contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.*
5. *Develop a contingency plan. The contingency plan should contain detailed guidance and procedures for restoring damaged organizational facilities unique to each business unit's impact level and recovery requirements.*
6. *Ensure plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.*
7. *Ensure plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.*[28]

This seven-step methodology recommended by NIST for DRP and BCP has been expanded to include details of the BIA and IRP, resulting in the model shown in Figure 4-14. As you read the remainder of this chapter, you might want to refer back to this diagram because many

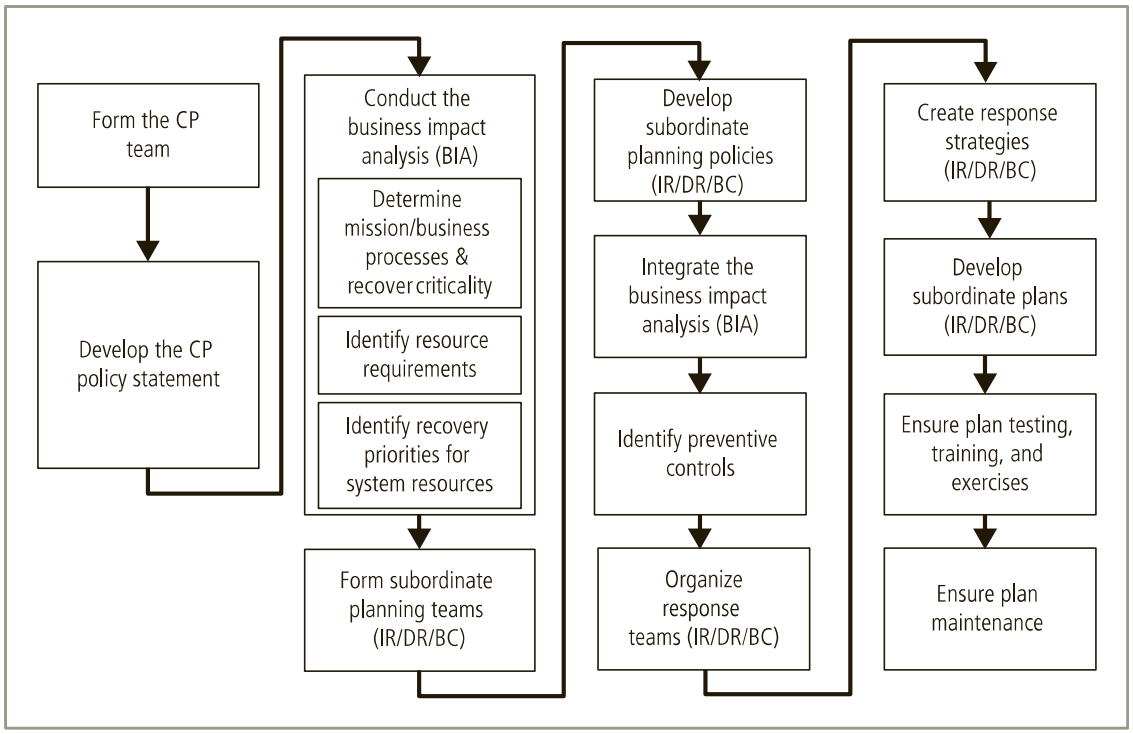


Figure 4-14 Major steps in contingency planning

upcoming sections correspond to the steps depicted in it. Note that each subordinate planning task begins with the creation (or update) of a corresponding policy document that specifies the purpose and scope of the plan and identifies roles and responsibilities for the plan's creation and implementation.

The stages of the CP development methodology are adapted from NIST's SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems (2010), and SP 800-61, Rev. 1, Computer Security Incident Handling Guide (2008). Including the formulation of the CPMT, these stages are:

1. "Form the CPMT. Assemble the management team that will guide CP planning and execution. This includes representatives from business management, operations, and the projected subordinate teams.
2. Develop the contingency planning policy statement. The CP policy is the formal policy that will guide the efforts of the subordinate teams in developing their plans, and the overall operations of the organization during contingency operations.
3. Conduct the business impact analysis (BIA). The BIA, described later in this chapter, helps identify and prioritize organizational functions, and the information systems and components critical to supporting the organization's mission/business processes.
4. Form subordinate planning teams. For each of the subordinate areas, organize a team to develop the IR, DR, and BC plans. These groups may or may not contain people responsible for implementing the plan.

5. Develop subordinate planning policies. Just as the CPMT develops an overall CP policy, the newly formed IR, DR, and BC planning teams will begin by developing an IR, DR, or BC planning policy, respectively.
6. Integrate the business impact analysis. Each of the subordinate planning teams will independently review and incorporate aspects of the BIA of importance to their planning efforts. As different teams may need different components, the actions and assessments of each team may vary.
7. Identify preventive controls. Assess those countermeasures and safeguards that mitigate the risk and impact of events on organizational data, operations, and personnel.
8. Organize response teams. Specify the skills needed on each subordinate response team (IR/DR/BC) and identify personnel needed. Ensure personnel rosters are exclusive (no personnel on two different teams) and that all needed skills are covered. These are the people who will be directly called up if a particular plan is activated in response to an actual incident or disaster.
9. Create contingency strategies. The CPMT, with input from the subordinate team leaders, will evaluate and invest in strategies that support the IR, DR, and BC efforts should an event affect business operations. These include data backup and recovery plans, off-site data storage, and alternate site occupancy strategies.
10. Develop subordinate plans. For each subordinate area, develop a plan to handle the corresponding actions and activities necessary to (a) respond to an incident, (b) recover from a disaster, and (c) establish operations at an alternate site following a disruptive event.
11. Ensure plan testing, training, and exercises. Ensure each subordinate plan is tested and the corresponding personnel are trained to handle any event that escalates into an incident or a disaster.
12. Ensure plan maintenance. Manage the plan, ensuring periodic review, evaluation, and update."

The CP Policy

The CP policy should contain the following sections:

- An introductory statement of philosophical perspective by senior management that explains the importance of contingency planning to the strategic, long-term operations of the organization
- A statement of the scope and purpose of the CP operations, specifically the requirement to cover all critical business functions and activities
- A call for periodic risk assessment and business impact analysis by the CPMT to include identification and prioritization of critical business functions (while this is intuitive to the CPMT, the formal inclusion in policy reinforces the need for such studies in the remainder of the organization)
- A specification of the CP's major components to be designed by the CPMT, as described earlier
- A call for, and guidance in, the selection of recovery options and business continuity strategies

- A requirement to test the various plans on a regular basis, whether semiannually, annually, or more often as needed
- Identification of key regulations and standards that affect CP planning and a brief overview of their relevancy
- Identification of key people responsible for CP operations, such as establishment of the COO as CPMT champion, the deputy COO as CPMT team lead/project manager, CISO as IR team lead, manager of business operations as DR team lead, manager of marketing and services as BC team lead, and legal counsel as crisis management team lead
- A challenge to individual members of the organization that asks for their support and reinforces their importance as part of the overall CP process
- Additional administrative information, including the date of the document's original authorship, revisions, and a schedule for periodic review and maintenance

Business Impact Analysis

Key Terms

business impact analysis (BIA) An investigation and assessment of the various adverse events that can affect the organization, conducted as a preliminary phase of the contingency planning process, which includes a determination of how critical a system or set of information is to the organization's core processes and recovery priorities.

maximum tolerable downtime (MTD) The total amount of time the system owner or authorizing official is willing to accept for a mission/business process outage or disruption, including all impact considerations.

recovery point objective (RPO) The point in time prior to a disruption or system outage to which mission/business process data can be recovered after an outage (given the most recent backup copy of the data).

recovery time objective (RTO) The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.

work recovery time (WRT) The amount of effort (expressed as elapsed time) necessary to make the business function operational after the technology element is recovered (as identified with RTO). Tasks include testing and validation of the system.

The next phase in developing the contingency planning process, after developing the CP policy, is the **business impact analysis** (**BIA**). The BIA, a preparatory activity common to both CP and risk management, helps determine which business functions and information systems are the most critical to the success of the organization.

A fundamental difference between a BIA and the risk management processes discussed in Chapter 5 is that risk management focuses on identifying the threats, vulnerabilities, and attacks to determine which controls can protect the information. The BIA assumes that these controls have been bypassed, have failed, or have otherwise proved ineffective; that the attack succeeded; and that the adversity being defended against has come to fruition. By assuming the worst has happened and then assessing how that adversity will affect the

organization, planners gain insight into how to respond to the adverse event, minimize the damage, recover from the effects, and return to normal operations. The BIA attempts to answer the question, "How will it affect us?"

When undertaking the BIA, the organization should consider the following:

1. Scope: The parts of the organization to be included in the BIA should be carefully considered to determine which business units to cover, which systems to include, and the nature of the risk being evaluated.
2. Plan: The needed data will likely be voluminous and complex, so work from a careful plan to ensure that the proper data is collected to enable a comprehensive analysis. Getting the correct information to address the needs of decision makers is important.
3. Balance: Some information may be objective in nature and other information may be available only as subjective or anecdotal references. Facts should be weighted properly against opinions; however, sometimes the knowledge and experience of key personnel can be invaluable.
4. Know the objective: Identify in advance what the key decision makers require for making choices. Structure the BIA so the information they need facilitates consideration of those choices.
5. Follow-up: Communicate periodically to ensure that process owners and decision makers will support the process and the end result of the BIA.[29]

According to NIST's SP 800-34, Rev. 1, the CPMT conducts the BIA in three stages, as described in the sections that follow:[30]

1. Determine mission/business processes and recovery criticality.
2. Identify resource requirements.
3. Identify recovery priorities for system resources.

Determine Mission/Business Processes and Recovery Criticality The first major BIA task is the analysis and prioritization of business processes within the organization, based on their relationship to the organization's mission. Each business department, unit, or division must be independently evaluated to determine how important its functions are to the organization as a whole. For example, recovery operations would probably focus on the IT Department and network operation before turning to the Personnel Department's hiring activities. Likewise, recovering a manufacturing company's assembly line is more urgent than recovering its maintenance tracking system. Personnel functions and assembly line maintenance are important, but unless the organization's main revenue-producing operations can be restored quickly, other functions are irrelevant.

It is important to collect critical information about each business unit before prioritizing the business units. Remember to avoid "turf wars" and instead focus on selecting business functions that must be sustained to continue business operations. While some managers or executives might feel that their function is the most critical to the organization, it might prove to be less critical in the event of a major incident or disaster. Senior management

must arbitrate these inevitable conflicts about priority because it has the perspective to make such trade-off decisions.

When organizations consider recovery criticality, key recovery measures are usually described in terms of how much of the asset they must recover within a specified time frame. The terms most commonly used to describe these values are:

- **Maximum tolerable downtime (MTD)**
- **Recovery time objective (RTO)**
- **Recovery point objective (RPO)**
- **Work recovery time (WRT)**

Planners should determine the optimal point for recovering the information system to meet BIA-mandated recovery needs while balancing the cost of system inoperability against the cost of resources required for restoring systems. This work must be done in the context of critical business processes identified by the BIA, and can be shown with a simple chart (see Figure 4-15).

The longer system availability is interrupted, the more impact it will have on the organization and its operations. Costs will increase as well. When plans require a short RTO, the required solutions are usually more expensive to design and use. For example, if a system must be recovered immediately, it will have an RTO of 0. These types of solutions will require fully redundant alternative processing sites and will therefore have much higher costs. On the other hand, a longer RTO would allow a less expensive recovery system.[31]

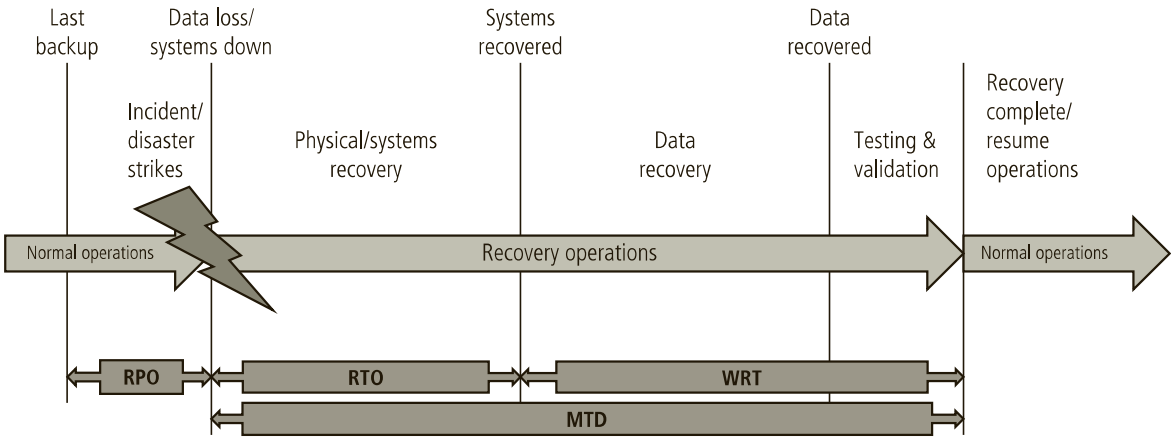


Figure 4-15 RPO, RTO, WRT, and MTD

Source: http://networksandservers.blogspot.com/2011/02/high-availability-terminology-ii.html.

Identify Resource Requirements Once the organization has created a prioritized list of its mission and business processes, it needs to determine which resources would be required to recover those processes and associated assets. Some processes are resource intensive, like IT functions. Supporting customer data, production data, and other organizational

information requires extensive quantities of information processing, storage, and transmission (through networking). Other business production processes require complex or expensive components to operate. For each process and information asset identified in the previous BIA stage, the organization should identify and describe the relevant resources needed to provide or support that process.

Identify Recovery Priorities for System Resources As the CPMT conducts the BIA, it will assess priorities and relative values for mission/business processes. To do so, it needs to understand the information assets used by those processes. The presence of high-value information assets may influence the valuation of a particular business process. Normally, this task would be performed as part of the risk assessment function within the risk management process. The organization should identify, classify, and prioritize its information assets, placing classification labels on each collection or repository of information to better understand its value and prioritize its protection. If the organization has not performed this task, the BIA process is the appropriate time to do so.

Incident Response Planning

Incident response planning includes the identification and classification of an incident and the response to it. The IR plan is made up of activities that must be performed when an incident has been identified. Before developing such a plan, you should understand the philosophical approach to incident response planning.

If an action that threatens information occurs and is completed, it is classified as an incident. All of the threats identified in earlier chapters could result in attacks that would be classified as information security incidents. For purposes of this discussion, however, adverse events are classified as incidents if they have the following characteristics:

- They are directed against information assets.
- They have a realistic chance of success.
- They could threaten the confidentiality, integrity, or availability of information resources.

Incident response planning focuses on detecting and correcting the impact of an incident on information assets. Prevention is purposefully omitted, as this activity is more a function of general information security than of incident response. In other words, IR is more reactive than proactive, with the exception of the planning that must occur to prepare Computer Security Incident Response Teams (CSIRTs) to react to an incident. While the IR planning team develops the plans to respond to an incident, the CSIRT carries them out, reacting to real-world incidents on a day-to-day basis.

IR consists of the following four phases:

1. Planning
2. Detection
3. Reaction
4. Recovery

Incident Response Policy An important early step for the IR team is to develop an IR policy. NIST's Special Publication 800-61, Rev. 2, *The Computer Security Incident Handling Guide*, identifies the following key components of a typical IR policy:

1. *Statement of management commitment*
2. *Purpose and objectives of the policy*
3. *Scope of the policy (to whom and what it applies and under what circumstances)*
4. *Definition of InfoSec incidents and related terms*
5. *Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, and the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process*
6. *Prioritization or severity ratings of incidents*
7. *Performance measures (discussed in Chapter 6)*
8. *Reporting and contact forms*[32]

Like all policies, IR policy must have the full support of top management and be clearly understood by all affected parties. It is especially important to gain the support of communities of interest that must alter business practices or make changes to their IT infrastructures. For example, if the IR team determines that the only way to stop a massive denial-of-service attack is to sever the organization's connection to the Internet, it should have a signed document locked in an appropriate filing cabinet to authorize such action. This document ensures that the IR team is performing authorized actions, and it protects IR team members and the organization from misunderstanding and potential liability.

Incident Planning Planning for an incident requires a detailed understanding of the scenarios developed for the BIA. With this information in hand, the IR planning team can develop a series of predefined responses that guide the organization's CSIRT and information security staff. These responses enable the organization to react quickly and effectively to the detected incident. This discussion assumes that the organization has a CSIRT and that the organization can detect the incident.

The CSIRT consists of people who must be present to handle systems and functional areas that can minimize the impact of an incident as it takes place. Picture a military movie in which U.S. forces have been attacked. If the movie is accurate in its portrayal of CSIRTs, you saw the military version of a CSIRT verifying the threat, determining the appropriate response, and coordinating the actions necessary to deal with the situation.

Incident Response Plan The idea of military team responses can be used to guide incident response planners. The planners should develop a set of documents that direct the actions of each person who must help the organization react to and recover from the incident. These plans must be properly organized and stored to be available when and where they are needed, and in a useful format.

Format and Content The IR plan must be organized to support quick and easy access to required information. The simplest measure is to create a directory of incidents with tabbed sections for each incident. To respond to an incident, the responder simply opens the binder, flips to the appropriate section, and follows the clearly outlined procedures for an assigned role. This means that planners must develop the detailed procedures necessary to respond to each incident. These procedures must include the actions to take *during* the incident and *afterward* as well. In addition, the document should prepare the staff for the incident by providing procedures to perform *before* it occurs.

Storage Information in the IR plan is sensitive and should be protected. If attackers learn how a company responds to a particular incident, they can improve their chances of success. On the other hand, the organization needs to have this information readily available to those who must respond to the incident. This typically means storing the IR plan within arm's reach of the information assets that must be modified or manipulated during or immediately after the attack. The organization could use physical binders stored adjacent to the administrator's workstation or in a bookcase in the server room. An even more effective solution is an encrypted file stored on an online resource. The bottom line is that the people who respond to the incident should not have to search frantically for the needed information.

Testing An untested plan is not a useful plan. Or, in military vernacular, "Train as you fight, and fight as you train." Even if an organization has an effective IR plan on paper, the procedures may be ineffective unless the plan has been practiced or tested. A plan can be tested in many different ways using one or more testing strategies. Four common testing strategies are presented here.[33]

1. Checklist: Copies of the IR plan are distributed to each person who has a role to play during an actual incident. Each person reviews the plan and identifies any inaccurate components for correction. Although the checklist is not a true test, it is an important step in reviewing the document before it is actually needed.
2. Structured walk-through: In a walk-through, each involved person practices the steps he or she will take during an actual event. Team members can conduct an "on-the-ground" walk-through, in which everyone discusses required actions at each location and juncture, or they can conduct a "talk-through," in which all team members sit around a conference table and discuss how they would act as the incident unfolded.
3. Simulation: Here, each involved person works individually rather than in conference, simulating the performance of each task required to react to and recover from a simulated incident. The simulation stops short of the physical tasks required, such as installing a backup or disconnecting a communications circuit. The major difference between a walk-through and a simulation is the independence of individual performers as they work on their own tasks and assume responsibility for identifying faults in their own procedures.
4. Full interruption: The final, most comprehensive and realistic test is to react to a mock incident as if it were real. In a full interruption test, team members follow every procedure, including interruption of service, restoration of data from backups, and notification of appropriate people, as discussed in subsequent sections. This test is often performed after normal business hours in organizations that cannot afford to disrupt

business functions or simulate disruption. This test is the best practice the team can get, but it is too risky for most businesses.

At a minimum, organizations should conduct periodic walk-throughs or talk-throughs of the IR plan. Because business and information resources change quickly, a failure to update the IR plan can result in inability to react effectively to an incident or possibly cause greater damage than the incident itself. If this plan sounds like a major training effort, note the following sayings from author Richard Marcinko, a former Navy SEAL. These remarks have been paraphrased (and somewhat sanitized) for your edification.[34]

- The more you sweat in training, the less you bleed in combat.
- Training and preparation hurt.
- Lead from the front, not the rear.
- You don't have to like it, just do it.
- Keep it simple.
- Never assume.
- You are paid for your results, not your methods.

Incident Detection

Key Terms

incident candidate See *adverse event*.
incident classification The process of examining an incident candidate and determining whether it constitutes an actual incident.

Members of an organization sometimes notify systems administrators, security administrators, or their managers of an unusual occurrence. This occurrence most often causes a complaint to the help desk from one or more users about a technology service. Complaints are often collected by the help desk, and can include reports such as "the system is acting unusual," "programs are slow," "my computer is acting weird," or "data is not available." Incident detection relies on either a human or automated system (often the help desk staff) to identify an unusual occurrence and classify it properly. The mechanisms that might detect an incident include intrusion detection and prevention systems (both host-based and network-based), virus detection software, systems administrators, and even end users. Intrusion detection systems and virus detection software are examined in detail in later chapters. This chapter focuses on the human element.

Note that an incident, as previously defined, is any *clearly identified* attack on the organization's information assets. An ambiguously identified event could be an actual attack, a problem with heavy network traffic, or even a computer malfunction. Only by carefully training users, the help desk, and all security personnel to analyze and identify attacks can the organization hope to identify and classify an incident quickly. Once an attack is properly identified through **incident classification**, the organization can effectively execute the corresponding procedures from the IR plan. Anyone with the appropriate level of

knowledge can classify an incident. Typically, a help desk operator brings the issue to a help desk supervisor, the security manager, or a designated incident watch manager. Once an adverse event (also known as an **incident candidate**) has been classified as an actual incident, the responsible manager must decide whether to implement the incident response plan.

Incident Indicators Several occurrences signal the presence of an incident candidate. Unfortunately, many of them are similar to the actions of an overloaded network, computer, or server, and some are similar to the normal operation of these information assets.

Other incident candidates resemble a misbehaving computing system, software package, or other less serious threat. Donald Pipkin, an IT security expert, identifies three categories of incident indicators: possible, probable, and definite.[35] The indicators identified by Pipkin are not exhaustive; each organization adds indicators based on its own context and experience.

The following four types of events are possible incident indicators:

1. Presence of unfamiliar files: If users discover new files in their home directories or on their office computers, or administrators find files that do not seem to have been placed in a logical location or were not created by an authorized user, an incident may have occurred.
2. Presence or execution of unknown programs or processes: If users or administrators detect unfamiliar programs running or processes executing on office machines or network servers, an incident may have occurred.
3. Unusual consumption of computing resources: Many computer operating systems can monitor the consumption of resources. Windows 2000 and XP, as well as many UNIX variants, allow users and administrators to monitor CPU and memory consumption. Most computers can monitor available hard drive space. Servers maintain logs of file creation and storage. The sudden consumption of resources can indicate a candidate incident.
4. Unusual system crashes: Some computer systems crash on a regular basis. Older operating systems running newer programs are notorious for locking up or rebooting when the OS is unable to execute a requested process or service. Many people are familiar with system error messages such as *Unrecoverable Application Error* and *General Protection Fault*, and many unfortunate users have seen the infamous NT Blue Screen of Death. However, if a computer system seems to be crashing, hanging, rebooting, or freezing more than usual, it could be a candidate incident.

The following four types of events are probable indicators of incidents:

1. Activities at unexpected times: If traffic levels on the organization's network exceed the measured baseline values, an incident is probably under way. If this surge in activity occurs when few members of the organization are at work, an incident is even more likely to be occurring. Similarly, if systems are accessing drives when the operator is not using them, an incident may be in progress.
2. Presence of new accounts: Periodic review can reveal an account (or accounts) that the administrator does not remember creating, or accounts that are not logged in the administrator's journal. Even one unlogged new account is a candidate incident. An

unlogged new account with root or other special privileges has an even higher probability of being an actual incident.

3. Reported attacks: If users of the system report a suspected attack, there is a high probability that an incident is under way or has already occurred. When considering the probability of an attack, you should consider the technical sophistication of the person making the report.
4. Notification from IDPS: If the organization has installed host-based or network-based intrusion detection and prevention systems, and they are correctly configured, a notification from the IDPS indicates a strong likelihood that an incident is in progress. The problem with most IDPSs is that they are seldom configured optimally, and even when they are, they tend to issue many false positives or false alarms. The administrator must determine whether the notification is significant or the result of a routine operation by a user or other administrator.

The following five types of events are definite indicators of incidents. Definite indicators are activities that clearly signal an incident is in progress or has occurred:

1. Use of dormant accounts: Many network servers maintain default accounts that came with the system from the manufacturer. Although industry best practices dictate that these accounts should be changed or removed, some organizations ignore these practices by making the default accounts inactive. In addition, systems may have any number of accounts that are not actively used, such as those for previous employees, employees on extended vacation or sabbatical, or dummy accounts set up to support system testing. If any of these dormant accounts suddenly becomes active without a change in user status, an incident has almost certainly occurred.
2. Changes to logs: The smart administrator backs up systems logs as well as systems data. As part of a routine incident scan, these logs may be compared to an online version to determine whether they have been modified. If logs have been modified and the systems administrator cannot determine explicitly that an authorized person modified them, an incident has occurred.
3. Presence of hacker tools: Hacker tools can be installed or stored on office computers so internal computers and networks can be scanned periodically to determine what a hacker can see. These tools are also used to support research into attack profiles. When a computer contains such tools, its antivirus program detects them as threats to the system every time the computer is booted. If users did not know they had installed the tools, their presence would constitute an incident. Many organizations have policies that explicitly prohibit the installation of such tools without the written permission of the CISO. Installing these tools without proper authorization is a policy violation and should result in disciplinary action. Most organizations that have sponsored and approved penetration-testing operations require all related tools in this category to be confined to specific systems that are not used on the general network unless active penetration testing is under way.
4. Notifications by partner or peer: Many organizations have business partners, upstream and downstream value-chain associations, and superior or subordinate organizations. If one of these organizations indicates that it is being attacked and that the attackers are using your computing systems, an incident has probably occurred or is likely in progress.

5. Notification by hacker: Some hackers enjoy taunting their victims. If your Web page suddenly begins displaying a "gotcha" from a hacker, an incident has occurred. If you receive an e-mail from a hacker that contains information from your "secured" corporate e-mail account, an incident has occurred. If you receive an extortion request for money in exchange for your customers' credit card files, an incident has occurred. Even if proof of loss is elusive, such claims can have an impact on an organization's reputation.

Several other situations are definite incident indicators:

1. Loss of availability: Information or information systems become unavailable.
2. Loss of integrity: Users report corrupt data files, garbage where data should be, or data that looks wrong.
3. Loss of confidentiality: You are notified of sensitive information leaks or informed that information you thought was protected has been disclosed.
4. Violation of policy: Organizational policies that address information or information security have been violated.
5. Violation of law: The law has been broken, and the organization's information assets are involved.

Incident Reaction

Key Terms

alert message A scripted description of the incident that usually contains just enough information so that each person knows what portion of the IR plan to implement without slowing down the notification process.

alert roster A document that contains contact information for people to be notified in the event of an incident.

hierarchical roster An alert roster in which the first person calls a few other people on the roster, who in turn call others. This method typically uses the organizational chart as a structure.

sequential roster An alert roster in which a single contact person calls each person on the roster.

Incident reaction consists of actions outlined in the IR plan that guide the organization in attempting to stop the incident, mitigate its impact, and provide information for recovery. These actions take place as soon as the incident is over. Several actions must occur quickly, including notification of key personnel and documentation of the incident. These actions should be prioritized and documented in the IR plan for quick use in the heat of the moment.

Notification of Key Personnel As soon as the help desk, a user, or a systems administrator determines that an incident is in progress, the right people must immediately be notified in the right order. Most organizations, including the military, maintain an **alert roster** for just such an emergency. There are two types of alert rosters: sequential and hierarchical. The **hierarchical roster** works faster, with more people calling at the same time, but the message may get distorted as it is passed from person to person. The **sequential roster** is more accurate because the contact person provides each person with the same **alert message**, but it takes longer.

As with any document, the alert roster must be maintained and tested to ensure accuracy. The notification process must be periodically rehearsed to ensure that it is effective and efficient.

Other personnel must also be notified in reaction to an incident, but they may not be part of the scripted alert notification because they are not needed until preliminary information has been collected and analyzed. Management must be notified, of course, but not so early that it causes undue alarm, especially if the incident is minor or turns out to be a false alarm. On the other hand, notification cannot be so late that the media or other external sources learn of the incident before management. Some incidents are disclosed to employees in general as a lesson in security, and some are not, as a measure of security. If the incident spreads beyond the target organization's information resources, or if the incident is part of a large-scale assault, it may be necessary to notify other organizations. An example of a large-scale assault is Mafiaboy's DDoS attack on multiple Web-based vendors in 1999. In such cases, the IR planning team must determine who to notify and when to offer guidance about additional notification steps.

Documenting an Incident As soon as an incident or disaster has been declared, key personnel must be notified and documentation of the unfolding event must begin. There are many reasons to document the event. First, it enables an organization to learn what happened, how it happened, and what actions were taken. The documentation records the *who*, *what*, *when*, *where*, *why*, and *how* of the event. Therefore, it can serve as a case study that the organization can use to determine if the right actions were taken and if they were effective. Second, documenting the event can prove that the organization did everything possible to prevent the spread of the incident if the response is questioned later. From a legal standpoint, the standards of due care protect the organization in cases where an incident affects people inside and outside the organization or other organizations that use the targeted systems. Finally, the documentation of an incident can be used to run a simulation in future training sessions.

Incident Containment Strategies The first priority of incident reaction is to stop the incident or contain its scope or impact. Unfortunately, the most direct means of containment, sometimes known as "cutting the wire," is often not an option for an organization. Incident containment strategies vary depending on the incident and on the amount of damage it causes or may cause. Before an incident can be contained, an organization needs to determine which information and information systems have been affected. This is not the time to conduct a detailed analysis of the affected areas; such analysis is typically performed after the fact in the forensics process. Instead, the organization needs to determine what kind of containment strategy is best and which systems or networks need to be contained. In general, incident containment strategies focus on two tasks: stopping the incident and recovering control of the systems.

The organization can stop the incident and attempt to recover control using several strategies:

- If the incident originates outside the organization, the simplest and most straightforward approach is to sever the affected communication circuits. However, if the organization's lifeblood runs through those circuits, such a drastic measure may not be feasible. If the

incident does not threaten the most critical functional areas, it may be more feasible to monitor the incident and contain it in another way. One approach is to apply filtering rules dynamically to limit certain types of network access. For example, if a threat agent is attacking a network by exploiting a vulnerability in the Simple Network Management Protocol (SNMP), applying a blocking filter for the commonly used IP ports stops the attack without compromising other network services. Depending on the nature of the attack and the organization's technical capabilities, such ad hoc controls can sometimes buy valuable time to devise a more permanent control strategy.

- If the incident involves the use of compromised accounts, those accounts can be disabled.
- If the incident involves bypassing a firewall, the firewall can be reconfigured to block that traffic.
- If the incident involves using a particular service or process, it can be disabled temporarily.
- If the incident involves using the organization's e-mail system to propagate itself, the application or server that supports e-mail can be taken down.

The ultimate containment option, which is reserved for only the most drastic scenarios, involves a full stop of all computers and network devices in the organization. Obviously, this step is taken only when all control of the infrastructure has been lost, and the only hope is to preserve the data stored on those computers so it can possibly be used in the future to restore operations.

The bottom line is that containment consists of isolating affected channels, processes, services, or computers; stopping the losses; and regaining control of affected systems. Taking down the entire system, servers, and network may accomplish this objective, but it is typically a measure of last resort. The incident response manager, with the guidance of the IR plan, determines the length of the interruption.

Incident Recovery

Key Terms

after-action review A detailed examination and discussion of the events that occurred, from first detection to final recovery.

computer forensics The process of collecting, analyzing, and preserving computer-related evidence.

evidence A physical object or documented information entered into a legal proceeding that proves an action occurred or identifies the intent of a perpetrator.

incident damage assessment The rapid determination of how seriously a breach of confidentiality, integrity, and availability affected information and information assets during an incident or just following one.

Once the incident has been contained and control of the systems is regained, the next stage of the IR plan is incident recovery. This stage of the plan must be executed immediately. As with incident reaction, the first task is to identify needed human resources and launch them

into action. Almost simultaneously, the organization must assess the full extent of the damage to determine how to restore the system to a fully functional state. Next, the process of computer forensics determines how the incident occurred and what happened. These facts emerge from a reconstruction of the data recorded before and during the incident. Next, the organization repairs vulnerabilities, addresses any shortcomings in its safeguards, and restores systems data and services.

Prioritization of Efforts As the dust settles from the incident, a state of confusion and disbelief may follow. The fallout from stressful workplace activity is well-documented; the common view is that cyberattacks, like conflicts of all kinds, affect everyone involved. To recover from the incident, the organization must keep people focused on the task ahead and make sure that the necessary personnel begin recovery operations according to the IR plan.

Damage Assessment An **incident damage assessment** may take only moments, or it may take days or weeks, depending on the extent of the damage. The damage caused by an incident can range from the minor effects of a curious hacker snooping around to extremely severe—a credit card number theft or the infection of hundreds of computer systems by a worm or virus.

Several sources of information can be used to determine the type, scope, and extent of damage, including system logs, intrusion detection logs, configuration logs and documents, documentation from the incident response, and the results of a detailed assessment of systems and data storage. Using these logs and documentation as a basis for comparison, the IR team can evaluate the current state of the information and systems. A related part of incident damage assessment is the field of **computer forensics**. Computer **evidence** must be carefully collected, documented, and maintained to be usable in formal or informal proceedings. Legally speaking, an item is evidence only once it has been admitted in a legal proceeding. Prior to that time, it is also referred to as an item of potential evidentiary value or evidentiary material (EM). Organizations may conduct informal proceedings when dealing with internal violations of policy or standards of conduct. They may also need to use evidence in formal administrative or legal proceedings. Sometimes the fallout from an incident lands in a courtroom for a civil trial. In each of these circumstances, the people who examine the damage incurred must receive special training so that if an incident becomes part of a crime or civil action, they are adequately prepared to participate.

Recovery Once the extent of the damage has been determined, the recovery process can begin in earnest. Full recovery from an incident requires the following actions:

1. Identify the vulnerabilities that allowed the incident to occur and spread. Resolve them.
2. Address the safeguards that failed to stop or limit the incident, or that were missing from the system in the first place. Install, replace, or upgrade these safeguards.
3. Evaluate monitoring capabilities if they are present. Improve their detection and reporting methods or install new monitoring capabilities.
4. Restore the data from backups. See the following Technical Details features for more information on data storage and management, system backups and recovery, and redundant array of independent disks (RAID). Restoration requires the IR team to understand the organization's backup strategy, restore the data contained in backups, and then recreate the data that was created or modified since the last backup.

5. Restore the services and processes in use. Compromised services and processes must be examined, cleaned, and then restored. If services or processes were interrupted while regaining control of the systems, they need to be brought back online.
6. Continuously monitor the system. If an incident happened once, it can easily happen again. Just because the incident is over doesn't mean the organization is in the clear. Hackers frequently boast of their abilities in chat rooms and dare peers to match their efforts. If word gets out, others may be tempted to try their hands at similar attacks. Therefore, it is important to maintain vigilance during the entire IR process.
7. Restore confidence to the organization's communities of interest. It may be advisable to issue a short memorandum that outlines the incident and assures everyone that it was controlled with as little damage as possible. If the incident was minor, the organization should say so. If the incident was major or severely damaged the systems or data, users should be reassured that they can expect operations to return to normal shortly. The objective is not to placate or lie, but to prevent panic or confusion from causing additional disruptions to the organization's operations.

Before returning to routine duties, the IR team must conduct an **after-action review** or AAR. All key players review their notes and verify that the IR documentation is accurate and precise.

All team members review their actions during the incident and identify areas in which the IR plan worked, didn't work, or should be improved. This approach allows team members to update the IR plan while the needed changes are fresh in their minds. The AAR is documented and can serve as a training case for future staff. The finished AAR completes the actions of the IR team.

Backup Media The following Technical Details feature provides additional insight into backup management and strategies. The most common types of local backup media include digital audio tapes (DAT), quarter-inch cartridge drives (QIC), 8-mm tape, and digital linear tape (DLT). Each type of tape has its restrictions and advantages. Backups can also be performed with CD-ROM and DVD options (CD-R, CD-RW, and DVD-RW), specialized drives (solid state flash drives), or tape arrays.

Online and Cloud Backup Many organizations are abandoning physical, local backup media in favor of online or cloud backups. In fact, as part of some organizations' strategies to have improved performance and resilience as well as to shift operations risk to key suppliers, cloud-based architectures are being adopted. The approaches use network-based computing infrastructure to operate critical business functions. When this happens, much of the responsibility for backup and recovery capability, along with many other aspects of system operations, shifts to the supplier of the services. This means that all aspects of operational capability and security (specifically including backup and recovery) must be accounted for in contracts and audit requirements.

One of the newest forms of data backup is online backup to a third-party data storage vendor. Several backup software and service providers now offer multi-terabyte online data storage anywhere. Even for the home user, companies like Microsoft (OneDrive, at *onedrive.live.com*), Memeo (*www.memeo.com*), Dropbox (*www.dropbox.com*), and Google

(Google Drive, at *http://drive.google.com*) offer options that range from free accounts for minimal amounts of storage to inexpensive multi-gigabyte and terabyte solutions.

For the corporate user, this online storage is sometimes referred to as data storage *in the cloud*. This option is more commonly associated with the leasing of computing resources from a third party, as in cloud computing, but many organizations also lease data storage from cloud vendors. Cloud computing is most commonly described in three offerings:

- Software as a Service (SaaS), in which applications are provided for a fee but hosted on third-party systems and accessed over the Internet and the Web.
- Platform as a Service (PaaS), in which development platforms are available to developers for a fee and are hosted by third parties.
- Infrastructure as a Service (IaaS), which is informally known as Everything as a Service, provides hardware and operating systems resources to host whatever the organization wants to implement. Again, the service is hosted by a third party for a fee.

Organizations can easily lease SaaS online backup services and receive data storage as part of the package. From an ownership perspective, clouds can be public, community, private, or some combination of the three:

- Public clouds: The most common implementation, in which a third party makes services available via the Internet and Web to anyone who needs them.
- Community clouds: A collaboration between a few entities for their sole benefit.
- Private clouds: An extension of an organization's intranet applied to cloud computing; this option technically negates one of the benefits of cloud computing, which is that it requires little or no capital investment. Some larger organizations choose to deploy cloud architectures and implement the services across subordinate organizations.

From a security perspective, the leasing of third-party services is always a challenge. If the organization doesn't own the hardware, software, and infrastructure, it can't guarantee effective security. Therefore, security must be obtained through a warranty; the organization must scrutinize the service agreement and insist on minimal standards of due care.

Automated Response New technologies are emerging in the field of incident response. Some of them build on existing technologies and extend their capabilities and functions. Traditional systems were configured to detect incidents and then notify a human administrator, but new systems can respond to the incident threat autonomously, based on preconfigured options. A more complete discussion of these technologies is presented in Chapter 7.

The disadvantages of current automated response systems may outweigh their benefits. For example, legal issues of tracking suspects with these systems have yet to be resolved. What if the "hacker" turns out to be a compromised system running an automated attack? What are the legal liabilities of a counterattack? How can security administrators condemn a hacker when they may have illegally hacked systems themselves to track the hacker? These issues are complex, but they must be resolved to give security professionals better tools to combat incidents.

TECHNICAL DETAILS

Data Storage and Management

Key Terms

differential backup The duplication of all files that have changed or been added since the last full backup.

full backup The duplication of all files for an entire system, including all applications, operating systems components, and data.

incremental backup The duplication of only the files that have been modified since the previous incremental backup.

To better understand what happens during data restoration in an incident response or disaster recovery, you should understand how system backups are created. Data backup is a complex operation that involves selecting the backup type, establishing backup schedules, and even duplicating data automatically using a redundant array of independent disks (see the next Technical Details feature).

There are three basic types of backups: full, differential, and incremental. The advantage of a **full backup** is that it takes a comprehensive snapshot of the organization's system. The primary disadvantages are that a lot of media are required to store such a large archive and the backup can be time consuming. The **differential backup** updates the backup set only with files that have changed since the last full backup. This method is faster and uses less storage space than the full backup, but each daily differential backup is larger and slower than that of the previous day. For example, if you conduct a full backup on Sunday, then Monday's backup contains all the files that have changed since Sunday, as does Tuesday's backup. By Friday, the file size will have grown substantially. Also, if one backup is corrupt, the previous day's backup contains almost all of the same information.

The third type of backup is the **incremental backup**. It captures files that have changed since the last incremental backup and requires less space and time than the differential method. The downside to incremental backups is that multiple backups would be needed to restore the full system if an incident occurs.

The first component of a backup and recovery system is scheduling and storing the backups. The most common schedule is a daily onsite incremental or differential backup and a weekly off-site full backup. Most backups are conducted overnight, when systems activity is lowest and the probability of user interruption is limited. There are many methods for selecting files to back up and determining where to store various versions of the backups. Organizations will choose methods that best balance security needs against allowing ready accessibility for less severe recovery needs.

(*continues*)

Regardless of the strategy employed, some fundamental principles remain the same. For example, all onsite and off-site storage must be secured. Fireproof safes or filing cabinets are commonly used to store tapes or external drives. Off-site storage in particular requires a safe location, such as a bank's safety deposit box or a professional backup and recovery service. (The trunk of the administrator's car is not secure off-site storage.) Most backup media (tape, hard drives, or optical drives) will likely require a conditioned environment—preferably an airtight, humidity-free, static-free storage container. Each device must be clearly labeled and write-protected. Because tapes frequently wear out, they should be retired periodically and replaced with new media.

TECHNICAL DETAILS

System Backups and Recovery—RAID

Key Terms

disk duplexing An approach to disk mirroring in which each drive has its own controller to provide additional redundancy.

disk mirroring A RAID implementation (typically referred to as RAID Level 1) in which the computer records all data to twin drives simultaneously, providing a backup if the primary drive fails.

disk striping A RAID implementation (typically referred to as RAID Level 0) in which one logical volume is created by storing data across several available hard drives in segments called stripes.

hot swap A hard drive feature that allows individual drives to be replaced without powering down the entire system and without causing a fault during the replacement.

redundant array of independent disks (RAID) A system of drives that stores information across multiple units to spread out data and minimize the impact of a single drive failure. By storing the data redundantly, the loss of a drive will not necessarily cause a loss of data. Also known as RAID.

server fault tolerance A level of redundancy provided by mirroring entire servers to provide redundant capacity for services.

One form of data backup for online usage is the **redundant array of independent disks (RAID)**, originally known as *redundant array of inexpensive disks*. Unlike tape backups, RAID uses several hard drives to store information across multiple units, which spreads out data and minimizes the impact of a single drive failure. There are nine established RAID configurations, many of which are illustrated in Figure 4-16.

RAID Level 0: RAID 0 is not actually a form of redundant storage—it creates one large logical volume and stores the data in segments called stripes across all available hard disk drives in the array. This method is also often called **disk striping** without

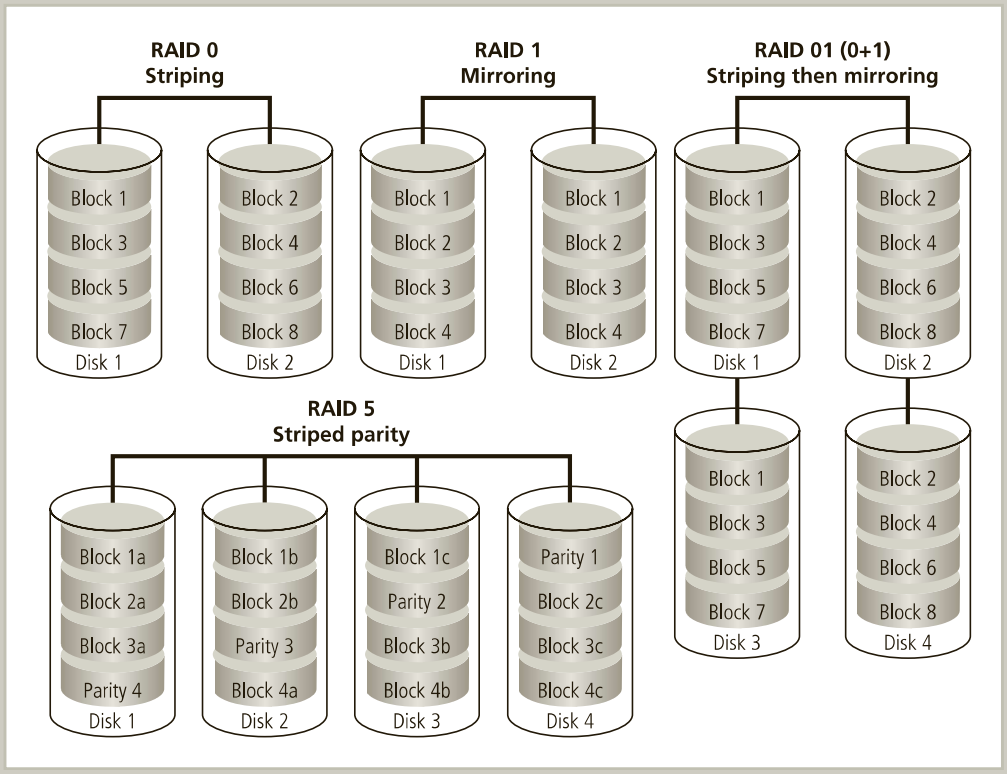


Figure 4-16 Common RAID implementations

parity, and it is frequently used to combine smaller drive volumes into fewer, larger volumes. Unfortunately, failure of one drive may make all data inaccessible. This type of RAID is useful when larger aggregate volume sizes are needed without regard for redundancy or reliability.

RAID Level 1: Commonly called **disk mirroring**, RAID Level 1 uses twin drives in a computer system. The computer records all data to both drives simultaneously, providing a backup if the primary drive fails. However, RAID 1 is a rather expensive and inefficient use of media. A variation of mirroring called **disk duplexing** provides additional redundancy by incorporating separate controllers for each drive. Mirroring is often used to create duplicate copies of operating system volumes for high-availability systems. This type of RAID is useful when a high degree of redundancy and improved access performance are required.

RAID Level 2: This specialized form of disk striping with parity is not widely employed. It uses a specialized parity coding mechanism known as the Hamming Code to store stripes of data on multiple data drives and corresponding redundant error correction on separate error-correcting drives. This approach allows the reconstruction of data if some of the data or redundant parity information is lost. There are no commercial implementations of RAID Level 2.

(*continues*)

RAID Levels 3 and 4: RAID 3 is byte-level striping of data and RAID 4 is block-level striping, in which data is stored in segments on dedicated data drives and parity information is stored on a separate drive. As with RAID 0, one large volume is used for the data, but the parity drive operates independently to provide error recovery.

This level of RAID is used when an organization requires a trade-off between disk capacity usage and reliability of recovery.

RAID Level 5: This form of RAID is most commonly used in organizations that balance safety and redundancy against the costs of acquiring and operating the systems. It is similar to RAID 3 and 4 in that it stripes the data across multiple drives, but there is no dedicated parity drive. Instead, segments of data are interleaved with parity data and are written across all of the drives in the set. RAID 5 drives can also be **hot swapped**, which improves the organization's chances of regaining full capability, compared with a RAID 3 or 4 implementation.

RAID Level 6: RAID 5 with two sets of parity for each parcel of data, which provides an additional level of protection.

RAID Level 7: This is a variation on RAID 5, in which the array works as a single virtual drive. RAID Level 7 is sometimes performed by running special software over RAID 5 hardware.

RAID Level 10: This is a combination of RAID 1 and RAID 0 (0+1: mirroring then striping).

Additional redundancy can be provided by mirroring entire servers called redundant servers or **server fault tolerance.**

› Disaster Recovery Planning

An event can be categorized as a disaster when an organization is unable to mitigate the impact of an incident while it is occurring and the level of damage or destruction is so severe that the organization is unable to recover quickly. The difference between an incident and a disaster may be subtle; the contingency planning team must make the distinction between the two, which may not be possible until an attack occurs. Often an event that is initially classified as an incident is later determined to be a disaster. When this happens, the organization must change its response and secure its most valuable assets to preserve their value for the long term, even at the risk of more short-term disruption.

Disaster recovery (DR) planning is the process of preparing an organization to handle a disaster and recover from it, whether the disaster is natural or man-made. The key emphasis of a DR plan is to reestablish operations at the primary site, the location at which the organization performs its business. The goal of the plan is to make things whole, or as they were before the disaster.

The Disaster Recovery Plan Similar in structure to the IR plan, the DR plan provides detailed guidance in the event of a disaster. It is organized by the type or nature of the disaster, and it specifies recovery procedures during and after each type of disaster. It also provides details about the roles and responsibilities of the people involved in the DR effort, and it identifies the personnel and agencies that must be notified. The DR plan must be tested using the same testing mechanisms as the IR plan. At a minimum, the DR plan must be reviewed periodically during a walk-through or talk-through. As with IR teams, the DR group consists of a planning team and a response team.

Many of the same precepts of incident response apply to disaster recovery:

- Priorities must be clearly established. The first priority is always the preservation of human life. The protection of data and systems immediately falls to the wayside if the disaster threatens the lives, health, or welfare of the organization's employees or community. Only after all employees and neighbors have been safeguarded can the disaster recovery team attend to protecting other assets.
- Roles and responsibilities must be clearly delineated. All members of the DR response team should be aware of their expected actions during a disaster. Some people are responsible for coordinating with local authorities, such as fire, police, and medical staff. Others are responsible for the evacuation of personnel, if required. Still others are tasked simply to pack up and leave.
- Someone must initiate the alert roster and notify key personnel, including the fire, police, or medical authorities mentioned earlier, as well as insurance agencies, disaster teams like the Red Cross, and management teams.
- Someone must be tasked with documenting the disaster. As with an IR reaction, someone must begin recording what happened to serve as a basis for later determining why and how the event occurred.
- If possible, attempts must be made to mitigate the impact of the disaster on the organization's operations. If everyone is safe and all needed authorities have been notified, some employees can be tasked with the evacuation of physical assets. Some can be responsible for making sure all systems are securely shut down to prevent further loss of data.

Recovery Operations Reactions to a disaster can vary so widely that it is impossible to describe the process with any accuracy. Each organization must examine the scenarios developed at the start of contingency planning and determine how to respond.

Should the physical facilities be spared after the disaster, the disaster recovery response team should begin restoring systems and data to reestablish full operational capability. If the organization's facilities do not survive, alternative actions must be taken until new facilities can be acquired. When a disaster threatens the viability of the organization at the primary site, the disaster recovery process transitions into the process of business continuity planning.

› Business Continuity Planning

Business continuity planning prepares an organization to reestablish or relocate critical business operations during a disaster that affects operations at the primary site. If a disaster has rendered the current location unusable, a plan must be in place to allow the business to continue to function. Not every business needs such a plan or such facilities. Small companies or fiscally sound organizations may have the latitude to cease operations until the physical facilities can be restored. Manufacturing and retail organizations may not have this option because they depend on physical commerce and may not be able to relocate operations.

Developing Continuity Programs Once the incident response and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support its continued viability in a disaster. A BC plan is somewhat simpler to develop than an IR plan or DR plan because it consists primarily of selecting a continuity strategy and integrating the off-site data storage and recovery functions into this strategy. Some components of the BC plan, such as an off-site backup service, could already be integral to the

organization's normal operations. Other components require special consideration and negotiation.

The first part of business continuity planning is performed when the joint DR/BC plan is developed. The identification of critical business functions and the resources needed to support them is the cornerstone of the BC plan. When a disaster strikes, these functions are the first to be reestablished at the alternate site. The contingency planning team needs to appoint a group of people to evaluate and compare various alternatives and recommend which strategy should be selected and implemented. The selected strategy usually involves some form of off-site facility, which should be inspected, configured, secured, and tested on a periodic basis. The selection should be reviewed periodically to determine if a superior alternative has emerged or if the organization needs a different solution.

Site and Data Contingency Strategies

Key Terms

cold site A facility that provides only rudimentary services, with no computer hardware or peripherals. Cold sites are used for BC operations.

database shadowing A backup strategy to store duplicate online transaction data along with duplicate databases at the remote site on a redundant server. This server combines electronic vaulting with remote journaling by writing multiple copies of the database simultaneously to two locations.

electronic vaulting A backup method that uses bulk batch transfer of data to an off-site facility; this transfer is usually conducted via leased lines or secure Internet connections.

hot site A fully configured computing facility that includes all services, communications links, and physical plant operations. Hot sites are used for BC operations.

mutual agreement A continuity strategy in which two organizations sign a contract to assist the other in a disaster by providing BC facilities, resources, and services until the organization in need can recover from the disaster.

remote journaling The backup of data to an off-site facility in close to real time based on transactions as they occur.

service bureau A continuity strategy in which an organization contracts with a service agency to provide a BC facility for a fee.

time-share A continuity strategy in which an organization co-leases facilities with a business partner or sister organization. A time-share allows the organization to have a BC option while reducing its overall costs.

warm site A facility that provides many of the same services and options as a hot site, but typically without installed and configured software applications. Warm sites are used for BC operations.

An organization can choose from several strategies when planning for business continuity. The determining factor when selecting a strategy is usually cost. In general, organizations have three exclusive options: hot sites, warm sites, and cold sites. Options are also available for three shared functions: time-shares, service bureaus, and mutual agreements.

Hot Sites A **hot site** is a fully configured computer facility with all services, communications links, and physical plant operations, including heating and air conditioning. Hot sites duplicate computing resources, peripherals, phone systems, applications, and workstations. A hot

site is the pinnacle of contingency planning; it is a duplicate facility that needs only the latest data backups and personnel to become a fully operational twin of the original. A hot site can be operational in a matter of minutes, and in some cases it may be built to provide a process that is seamless to system users by picking up the processing load from a failing site. (This process is sometimes called a seamless fail-over.) The hot site is therefore the most expensive alternative available. Other disadvantages include the need to provide maintenance for all systems and equipment in the hot site, as well as physical and information security. However, if the organization needs a 24/7 capability for near real-time recovery, a hot site is the best option.

Warm Sites The next step down from the hot site is the warm site. A **warm site** provides many of the same services and options as the hot site. However, it typically does not include the actual applications the company needs, or the applications may not yet be installed and configured. A warm site frequently includes computing equipment and peripherals with servers, but not client workstations. A warm site has many of the advantages of a hot site, but at a lower cost. The downside is that a warm site requires hours, if not days, to become fully functional.

Cold Sites The final dedicated site option is the cold site. A **cold site** provides only rudimentary services and facilities. No computer hardware or peripherals are provided. All communications services must be installed after the site is occupied. Basically, a cold site is an empty room with heating, air conditioning, and electricity. Everything else is an option. Although the obvious disadvantages may preclude its selection, a cold site is better than nothing. The main advantage of cold sites over hot and warm sites is the cost. If the warm or hot site is a shared arrangement, not having to contend with other organizations and their equipment after a widespread disaster may make the cold site a better option, albeit slower. In spite of these advantages, some organizations feel it would be easier to lease a new space on short notice than pay maintenance fees on a cold site.

Time-shares A **time-share** allows the organization to maintain a disaster recovery and business continuity option by sharing the cost of a hot, warm, or cold site with one or more partners. The time-share has the same advantages as the type of site selected (hot, warm, or cold). The primary disadvantage is the possibility that more than one organization involved in the time-share may need the facility simultaneously. Other disadvantages include the need to stock the facility with equipment and data from all organizations involved, the negotiations for arranging the time-share, and additional agreements if one or more parties decide to cancel the agreement or sublease its options. A time-share is like agreeing to co-lease an apartment with a group of friends. The participating organizations need to remain on amiable terms because they would have physical access to each other's data.

Service Bureaus In case of a disaster, a **service bureau** agrees to provide physical facilities. These types of agencies also frequently provide off-site data storage for a fee. Contracts can be carefully created with service bureaus to specify exactly what the organization needs without having to reserve dedicated facilities. A service agreement usually guarantees space when needed, even if the service bureau has to acquire additional space in the event of a widespread disaster. This option is much like the rental car clause in your car insurance policy. The disadvantage is that the bureau is a service and must be renegotiated periodically. Also, using a service bureau can be quite expensive.

Mutual Agreements **Mutual agreements** stipulate that participating unaffected organizations are obligated to provide necessary facilities, resources, and services until the receiving

organization can recover from the disaster. This type of arrangement is like moving in with relatives or friends: it doesn't take long to outstay your welcome. The problem with this approach is that many organizations balk at the idea of having to fund duplicate services and resources for other parties, even in the short term. The arrangement is ideal if you need the assistance, but not if you are the host. Still, mutual agreements between divisions of the same parent company, between subordinate and superior organizations, or between business partners can be a cost-effective solution.

Other Options Specialized alternatives are available, such as a rolling mobile site configured in the payload area of a tractor or trailer, or externally stored resources. These resources can consist of a rental storage area that contains duplicate or second-generation equipment to be extracted in an emergency. An organization can also contract with a prefabricated building company for immediate, temporary facilities (mobile offices) that can be placed onsite in the event of a disaster.

One of the newest options available as a specialized alternative is called Disaster Recovery as a Service (DRaaS). DRaaS involves the use of cloud-based computing services as part of a service agreement with a third party. With DRaaS, the organization only needs to access its data (which should have been backed up regularly off-site) in order to regain operations, while employees could literally begin work from anywhere, almost negating the need for expensive, temporary physical offices in organizations with little or no manufacturing functions. These alternatives should be considered when evaluating strategy options.

Off-site Disaster Data Storage To get continuity sites up and running quickly, the organization must be able to move data into the new site's systems. Besides the traditional backup methods mentioned earlier, several more options are available, and some can be used for purposes other than restoring continuity:

- **Electronic vaulting** transfers data off-site in batches, usually through leased lines or services provided for a fee. The receiving server archives the data until the next electronic vaulting process is received. Some disaster recovery companies specialize in electronic vaulting services.
- **Remote journaling** differs from electronic vaulting in that only transactions are transferred, not archived data; also, the transfer is in real time. Electronic vaulting is much like a traditional backup, with a dump of data to the off-site storage, but remote journaling involves activities at a systems level, much like server fault tolerance, with data written to two locations simultaneously.
- An improvement to the process of remote journaling, **database shadowing** combines the server fault tolerance mentioned earlier with remote journaling, writing three or more copies of the database simultaneously to backup systems locally and at one or more remote locations.

› Crisis Management

Key Term

crisis management An organization's set of planning and preparation efforts for dealing with potential human injury, emotional trauma, or loss of life as a result of a disaster.

Disasters, of course, are larger in scale and less manageable than incidents, but the planning processes for both are the same and in many cases are conducted simultaneously. What may truly distinguish an incident from a disaster are the actions of the response teams. An incident response team typically rushes to duty stations or to the office from home. The first act is to reach for the IR plan. A disaster recovery response team may not have the luxury of flipping through a binder to see what must be done. Disaster recovery response personnel must know their roles without any supporting documentation. This knowledge is a function of preparation, training, and rehearsal. You probably remember frequent fire, tornado, or hurricane drills—or even nuclear blast drills—from your school days. Moving from school to the business world doesn't lessen the threat of a fire or other disaster.

The actions taken during and after a disaster are referred to as **crisis management**. Crisis management differs dramatically from incident response, as it focuses first and foremost on the people involved. The disaster recovery team works closely with the crisis management team. According to Gartner Research, the crisis management response team is:

> *responsible for managing the event from an enterprise perspective and covers the following major activities:*
>
> - *Supporting personnel and their loved ones during the crisis*
> - *Determining the event's impact on normal business operations and, if necessary, making a disaster declaration*
> - *Keeping the public informed about the event and the actions being taken to ensure the recovery of personnel and the enterprise*
> - *Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties.*[36]

The crisis management response team should establish a base of operations or command center to support communications until the disaster has ended. The crisis management response team includes people from all functional areas of the organization to facilitate communications and cooperation. Some key areas of crisis management include the following:

- Verifying personnel head count: Everyone must be accounted for, including people on vacations, leaves of absence, and business trips.
- Checking the alert roster: Alert rosters and general personnel phone lists are used to notify people whose assistance may be needed or simply to tell employees not to report to work until the crisis or event is over.
- Checking emergency information cards: It is important that each employee has two types of emergency information cards. The first is personal information that includes next of kin and other contacts in case of an emergency, medical conditions, and a form of identification. The second is a set of instructions for what to do in an emergency. This mini-snapshot of the disaster recovery plan should contain at least a contact number or hotline number; emergency services numbers for fire, police, and medical assistance; evacuation and assembly locations, such as storm shelters; the name and number of the disaster recovery coordinator; and any other needed information.

Crisis management must balance the needs of employees with the needs of the business in providing personnel with support at home during disasters.

The Consolidated Contingency Plan

Using the strategy described earlier and illustrated in Figure 4-14, an organization can build a single document that combines all aspects of the contingency policy and plan, incorporating the IR, DR, and BC plans. In large organizations, such a document may be massive; because it would be unwieldy in physical form, it is often created and stored electronically in a safe and secure off-site location. The document should be online and easily accessible via the Internet by appropriate employees in time of need. The document may be stored in an encrypted file and within a password-protected repository.

Small and medium-sized organizations can use the same approach, but they may also store hard copies of the document both within and outside the organization, at the residences of people who may need them.

All contingency planners live by the following words: *plan for the worst and hope for the best*.

Law Enforcement Involvement

Sometimes, an attack, breach of policy, or other incident constitutes a violation of law. Perhaps the incident was originally considered an accident, but turns out to have been an attempt at corporate espionage, sabotage, or theft. When an organization considers involving law enforcement in an incident, several questions must be answered. When should the organization get law enforcement involved? What level of law enforcement agency should be involved—local, state, or federal? What happens when a law enforcement agency is involved? Some of these questions are best answered by the organization's legal department, but organizations should be prepared to address them in the absence of legal staff. These incidents often occur under circumstances that do not allow for leisurely decision making. Some agencies that may be involved were discussed in detail in Chapter 3.

Benefits and Drawbacks of Law Enforcement Involvement The involvement of law enforcement agencies has advantages and disadvantages. The agencies may be much more capable of processing evidence than an organization. In fact, unless the organization's security forces have been trained in processing evidence and computer forensics, they may do more harm than good when extracting the necessary information to legally convict a suspected criminal. Law enforcement agencies can issue the warrants and subpoenas necessary to document a case, and are adept at obtaining statements from witnesses, affidavits, and other required documents. Law enforcement personnel can be a security administrator's greatest ally in the war on computer crime. Therefore, organizations should get to know the local and state officials charged with enforcing information security laws before having to make a call to report a suspected crime.

Once a law enforcement agency takes over a case, however, the organization cannot entirely control the chain of events, the collection of information and evidence, and the prosecution of suspects. A suspect who might face censure and dismissal by an organization may also face criminal charges and all the attendant publicity. The organization may not be informed about the case's progress for weeks or even months. Equipment that is vital to the organization's business may be tagged as evidence and then removed, stored, and preserved until it is no longer needed for the criminal case. In fact, the equipment may never be returned.

If an organization detects a criminal act, it is legally obligated to involve appropriate law enforcement officials. Failure to do so can subject the organization and its officers to prosecution as accessories to the crimes or as impediments to an investigation. The security administrator must ask law enforcement officials when their agencies need to become involved and which crimes need to be addressed by each agency.

Selected Readings

Many excellent sources of additional information are available in the area of information security. The following can add to your understanding of this chapter's content:

- Information Security Governance: Guidance for Boards of Directors and Executive Management, available by searching at *www.isaca.org*.
- Information Security Governance: A Call to Action, available from *www.cccure.org /Documents/Governance/InfoSecGov4_04.pdf*.
- *Information Security Policies Made Easy*, Version 12, by Charles Cresson Wood and Dave Lineman. 2012. Information Shield.
- *Management of Information Security*, by Michael E. Whitman and Herbert J. Mattord. 2016. Cengage Learning.
- *Principles of Incident Response and Disaster Recovery*, by Michael E. Whitman, Herbert J. Mattord, and Andrew Green. 2013. Cengage Learning.

Chapter Summary

- Information security governance is the application of the principles of corporate governance to the information security function. These principles include executive management's responsibility to provide strategic direction, ensure the accomplishment of objectives, oversee that risks are appropriately managed, and validate responsible resource use.
- Management must use policies as the basis for all information security planning, design, and deployment. Policies direct how issues should be addressed and technologies should be used.
- Standards are more detailed than policies and describe the steps that must be taken to conform to policies.
- Management must define three types of security policies: general or security program policies, issue-specific security policies, and systems-specific security policies.
- The enterprise information security policy (EISP) should be a driving force in the planning and governance activities of the organization as a whole.
- Several published information security frameworks by government organizations, private organizations, and professional societies supply information on best practices for their members.
- One of the foundations of security architectures is the layered implementation of security. This layered approach is referred to as defense in depth.

- Information security policy is best disseminated in a comprehensive security education, training, and awareness (SETA) program. A security awareness program is one of the least frequently implemented but most beneficial programs in an organization. A security awareness program is designed to keep information security at the forefront of users' minds.
- Contingency planning (CP) comprises a set of plans designed to ensure effective reactions to an attack and recovery from it. These plans also help restore an organization to normal modes of business operations.
- Organizations must develop disaster recovery plans, incident response plans, and business continuity plans using a business impact analysis (BIA). This process consists of five stages: identification and prioritization of the threat attack, business unit analysis and prioritization, attack success scenario development, potential damage assessment, and subordinate plan classification.
- Incident response planning consists of four phases: incident planning, incident detection, incident reaction, and incident recovery.
- Disaster recovery planning outlines the response to a disaster and recovery from it, whether the disaster is natural or man-made.
- Business continuity planning includes the steps organizations take so they can function when business cannot be resumed at the primary site.
- Crisis management refers to the actions an organization takes during and immediately after a disaster. Crisis management focuses first and foremost on the people involved.
- It is important to understand when and if to involve law enforcement in a corporate incident. Getting to know local and state law enforcement can assist organizations in these decisions.

Review Questions

1. How can a security framework assist in the design and implementation of a security infrastructure? What is information security governance? Who in the organization should plan for it?
2. Where can a security administrator find information on established security frameworks?
3. What is the ISO 27000 series of standards? Which individual standards make up the series?
4. What are the issues associated with adopting a formal framework or model?
5. What documents are available from the NIST Computer Security Resource Center, and how can they support the development of a security framework?
6. What benefit can a private, for-profit agency derive from best practices designed for federal agencies?
7. What Web resources can aid an organization in developing best practices as part of a security framework?
8. Briefly describe management, operational, and technical controls, and explain when each would be applied as part of a security framework.

9. What are the differences between a policy, a standard, and a practice? What are the three types of security policies? Where would each be used? What type of policy would be needed to guide use of the Web? E-mail? Office equipment for personal use?
10. Who is ultimately responsible for managing a technology? Who is responsible for enforcing policy that affects the use of a technology?
11. What is contingency planning? How is it different from routine management planning? What are the components of contingency planning?
12. When is the IR plan used?
13. When is the DR plan used?
14. When is the BC plan used? How do you determine when to use the IR, DR, and BC plans?
15. What are the elements of a business impact analysis?
16. What are Pipkin's three categories of incident indicators?
17. What is containment, and why is it part of the planning process?
18. When should law enforcement be involved in an IR or DR action? What are the issues associated with law enforcement involvement?
19. What is an after-action review? When is it performed? Why is it done?
20. List and describe the six site and data contingency strategies identified in the text.

Exercises

1. Using a graphics program, design several security awareness posters on the following themes: updating antivirus signatures, protecting sensitive information, watching out for e-mail viruses, prohibiting the personal use of company equipment, changing and protecting passwords, avoiding social engineering, and protecting software copyrights. What other themes can you imagine?
2. Search the Web for security education and training programs in your area. Keep a list and see which category has the most examples. See if you can determine the costs associated with each example. Which do you think would be more cost-effective in terms of both time and money?
3. Search the Web for examples of issue-specific security policies. What types of policies can you find? Using the format provided in this chapter, draft a simple issue-specific policy that outlines fair and responsible use of computers at your college, based on the rules and regulations of your institution. Does your school have a similar policy? Does it contain all the elements listed in the text?
4. Use your library or the Web to find a reported natural disaster that occurred at least six months ago. From the news accounts, determine whether local or national officials had prepared disaster plans and if the plans were used. See if you can determine how the plans helped officials improve disaster response. How do the plans help the recovery?

5. Classify each of the following occurrences as an incident or disaster. If an occurrence is a disaster, determine whether business continuity plans would be called into play.
   a. A hacker breaks into the company network and deletes files from a server.
   b. A fire breaks out in the storeroom and sets off sprinklers on that floor. Some computers are damaged, but the fire is contained.
   c. A tornado hits a local power station, and the company will be without power for three to five days.
   d. Employees go on strike, and the company could be without critical workers for weeks.
   e. A disgruntled employee takes a critical server home, sneaking it out after hours.

For each of the scenarios (a–e), describe the steps necessary to restore operations. Indicate whether law enforcement would be involved.

Case Exercises

Charlie sat at his desk the morning after his nightmare. He had answered the most pressing e-mails in his inbox and had a piping hot cup of coffee at his elbow. He looked down at a blank legal pad, ready to make notes about what to do in case his nightmare became reality.

Discussion Questions

1. What would be the first note you wrote down if you were Charlie?
2. What else should be on Charlie's list?
3. Suppose Charlie encountered resistance to his plans to improve continuity planning. What appeals could he use to sway opinions toward improved business continuity planning?

Ethical Decision Making

The policies that organizations put in place are similar to laws, in that they are directives for how to act properly. Like laws, policies should be impartial and fair, and are often founded on ethical and moral belief systems of the people who create them.

In some cases, especially when organizations expand into foreign countries, they experience a form of culture shock when the laws of their new host country conflict with their internal policies. Suppose that SLS has expanded its operations in France. Setting aside any legal requirements that SLS make its policies conform to French law, does SLS have an ethical imperative to modify its policies to better meet the needs of its stakeholders in the new country?

Suppose SLS has altered its policies for all operations in France and that the changes are much more favorable to employees—such as a requirement to provide child and elder-care services at no cost to the employee. Is SLS under any ethical burden to offer the same benefit to employees in its original country?

Endnotes

1. IT Governance Institute. *Board Briefing on IT Governance*, 2nd Edition. 2003. The Chartered Institute of Management Accountants (CIMA) and the International Federation of Accountants (IFAC) also adopted this definition in 2004. Accessed 5 July 2016 from *www.isaca.org*.
2. ITGI. "Information Security Governance: Guidance for Information Security Managers." Accessed 11 October 2016 from *www.isaca.org*.
3. Wood, Charles Cresson. "Integrated Approach Includes Information Security." *Security* 37, no. 2 (February 2000): 43–44.
4. "Former Andersen Auditor Admits to Breaking Law." 14 May 2002. Accessed 11 October 2016 from *www.pbs.org/newshour/updates/business-jan-june02-andersen_05-14/*.
5. Beltran, Luisa. "Andersen Exec: Shredding Began after E-mail." 21 January 2002. Accessed 4 July 2016 from *http://money.cnn.com/2002/01/21/companies/enron_odom/*.
6. US-CERT. "Security Recommendations to Prevent Cyber Intrusions." Accessed 4 July 2016 from *www.us-cert.gov/ncas/alerts/TA11-200A*.
7. National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. SP 800-12. Gaithersburg, MD, 1996.
8. Whitman, Michael E., Anthony M. Townsend, and Robert J. Aalberts. "Considerations for an Effective Telecommunications Use Policy." *Communications of the ACM* 42, no. 6 (June 1999): 101–109.
9. Ibid.
10. Derived from a number of sources, the most notable of which was accessed 4 July 2016 from *www.wustl.edu/policies/infosecurity.html*.
11. National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. SP 800-12. Gaithersburg, MD, 1996.
12. NetIQ Security Technologies, Inc. *User Guide, NetIQ*. August 2011. Accessed 4 July 2016 from *https://www.netiq.com/documentation/vigilent-policy-center/pdfdoc/vigilent-policy-center-user-guide/vigilent-policy-center-user-guide.pdf*
13. National Institute of Standards and Technology. *International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management*. November 2002. Accessed 4 July 2016 from *http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq-110502.pdf*.
14. Compiled from a number of sources, including: "ISO/IEC 27002:2013 Information Technology—Security Techniques—Code of Practice for Information Security Controls." Accessed 4 July 2016 from *www.iso27001security.com/html/27002.html*; and "Introduction to ISO 27002." Accessed 4 July 2016 from *www.27000.org/iso-27002.htm*.
15. Adapted from diagram of ISO 27001:2013 implementation process. Accessed 4 July 2016 from *www.iso27001standard.com/en/free-downloads*.
16. National Institute of Standards and Technology. *Information Security Management, Code of Practice for Information Security Management*. ISO/IEC 17799. 6 December 2001. Geneva, Switzerland.

17. About the ISO27k standards. Accessed 4 July 2016 from *www.iso27001security.com /html/iso27000.html*.

18. National Institute of Standards and Technology. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. SP 800-14. September 1996. Gaithersburg, MD.

19. National Institute of Standards and Technology. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Accessed 4 July 2016 at *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37 -rev1-final.pdf*.

20. National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0." 12 February 2014. Accessed 4 July 2016 from *www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf*.

21. Ibid.

22. Ibid.

23. Ibid.

24. National Institute of Standards and Technology. "Roadmap for Improving Critical Infrastructure Cybersecurity." 12 February 2014. Accessed 4 July 2016 from *www .nist.gov/cyberframework/upload/roadmap-021214.pdf*.

25. National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. SP 800-12. Gaithersburg, MD, 1996.

26. Ibid.

27. King, William R., and Gray, Paul. *The Management of Information Systems*. 1989. Chicago: Dryden Press, 359.

28. Swanson, M., Bowen, P., Phillips, A., Gallup, D., and Lynes, D. National Institute of Standards and Technology. *Contingency Planning Guide for Federal Information Systems*. SP 800-34, Rev. 1. Accessed 4 July 2016 at *http://nvlpubs.nist.gov/nistpubs /Legacy/SP/nistspecialpublication800-34r1.pdf*.

29. Zawada, B., and Evans, L. "Creating a More Rigorous BIA." *CPM Group*. November /December 2002. Accessed 12 May 2005 at *www.contingencyplanning.com/archives /2002/novdec/4.aspx*.

30. Swanson, M., Bowen, P., Phillips, A., Gallup, D., and Lynes, D. National Institute of Standards and Technology. *Contingency Planning Guide for Federal Information Systems*. SP 800-34, Rev. 1. Accessed 4 July 2016 at *http://nvlpubs.nist.gov/nistpubs /Legacy/SP/nistspecialpublication800-34r1.pdf*.

31. Ibid.

32. Cichonski, P., Millar, T., Grance, T., and Scarfone, K. National Institute of Standards and Technology. *Computer Security Incident Handling Guide*. SP 800-61, Rev. 2. August 2012. Accessed 11 October 2016 at *http://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-61r2.pdf*.

33. Krutz, Ronald L., and Vines, Russell Dean. *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*. 2001. New York: John Wiley and Sons Inc., 288.

34. Marcinko, Richard, and Weisman, John. *Designation Gold*. 1998. New York: Pocket Books, preface.

35. Pipkin, D. L. *Information Security: Protecting the Global Enterprise*. 2000. Upper Saddle River, NJ: Prentice Hall, 256.

36. Witty, Roberta. "What is Crisis Management?" *Gartner Online*. 19 September 2001. Accessed 11 October 2016 from *www.gartner.com/DisplayDocument?id=340971*.