Chapter 8

SECURITY AND PLANNING IN THE COMPUTER SYSTEM LIFE CYCLE

Like other aspects of information processing systems, security is most effective and efficient if planned and managed throughout a computer system's life cycle, from initial planning, through design, implementation, and operation, to disposal.[65] Many security-relevant events and analyses occur during a system's life. This chapter explains the relationship among them and how they fit together.[66] It also discusses the important role of security planning in helping to ensure that security issues are addressed comprehensively.

This chapter examines:

- system security plans,
- the components of the computer system life cycle,
- the benefits of integrating security into the computer system life cycle, and
- techniques for addressing security in the life cycle.

8.1 Computer Security Act Issues for Federal Systems

Planning is used to help ensure that security is addressed in a comprehensive manner throughout a system's life cycle. For federal systems, the Computer Security Act of 1987 sets forth a statutory requirement for the preparation of computer security plans for all sensitive systems.[67] The intent and spirit of the Act is to improve computer security in the federal government, not to create paperwork. In keeping with this intent, the Office of Management and Budget (OMB) and NIST have guided agencies toward a planning process that emphasizes good planning and management of computer security within an agency and for each computer system. As emphasized in this chapter, computer *security* management should be a part of computer *systems*

---

[65] A computer system refers to a collection of processes, hardware, and software that perform a function. This includes applications, networks, or support systems.

[66] Although this chapter addresses a life cycle process that starts with system initiation, the process can be initiated at any point in the life cycle.

[67] An organization will typically have many computer security plans. However, it is not necessary that a separate and distinct plan exist for every physical system (e.g., PCs). Plans may address, for example, the computing resources within an operational element, a major application, or a group of similar systems (either technologically or functionally).

management. The benefit of having a distinct computer security plan is to ensure that computer security is not overlooked.

The Act required the submission of plans to NIST and the National Security Agency (NSA) for review and comment, a process which has been completed. Current guidance on implementing the Act requires agencies to obtain independent review of computer security plans. This review may be internal or external, as deemed appropriate by the agency.

> "The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. The system security plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system."
>
> - OMB Bulletin 90-08

A "typical" plan briefly describes the important security considerations for the system and provides references to more detailed documents, such as system security plans, contingency plans, training programs, accreditation statements, incident handling plans, or audit results. This enables the plan to be used as a management tool without requiring repetition of existing documents. For smaller systems, the plan may include all security documentation. As with other security documents, if a plan addresses specific vulnerabilities or other information that could compromise the system, it should be kept private. It also has to be kept up-to-date.

8.2 Benefits of Integrating Security in the Computer System Life Cycle

> Different people can provide security input throughout the life cycle of a system, including the accrediting official, data users, systems users, and system technical staff.

Although a computer security plan can be developed for a system at any point in the life cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle. Security, like other aspects of a computer system, is best managed if planned for throughout the computer system life cycle. It has long been a tenet of the computer community that it costs ten times more to add a feature in a system *after* it has been designed than to include the feature in the system at the initial design phase. The principal reason for implementing security during a system's development is that it is more difficult to implement it later (as is usually reflected in the higher costs of doing so). It also tends to disrupt ongoing operations.

Security also needs to be incorporated into the later phases of the computer system life cycle to help ensure that security keeps up with changes in the system's environment, technology, procedures, and personnel. It also ensures that security is considered in system upgrades, including the purchase of new components or the design of new modules. Adding new security controls to a system after a security breach, mishap, or audit can lead to haphazard security that can be more expensive and less effective that security that is already integrated into the system.

It can also significantly degrade system performance. Of course, it is virtually impossible to anticipate the whole array of problems that may arise during a system's lifetime. Therefore, it is generally useful to update the computer security plan at least at the end of each phase in the life cycle and after each re-accreditation. For many systems, it may be useful to update the plan more often.

Life cycle management also helps document security-relevant decisions, in addition to helping assure management that security is fully considered in all phases. This documentation benefits system management officials as well as oversight and independent audit groups. System management personnel use documentation as a self-check and reminder of why decisions were made so that the impact of changes in the environment can be more easily assessed. Oversight and independent audit groups use the documentation in their reviews to verify that system management has done an adequate job and to highlight areas where security may have been overlooked. This includes examining whether the documentation accurately reflects how the system is actually being operated.

Within the federal government, the Computer Security Act of 1987 and its implementing instructions provide specific requirements for computer security plans. These plans are a form of documentation that helps ensure that security is considered not only during system design and development but also throughout the rest of the life cycle. Plans can also be used to be sure that requirements of Appendix III to OMB Circular A-130, as well as other applicable requirements, have been addressed.

8.3 Overview of the Computer System Life Cycle

There are many models for the computer system life cycle but most contain five basic phases, as pictured in Figure 8.1.

- *Initiation*. During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

- *Development/Acquisition*. During this phase the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

- *Implementation*. After initial system testing, the system is installed or fielded.

- *Operation/Maintenance*. During this phase the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events.

- *Disposal*. The computer system is disposed of once the transition to a new computer system is completed.

Many different "life cycles" are associated with computer systems, including the system development, acquisition, and information life cycles.

Each phase can apply to an entire system, a new component or module, or a system upgrade. As with other aspects of systems management, the level of detail and analysis for each activity described here is determined by many factors including size, complexity, system cost, and sensitivity.

Many people find the concept of a computer system life cycle confusing because many cycles occur within the broad framework of the *entire* computer system life cycle. For example, an organization could develop a system, using a system *development* life cycle. During the system's life, the organization might purchase new components, using the *acquisition* life cycle.

Moreover, the computer system life cycle itself is merely one component of other life cycles. For example, consider the *information life cycle*. Normally information, such as personnel data, is used much longer than the life of one computer system. If an employee works for an organization for thirty years and collects retirement for another twenty, the employee's automated personnel record will probably pass through many different organizational computer systems owned by the company. In addition, parts of the information will also be used in other computer systems, such as those of the Internal Revenue Service and the Social Security Administration.

8.4 Security Activities in the Computer System Life Cycle[68]

This section reviews the security activities that arise in each stage of the computer system life cycle. (See Figure 8.1.)

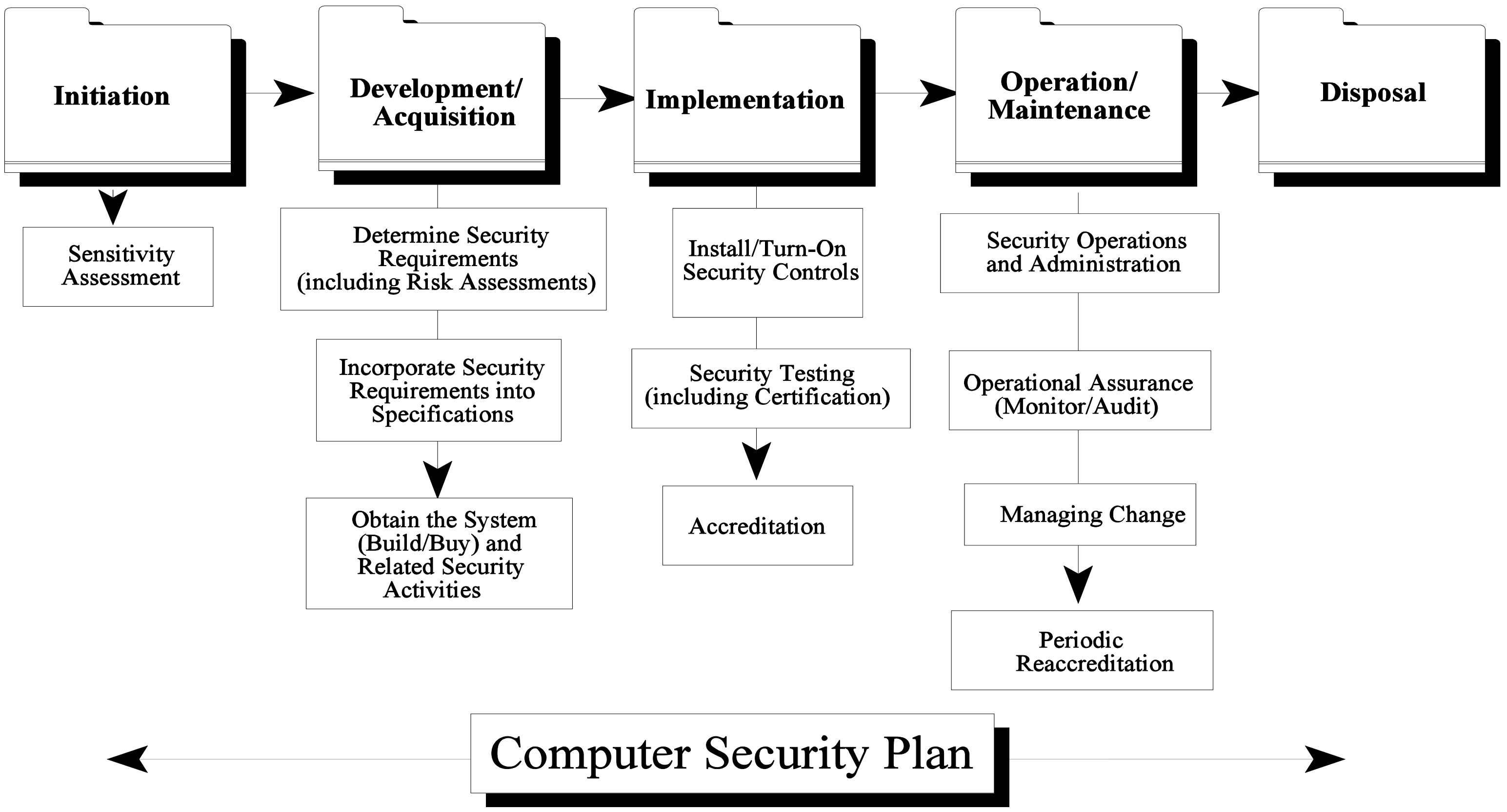
8.4.1 Initiation

The conceptual and early design process of a system involves the discovery of a need for a new system or enhancements to an existing system; early ideas as to system characteristics and proposed functionality; brainstorming sessions on architectural, performance, or functional system aspects; and environmental, financial, political, or other constraints. At the same time, the basic *security* aspects of a system should be developed along with the early system design. This can be done through a *sensitivity assessment.*

---

[68] For brevity and because of the uniqueness of each system, none of these discussions can include the details of all possible security activities at any particular life cycle phase.

Security in the System Life Cycle



The life cycle process described in this chapter consists of five separate phases. Security issues are present in each.

Figure 8.1

8.4.1.1 Conducting a Sensitivity Assessment

The definition of *sensitive* is often misconstrued. *Sensitive* is synonymous with *important* or *valuable*. Some data is sensitive because it must be kept confidential. Much more data, however, is sensitive because its integrity or availability must be assured. The Computer Security Act and OMB Circular A-130 clearly state that information is sensitive if its unauthorized disclosure, modification (i.e., loss of integrity), or unavailability would harm the agency. In general, the more important a system is to the mission of the agency, the more sensitive it is.

A *sensitivity assessment* looks at the sensitivity of both the information to be processed and the system itself. The assessment should consider legal implications, organization policy (including federal and agency policy if a federal system), and the functional needs of the system. Sensitivity is normally expressed in terms of integrity, availability, and confidentiality. Such factors as the importance of the system to the organization's mission and the consequences of unauthorized modification, unauthorized disclosure, or unavailability of the system or data need to be examined when assessing sensitivity. To address these types of issues, the people who use or own the system or information should participate in the assessment.

A sensitivity assessment should answer the following questions:

- What information is handled by the system?
- What kind of potential damage could occur through error, unauthorized disclosure or modification, or unavailability of data or the system?
- What laws or regulations affect security (e.g., the Privacy Act or the Fair Trade Practices Act)?
- To what threats is the system or information particularly vulnerable?
- Are there significant environmental considerations (e.g., hazardous location of system)?
- What are the security-relevant characteristics of the user community (e.g., level of technical sophistication and training or security clearances)?
- What internal security standards, regulations, or guidelines apply to this system?

The sensitivity assessment starts an analysis of security that continues throughout the life cycle. The assessment helps determine if the project needs special security oversight, if further analysis is needed before committing to begin system development (to ensure feasibility at a reasonable cost), or in rare instances, whether the security requirements are so strenuous and costly that system development or acquisition will not be pursued. The sensitivity assessment can be included with the system initiation documentation either as a separate document or as a section of another planning document. The development of security features, procedures, and assurances, described in the next section, builds on the sensitivity assessment.

A sensitivity assessment can also be performed during the planning stages of system upgrades (for either upgrades being procured or developed in house). In this case, the assessment focuses on the affected areas. If the upgrade significantly affects the original assessment, steps can be taken to analyze the impact on the rest of the system. For example, are new controls needed? Will some controls become unnecessary?

8.4.2 Development/Acquisition

For most systems, the development/acquisition phase is more complicated than the initiation phase. Security activities can be divided into three parts:

- determining security features, assurances, and operational practices;
- incorporating these security requirements into design specifications; and
- actually acquiring them.

These divisions apply to systems that are designed and built in house, to systems that are purchased, and to systems developed using a hybrid approach.

During this phase, technical staff and system sponsors should actively work together to ensure that the technical designs reflect the system's security needs. As with development and incorporation of other system requirements, this process requires an open dialogue between technical staff and system sponsors. It is important to address security requirements effectively in synchronization with development of the overall system.

8.4.2.1 Determining Security Requirements

During the first part of the development/ acquisition phase, system planners define the requirements of the system. *Security requirements should be developed at the same time.* These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training). System security requirements, like other system requirements, are derived from a number of sources including law, policy, applicable standards and guidelines, functional needs of the system, and cost-benefit trade-offs.

Law. Besides specific laws that place security requirements on information, such as the Privacy Act of 1974, there are laws, court cases, legal opinions, and other similar legal material that may affect security directly or indirectly.

Policy. As discussed in Chapter 5, management officials issue several different types of policy. System security requirements are often derived from issue-specific policy.

Standards and Guidelines. International, national, and organizational standards and guidelines are another source for determining security features, assurances, and operational practices. Standards and guidelines are often written in an "if...then" manner (e.g., if the system is encrypting data, then a particular cryptographic algorithm should be used). Many organizations specify baseline controls for different types of systems, such as administrative, mission- or business-critical, or proprietary. As required, special care should be given to interoperability standards.

Functional Needs of the System. The purpose of security is to support the function of the system, not to undermine it. Therefore, many aspects of the function of the system will produce related security requirements.

Cost-Benefit Analysis. When considering security, cost-benefit analysis is done through risk assessment, which examines the assets, threats, and vulnerabilities of the system in order to determine the most appropriate, cost-effective safeguards (that comply with applicable laws, policy, standards, and the functional needs of the system). Appropriate safeguards are normally those whose anticipated benefits outweigh their costs. Benefits and costs include monetary and nonmonetary issues, such as prevented losses, maintaining an organization's reputation, decreased user friendliness, or increased system administration.

Risk assessment, like cost-benefit analysis, is used to support decision making. It helps managers select cost-effective safeguards. The extent of the risk assessment, like that of other cost-benefit analyses, should be commensurate with the complexity and cost (normally an indicator of complexity) of the system and the expected benefits *of the assessment.* Risk assessment is further discussed in Chapter 7.

Risk assessment can be performed during the requirements analysis phase of a procurement or the design phase of a system development cycle. Risk should also normally be assessed during the development/acquisition phase of a system upgrade. The risk assessment may be performed once or multiple times, depending upon the project's methodology.

Care should be taken in differentiating between *security* risk assessment and *project* risk analysis. Many system development and acquisition projects analyze the risk of failing to successfully complete the project – a different activity from *security* risk assessment.

8.4.2.2 Incorporating Security Requirements Into Specifications

Determining security features, assurances, and operational practices can yield significant security information and often voluminous requirements. This information needs to be validated, updated, and organized into the detailed security protection requirements and specifications used by systems designers or purchasers. Specifications can take on quite different forms, depending on the methodology used for to develop the system, or whether the system, or parts of the system, are being purchased off the shelf.

As specifications are developed, it may be necessary to update initial risk assessments. A safeguard recommended by the risk assessment could be incompatible with other requirements, or a control may be difficult to implement. For example, a security requirement that prohibits dial-in access could prevent employees from checking their e-mail while away from the office.[69]

> Developing testing specifications early can be critical to being able to cost-effectively test security features.

Besides the technical and operational controls of a system, assurance also should be addressed. The degree to which assurance (that the security features and practices can and do work correctly and effectively) is needed should be determined early. Once the desired level of assurance is determined, it is necessary to figure out how the system will be tested or reviewed to determine whether the specifications have been satisfied (to obtain the desired assurance). This applies to both system developments and acquisitions. For example, if rigorous assurance is needed, the ability to test the system or to provide another form of initial and ongoing assurance needs to be designed into the system or otherwise provided for. See Chapter 9 for more information.

8.4.2.3 Obtaining the System and Related Security Activities

During this phase, the system is actually built or bought. If the system is being built, security activities may include developing the system's security aspects, monitoring the development process itself for security problems, responding to changes, and monitoring threat. Threats or vulnerabilities that may arise during the development phase include Trojan horses, incorrect code, poorly functioning development tools, manipulation of code, and malicious insiders.

If the system is being acquired off the shelf, security activities may include monitoring to ensure security is a part of market surveys, contract solicitation documents, and evaluation of proposed systems. Many systems use a combination of development and acquisition. In this case, security activities include both sets.

---

[69] This is an example of a risk-based decision.

> In federal government contracting, it is often useful if personnel with security expertise participate as members of the source selection board to help evaluate the security aspects of proposals.

As the system is built or bought, choices are made about the system, which can affect security. These choices include selection of specific off-the-shelf products, finalizing an architecture, or selecting a processing site or platform. Additional security analysis will probably be necessary.

In addition to obtaining the system, operational practices need to be developed. These refer to human activities that take place around the system such as contingency planning, awareness and training, and preparing documentation. The chapters in the Operational Controls section of this handbook discuss these areas. These need to be developed along with the system, although they are often developed by different individuals. These areas, like technical specifications, should be considered from the beginning of the development and acquisition phase.

8.4.3 Implementation

A separate implementation phase is not always specified in some life cycle planning efforts. (It is often incorporated into the end of development and acquisition or the beginning of operation and maintenance.) However, from a security point of view, a critical security activity, *accreditation*, occurs between development and the start of system operation. The other activities described in this section, turning on the controls and testing, are often incorporated at the end of the development/acquisition phase.

8.4.3.1 Install/Turn-On Controls

While obvious, this activity is often overlooked. When acquired, a system often comes with security features disabled. These need to be enabled and configured. For many systems this is a complex task requiring significant skills. Custom-developed systems may also require similar work.

8.4.3.2 Security Testing

System security testing includes both the testing of the particular parts of the system that have been developed or acquired and the testing of the entire system. Security management, physical facilities, personnel, procedures, the use of commercial or in-house services (such as networking services), and contingency planning are examples of areas that affect the security of the entire system, but may be specified outside of the development or acquisition cycle. Since only items within the development or acquisition cycle will have been tested during system acceptance testing, separate tests or reviews may need to be performed for these additional security elements.

Security certification is a formal testing of the security safeguards implemented in the computer system to determine whether they meet applicable requirements and specifications.[70] To provide more reliable technical information, certification is often performed by an independent reviewer, rather than by the people who designed the system.

8.4.3.3 Accreditation

System security accreditation is the *formal authorization* by the accrediting (management) official for system operation and an *explicit acceptance of risk*. It is usually supported by a review of the system, including its management, operational, and technical controls. This review may include a detailed technical evaluation (such as a Federal Information Processing Standard 102 certification, particularly for complex, critical, or high-risk systems), security evaluation, risk assessment, audit, or other such review. If the life cycle process is being used to manage a project (such as a system upgrade), it is important to recognize that the accreditation is for the entire system, not just for the new addition.

The best way to view computer security accreditation is as a form of quality control. It forces managers and technical staff to work together to find the best fit for security, given technical constraints, operational constraints, and mission requirements. The accreditation process obliges managers to make critical decisions regarding the adequacy of security safeguards. A decision based on reliable information about the effectiveness of technical and non-technical safeguards and the residual risk is more likely to be a sound decision.

Sample Accreditation Statement

In accordance with (Organization Directive), I hereby issue an accreditation for (name of system). This accreditation is my formal declaration that a satisfactory level of operational security is present and that the system can operate under reasonable risk. This accreditation is valid for three years. The system will be re-evaluated annually to determine if changes have occurred affecting its security.

After deciding on the acceptability of security safeguards and residual risks, the accrediting official should issue a formal accreditation statement. While most flaws in system security are not severe enough to remove an operational system from service or to prevent a new system from becoming operational, the flaws may require some restrictions on operation (e.g., limitations on dial-in access or electronic connections to other organizations). In some cases, an interim accreditation may be granted, allowing the system to operate requiring review at the end of the interim period, presumably after security upgrades have been made.

---

[70] Some federal agencies use a broader definition of the term certification to refer to security reviews or evaluations, formal or information, that take place prior to and are used to support accreditation.

8.4.4 Operation and Maintenance

Many security activities take place during the operational phase of a system's life. In general, these fall into three areas: (1) security operations and administration; (2) operational assurance; and (3) periodic re-analysis of the security. Figure 8.2 diagrams the flow of security activities during the operational phase.

8.4.4.1 Security Operations and Administration

Operation of a system involves many security activities discussed throughout this handbook. Performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software are some examples.

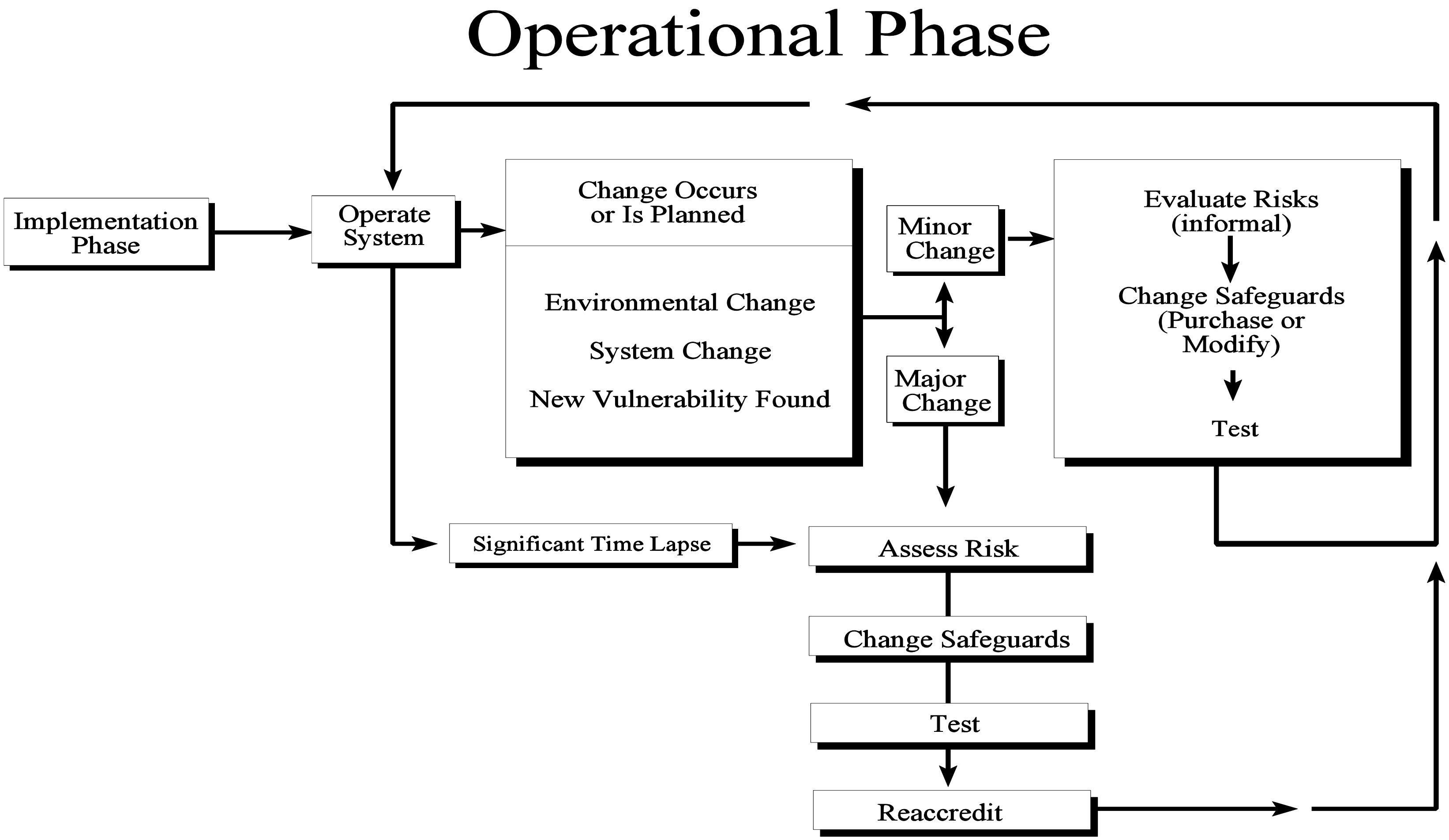
8.4.4.2 Operational Assurance

Operational assurance examines whether a system is operated according to its current security requirements. This includes both the actions of people who operate or use the system and the functioning of technical controls.

Security is *never* perfect when a system is implemented. In addition, system users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Changes in the system or the environment can create new vulnerabilities. Strict adherence to procedures is rare over time, and procedures become outdated. Thinking risk is minimal, users may tend to bypass security measures and procedures.

As shown in Figure 8.2, changes occur. Operational assurance is one way of becoming aware of these changes whether they are new vulnerabilities (or old vulnerabilities that have not been corrected), system changes, or environmental changes. Operational assurance is the process of reviewing an operational system to see that security controls, both automated and manual, are functioning correctly and effectively.

To maintain operational assurance, organizations use two basic methods: *system audits* and *monitoring*. These terms are used loosely within the computer security community and often overlap. A system audit is a one-time or periodic event to evaluate security. Monitoring refers to an ongoing activity that examines either the system or the users. In general, the more "real-time" an activity is, the more it falls into the category of monitoring. (See Chapter 9.)



During the operational phase of a system life cycle, major and minor changes will occur. This figure diagrams appropriate responses to change to help ensure the continued security of the system at a level acceptable to the accrediting official.

Figure 8.2

8.4.4.3 Managing Change

Security change management helps develop new security requirements.

Computer systems and the environments in which they operate change continually. In response to various events such as user complaints, availability of new features and services, or the discovery of new threats and vulnerabilities, system managers and users modify the system and incorporate new features, new procedures, and software updates.

The environment in which the system operates also changes. Networking and interconnections tend to increase. A new user group may be added, possibly external groups or anonymous groups. New threats may emerge, such as increases in network intrusions or the spread of personal computer viruses. If the system has a configuration control board or other structure to manage technical system changes, a security specialist can be assigned to the board to make determinations about whether (and if so, how) changes will affect security.

Security should also be considered during system upgrades (and other planned changes) and in determining the impact of unplanned changes. As shown in Figure 8.2, when a change occurs or is planned, a determination is made whether the change is major or minor. A major change, such as reengineering the structure of the system, significantly affects the system. Major changes often involve the purchase of new hardware, software, or services or the development of new software modules.

An organization does not need to have a specific cutoff for major-minor change decisions. A sliding scale between the two can be implemented by using a combination of the following methods:

- *Major change*. A major change requires analysis to determine security requirements. The process described above can be used, although the analysis may focus only on the area(s) in which the change has occurred or will occur. If the original analysis and system changes have been documented throughout the life cycle, the analysis will normally be much easier. Since these changes result in significant system acquisitions, development work, or changes in policy, the system should be reaccredited to ensure that the residual risk is still acceptable.

- *Minor change*. Many of the changes made to a system do not require the extensive analysis performed for major changes, but do require some analysis. Each change can involve a limited risk assessment that weighs the pros (benefits) and cons (costs) and that can even be performed on-the-fly at meetings. Even if the analysis is conducted informally, decisions should still be appropriately documented. This process recognizes that even "small" decisions should be risk-based.

8.4.4.4 Periodic Reaccreditation

Periodically, it is useful to formally reexamine the security of a system from a wider perspective. The analysis, which leads to reaccreditation, should address such questions as: Is the security still sufficient? Are major changes needed?

The reaccreditation should address high-level security and management concerns as well as the implementation of the security. It is not always necessary to perform a new risk assessment or certification in conjunction with the re-accreditation, but the activities support each other (and both need be performed periodically). The more extensive system changes have been, the more extensive the analyses should be (e.g., a risk assessment or re-certification). A risk assessment is likely to uncover security concerns that result in system changes. After the system has been changed, it may need testing (including certification). Management then reaccredits the system for continued operation if the risk is acceptable.

> It is important to consider legal requirements for records retention when disposing of computer systems. For federal systems, system management officials should consult with their agency office responsible for retaining and archiving federal records.

8.4.5 Disposal

The disposal phase of the computer system life cycle involves the disposition of information, hardware, and software. Information may be moved to another system, archived, discarded, or destroyed. When archiving information, consider the method for retrieving the information in the future. The technology used to create the records may not be readily available in the future.

Hardware and software can be sold, given away, or discarded. There is rarely a need to destroy hardware, except for some storage media containing confidential information that cannot be sanitized without destruction. The disposition of software needs to be in keeping with its license or other agreements with the developer, if applicable. Some

> **Media Sanitization**
>
> Since electronic information is easy to copy and transmit, information that is sensitive to disclosure often needs to be controlled throughout the computer system life cycle so that managers can ensure its proper disposition. The removal of information from a storage medium (such as a hard disk or tape) is called *sanitization*. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by keyboard attack) and purging (rendering information unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, degaussing (for magnetic media only), and destruction.

licenses are site-specific or contain other agreements that prevent the software from being transferred.

Measures may also have to be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys.

8.5 Interdependencies

Like many management controls, life cycle planning relies upon other controls. Three closely linked control areas are policy, assurance, and risk management.

Policy. The development of system-specific policy is an integral part of determining the security requirements.

Assurance. Good life cycle management provides assurance that security is appropriately considered in system design and operation.

Risk Management. The maintenance of security throughout the operational phase of a system is a process of risk management: analyzing risk, reducing risk, and monitoring safeguards. Risk assessment is a critical element in designing the security of systems and in reaccreditations.

8.6 Cost Considerations

Security is a factor throughout the life cycle of a system. Sometimes security choices are made by default, without anyone analyzing why choices are made; sometimes security choices are made carefully, based on analysis. The first case is likely to result in a system with poor security that is susceptible to many types of loss. In the second case, the cost of life cycle management should be *much smaller* than the losses avoided. The major cost considerations for life cycle management are personnel costs and some delays as the system progresses through the life cycle for completing analyses and reviews and obtaining management approvals.

It is possible to overmanage a system: to spend more time planning, designing, and analyzing risk than is necessary. Planning, by itself, does not further the mission or business of an organization. Therefore, while security life cycle management can yield significant benefits, the effort should be commensurate with the system's size, complexity, and sensitivity and the risks associated with the system. In general, the higher the value of the system, the newer the system's architecture, technologies, and practices, and the worse the impact if the system security fails, the more effort should be spent on life cycle management.

References

Communications Security Establishment. *A Framework for Security Risk Management in*

Information Technology Systems. Canada.

Dykman, Charlene A. ed., and Charles K. Davis, asc. ed. *Control Objectives – Controls in an Information Systems Environment: Objectives, Guidelines, and Audit Procedures.* (fourth edition). Carol Stream, IL: The EDP Auditors Foundation, Inc., April 1992.

Guttman, Barbara. *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials.* Special Publication 800-4. Gaithersburg, MD: National Institute of Standards and Technology, March 1992.

Institute of Internal Auditors Research Foundation. *System Auditability and Control Report.* Altamonte Springs, FL: The Institute of Internal Auditors, 1991.

Murphy, Michael, and Xenia Ley Parker. *Handbook of EDP Auditing*, especially Chapter 2 "The Auditing Profession," and Chapter 3, "The EDP Auditing Profession." Boston, MA: Warren, Gorham & Lamont, 1989.

National Bureau of Standards. *Guideline for Computer Security Certification and Accreditation.* Federal Information Processing Standard Publication 102. September 1983.

National Institute of Standards and Technology. "Disposition of Sensitive Automated Information." Computer Systems Laboratory Bulletin. October 1992.

National Institute of Standards and Technology. "Sensitivity of Information." Computer Systems Laboratory Bulletin. November 1992.

Office of Management and Budget. "Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information." OMB Bulletin 90-08. 1990.

Ruthberg, Zella G, Bonnie T. Fisher and John W. Lainhart IV. *System Development Auditor.* Oxford, England: Elsevier Advanced Technology, 1991.

Ruthberg, Z., et al. *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach.* Special Publication 500-153. Gaithersburg, MD: National Bureau of Standards. April 1988.

Vickers Benzel, T. C. *Developing Trusted Systems Using DOD-STD-2167A.* Oakland, CA: IEEE Computer Society Press, 1990.

Wood, C. "Building Security Into Your System Reduces the Risk of a Breach." *LAN Times*, 10(3), 1993. p 47.

Chapter 9

ASSURANCE

Computer security assurance is the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. Assurance is not, however, an absolute guarantee that the measures work as intended. Like the closely related areas of reliability and quality, assurance can be difficult to analyze; however, it is something people expect and obtain (though often without realizing it). For example, people may routinely get product recommendations from colleagues but may not consider such recommendations as providing assurance.

Assurance is a degree of confidence, not a true measure of how secure the system actually is. This distinction is necessary because it is extremely difficult -- and in many cases virtually impossible -- to know exactly how secure a system is.

> Security assurance is the degree of confidence one has that the security controls operate correctly and protect the system as intended.

Assurance is a challenging subject because it is difficult to describe and even more difficult to quantify. Because of this, many people refer to assurance as a "warm fuzzy feeling" that controls work as intended. However, it is possible to apply a more rigorous approach by knowing two things: (1) who needs to be assured and (2) what types of assurance can be obtained. The person who needs to be assured is the management official who is ultimately responsible for the security of the system. Within the federal government, this person is the *authorizing or accrediting official*.[71]

There are many methods and tools for obtaining assurance. For discussion purposes, this chapter categorizes assurance in terms of a general system life cycle. The chapter first discusses planning for assurance and then presents the two categories of assurance methods and tools: (1) design and implementation assurance and (2) operational assurance. Operational assurance is further categorized into audits and monitoring.

The division between design and implementation assurance and operational assurance can be fuzzy. While such issues as configuration management or audits are discussed under operational assurance, they may also be vital during a system's development. The discussion tends to focus more on technical issues during design and implementation assurance and to be a mixture of management, operational, and technical issues under operational assurance. The reader should

---

[71] Accreditation is a process used primarily within the federal government. It is the process of managerial authorization for processing. Different agencies may use other terms for this approval function. The terms used here are consistent with Federal Information Processing Standard 102, *Guideline for Computer Security Certification and Accreditation*. (See reference section of this chapter.)

keep in mind that the division is somewhat artificial and that there is substantial overlap.

9.1 Accreditation and Assurance

Accreditation is a management official's formal acceptance of the adequacy of a system's security. The best way to view computer security accreditation is as a form of quality control. It forces managers and technical staff to work together to find workable, cost-effective solutions given security needs, technical constraints, operational constraints, and mission or business requirements. The accreditation process obliges managers to make the critical decision regarding the adequacy of security safeguards and, therefore, to recognize and perform their role in securing their systems. In order for the decisions to be sound, they need to be based on reliable information about the implementation of both technical and nontechnical safeguards. These include:

- Technical features (Do they operate as intended?).
- Operational practices (Is the system operated according to stated procedures?).
- Overall security (Are there threats which the technical features and operational practices do not address?).
- Remaining risks (Are they acceptable?).

A computer system should be accredited before the system becomes operational with periodic reaccreditation after major system changes or when significant time has elapsed.[72] Even if a system was not initially accredited, the accreditation process can be initiated at any time. Chapter 8 further discusses accreditation.

9.1.1 Accreditation and Assurance

Assurance is an extremely important -- but not the only -- element in accreditation. As shown in the diagram, assurance addresses whether the technical measures and procedures operate either (1) according to a set of security requirements and specifications or (2) according to general quality principles. Accreditation also addresses whether the system's security requirements are correct and well implemented and whether the level of quality is sufficiently high. These activities are discussed in Chapters 7 and 8.

---

[72] OMB Circular A-130 requires management security authorization of operation for federal systems.

9.1.2 Selecting Assurance Methods

The accrediting official makes the final decision about how much and what types of assurance are needed for a system. For this decision to be informed, it is derived from a review of security, such as a risk assessment or other study (e.g., certification), as deemed appropriate by the accrediting official.[73] The accrediting official needs to be in a position to analyze the pros and cons of the cost of assurance, the cost of controls, and the risks to the organization. At the end of the accreditation process, the accrediting official will be the one to accept the remaining risk. Thus, the selection of assurance methods should be coordinated with the accrediting official.

---

[73] In the past, accreditation has been defined to require a certification, which is an in-depth testing of technical controls. It is now recognized within the federal government that other analyses (e.g., a risk analysis or audit) can also provide sufficient assurance for accreditation.

In selecting assurance methods, the need for assurance should be weighed against its cost. Assurance can be quite expensive, especially if extensive testing is done. Each method has strengths and weaknesses in terms of cost and what kind of assurance is actually being delivered. A combination of methods can often provide greater assurance, since no method is foolproof, and can be less costly than extensive testing.

The accrediting official is not the only arbiter of assurance. Other officials who use the system should also be consulted. (For example, a Production Manager who relies on a Supply System should provide input to the Supply Manager.) In addition, there may be constraints outside the accrediting official's control that also affect the selection of methods. For instance, some of the methods may unduly restrict competition in acquisitions of federal information processing resources or may be contrary to the organization's privacy policies. Certain assurance methods may be required by organizational policy or directive.

9.2 Planning and Assurance

Assurance planning should begin during the planning phase of the system life cycle, either for new systems or a system upgrades. Planning for assurance when planning for other system requirements makes sense. If a system is going to need extensive testing, it should be built to facilitate such testing.

Planning for assurance helps a manager make decisions about what kind of assurance will be cost-effective. If a manager waits until a system is built or bought to consider assurance, the number of ways to obtain assurance may be much smaller than if the manager had planned for it earlier, and the remaining assurance options may be more expensive.

9.3 Design and Implementation Assurance

Design and implementation assurance should be examined from two points of view: the component and the system. Component assurance looks at the security of a specific product or system component, such as an operating system, application, security add-on, or telecommunications module. System assurance looks at the security of the entire system, including the interaction between products and modules.

Design and implementation assurance addresses whether the features of a system, application, or component meets security requirements and specifications and whether they are they are well designed and well built. Chapter 8 discusses the source for security requirements and specifications. Design and implementation assurance examines system design, development, and installation. Design and implementation assurance is usually associated with the development/acquisition and implementation phase of the system life cycle; however, it should also be considered throughout the life cycle as the system is modified.

As stated earlier, assurance can address whether the product or system meets a set of security specifications, or it can provide other evidence of quality. This section outlines the major methods for obtaining design and implementation assurance.

9.3.1 Testing and Certification

Testing can address the quality of the system as built, as implemented, or as operated. Thus, it can be performed throughout the development cycle, after system installation, and throughout its operational phase. Some common testing techniques include functional testing (to see if a given function works according to its requirements) or penetration testing (to see if security can be bypassed). These techniques can range from trying several test cases to in-depth studies using metrics, automated tools, or multiple detailed test cases.

Certification is a formal process for testing components or systems against a specified set of security requirements. Certification is normally performed by an independent reviewer, rather than one involved in building the system. Certification is more often cost-effective for complex or high-risk systems. Less formal security testing can be used for lower-risk systems. Certification can be performed at many stages of the system design and implementation process and can take place in a laboratory, operating environment, or both.

9.3.2 NIST Conformance Testing and Validation Suites

NIST produces validation suites and conformance testing to determine if a product (software, hardware, firmware) meets specified standards. These test suites are developed for specific standards and use many methods. Conformance to standards can be important for many reasons, including interoperability or strength of security provided. NIST publishes a list of validated products quarterly.

9.3.3 Use of Advanced or Trusted Development

In the development of both commercial off-the-shelf products and more customized systems, the use of advanced or trusted system architectures, development methodologies, or software engineering techniques can provide assurance. Examples include security design and development reviews, formal modeling, mathematical proofs, ISO 9000 quality techniques, or use of security architecture concepts, such as a trusted computing base (TCB) or reference monitor.

9.3.4 Use of Reliable Architectures

Some system architectures are intrinsically more reliable, such as systems that use fault-tolerance, redundance, shadowing, or redundant array of inexpensive disks (RAID) features. These examples are primarily associated with system availability.

9.3.5 Use of Reliable Security

One factor in reliable security is the concept of *ease of safe use*, which postulates that a system that is easier to secure will be more likely to be secure. Security features may be more likely to be used when the initial system defaults to the "most secure" option. In addition, a system's security may be deemed more reliable if it does not use very new technology that has not been tested in the "real" world (often called "bleeding-edge" technology). Conversely, a system that uses older, well-tested software may be less likely to contain bugs.

9.3.6 Evaluations

A product evaluation normally includes testing. Evaluations can be performed by many types of organizations, including government agencies, both domestic and foreign; independent organizations, such as trade and professional organizations; other vendors or commercial groups; or individual users or user consortia. Product reviews in trade literature are a form of evaluation, as are more formal reviews made against specific criteria. Important factors for using evaluations are the degree of independence of the evaluating group, whether the evaluation criteria reflect needed security features, the rigor of the testing, the testing environment, the age of the evaluation, the competence of the evaluating organization, and the limitations placed on the evaluations by the evaluating group (e.g., assumptions about the threat or operating environment).

9.3.7 Assurance Documentation

The ability to describe security requirements and how they were met can reflect the degree to which a system or product designer understands applicable security issues. Without a good understanding of the requirements, it is not likely that the designer will be able to meet them.

Assurance documentation can address the security either for a system or for specific components. System-level documentation should describe the system's security requirements and how they have been implemented, including *interrelationships* among applications, the operating system, or networks. System-level documentation addresses more than just the operating system, the security system, and applications; it describes the system as *integrated* and *implemented in a particular environment*. Component documentation will generally be an off-the-shelf product, whereas the system designer or implementer will generally develop system documentation.

9.3.8 Accreditation of Product to Operate in Similar Situation

The accreditation of a product or system to operate in a similar situation can be used to provide some assurance. However, it is important to realize that an accreditation is environment- and system-specific. Since accreditation balances risk against advantages, the same product may be appropriately accredited for one environment but not for another, even by the same accrediting official.

9.3.9 Self-Certification

A vendor's, integrator's, or system developer's self-certification does not rely on an impartial or independent agent to perform a technical evaluation of a system to see how well it meets a stated security requirement. Even though it is not impartial, it can still provide assurance. The self-certifier's reputation is on the line, and a resulting certification report can be read to determine whether the security requirement was defined and whether a meaningful review was performed.

A hybrid certification is possible where the work is performed under the auspices or review of an independent organization by having that organization analyze the resulting report, perform spot checks, or perform other oversight. This method may be able to combine the lower cost and greater speed of a self-certification with the impartiality of an independent review. The review, however, may not be as thorough as independent evaluation or testing.

9.3.10 Warranties, Integrity Statements, and Liabilities

Warranties are another source of assurance. If a manufacturer, producer, system developer, or integrator is willing to correct errors within certain time frames or by the next release, this should give the system manager a sense of commitment to the product and of the product's quality. An integrity statement is a formal declaration or certification of the product. It can be backed up by a promise to (a) fix the item (warranty) or (b) pay for losses (liability) if the product does not conform to the integrity statement.

9.3.11 Manufacturer's Published Assertions

A manufacturer's or developer's published assertion or formal declaration provides a limited amount of assurance based exclusively on reputation.

9.3.12 Distribution Assurance

It is often important to know that software has arrived unmodified, especially if it is distributed electronically. In such cases, checkbits or digital signatures can provide high assurance that code has not been modified. Anti-virus software can be used to check software that comes from sources with unknown reliability (such as a bulletin board).

9.4 Operational Assurance

Design and implementation assurance addresses the quality of security features built into systems. Operational assurance addresses whether the system's technical features are being bypassed or have vulnerabilities and whether required procedures are being followed. It does not address changes in the system's security requirements, which could be caused by changes to the system and its operating or threat environment. (These changes are addressed in Chapter 8.)

Security tends to degrade during the operational phase of the system life cycle. System users and operators discover new ways to intentionally or unintentionally bypass or subvert security (especially if there is a perception that bypassing security improves functionality). Users and administrators often think that nothing will happen to them or their system, so they shortcut security. Strict adherence to procedures is rare, and they become outdated, and errors in the system's administration commonly occur.

Organizations use two basic methods to maintain operational assurance:

- A *system audit* -- a *one-time* or *periodic* event to evaluate security. An audit can vary widely in scope: it may examine an entire system for the purpose of reaccreditation or it may investigate a single anomalous event.
- *Monitoring* -- an *ongoing* activity that checks on the system, its users, or the environment.

In general, the more "real-time" an activity is, the more it falls into the category of monitoring. This distinction can create some unnecessary linguistic hairsplitting, especially concerning system-generated audit trails. Daily or weekly reviewing of the audit trail (for unauthorized access attempts) is generally monitoring, while an historical review of several months' worth of the trail (tracing the actions of a specific user) is probably an audit.

9.4.1 Audit Methods and Tools

An audit conducted to support operational assurance examines whether the system is meeting stated or implied security requirements including system and organization policies. Some audits also examine whether security requirements are appropriate, but this is outside the scope of operational assurance. (See Chapter 8.) Less formal audits are often called *security reviews*.

Audits can be self-administered or independent (either internal or external).[74] Both types can provide excellent information about technical, procedural, managerial, or other aspects of security. The essential difference between a self-audit and an independent audit is objectivity. Reviews done by system management staff, often called self-audits/ assessments, have an inherent conflict of interest. The system management staff may have little incentive to say that the computer system was poorly designed or is sloppily operated. On the other hand, they may be motivated by a strong desire to improve the security of the system. In addition, they are knowledgeable about the system and may be able to find hidden problems.

A person who performs an independent audit should be free from personal and external constraints which may impair their independence and should be organizationally independent.

The independent auditor, by contrast, should have no professional stake in the system. Independent audit may be performed by a professional audit staff in accordance with generally accepted auditing standards.

There are many methods and tools, some of which are described here, that can be used to audit a system. Several of them overlap.

9.4.1.1 Automated Tools

Even for small multiuser computer systems, it is a big job to manually review security features. Automated tools make it feasible to review even large computer systems for a variety of security flaws.

There are two types of automated tools: (1) active tools, which find vulnerabilities by trying to exploit them, and (2) passive tests, which only examine the system and infer the existence of problems from the state of the system.

Automated tools can be used to help find a variety of threats and vulnerabilities, such as improper access controls or access control configurations, weak passwords, lack of integrity of the system software, or not using all relevant software updates and patches. These tools are often very successful at finding vulnerabilities and are sometimes used by hackers to break into systems. Not taking advantage of these tools puts system administrators at a disadvantage. Many of the tools are simple to use; however, some programs (such as access-control auditing

---

[74] An example of an internal auditor in the federal government is the Inspector General. The General Accounting Office can perform the role of external auditor in the federal government. In the private sector, the corporate audit staff serves the role of internal auditor, while a public accounting firm would be an external auditor.

tools for large mainframe systems) require specialized skill to use and interpret.

9.4.1.2 Internal Controls Audit

An auditor can review controls in place and determine whether they are effective. The auditor will often analyze both computer and noncomputer-based controls. Techniques used include inquiry, observation, and testing (of both the controls themselves and the data). The audit can also detect illegal acts, errors, irregularities, or a lack of compliance with laws and regulations. Security checklists and penetration testing, discussed below, may be used.

> The General Accounting Office provides standards and guidance for internal controls audits of federal agencies.

9.4.1.3 Security Checklists

Within the government, the computer security plan provides a checklist against which the system can be audited. This plan, discussed in Chapter 8, outlines the major security considerations for a system, including management, operational, and technical issues. One advantage of using a computer security plan is that it reflects the unique security environment of the system, rather than a generic list of controls. Other checklists can be developed, which include national or organizational security policies and practices (often referred to as *baselines*). Lists of "generally accepted security practices" (GSSPs) can also be used. Care needs to be taken so that deviations from the list are not automatically considered wrong, since they may be appropriate for the system's particular environment or technical constraints.

> Warning: Security Checklists that are passed (e.g., with a B+ or better score) are often used mistakenly as proof (instead of an indication) that security is sufficient. Also, managers of systems which "fail" a checklist often focus too much attention on "getting the points," rather than whether the security measures makes sense in the particular environment and are correctly implemented.

Checklists can also be used to verify that changes to the system have been reviewed from a security point of view. A common audit examines the system's configuration to see if major changes (such as connecting to the Internet) have occurred that have not yet been analyzed from a security point of view.

9.4.1.4 Penetration Testing

Penetration testing can use many methods to attempt a system break-in. In addition to using active automated tools as described above, penetration testing can be done "manually." The most useful type of penetration testing is to use methods that might really be used against the system. For hosts on the Internet, this would certainly include automated tools. For many systems, lax procedures or a lack of internal controls on applications are common vulnerabilities that penetration testing can target. Another method is "social engineering," which involves getting users or administrators to divulge information about systems, including their passwords.[75]

9.4.2 Monitoring Methods and Tools

Security monitoring is an ongoing activity that looks for vulnerabilities and security problems. Many of the methods are similar to those used for audits, but are done more regularly or, for some automated tools, in real time.

9.4.2.1 Review of System Logs

As discussed in Chapter 8, a periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours.

9.4.2.2 Automated Tools

Several types of automated tools monitor a system for security problems. Some examples follow:

- *Virus scanners* are a popular means of checking for virus infections. These programs test for the presence of viruses in executable program files.

- *Checksumming* presumes that program files should not change between updates. They work by generating a mathematical value based on the contents of a particular file. When the integrity of the file is to be verified, the checksum is generated on the current file and compared with the previously generated value. If the two values are equal, the integrity of the file is verified. Program checksumming can detect viruses, Trojan horses, accidental changes to files caused by hardware failures, and other changes to files. However, they may be subject to covert replacement by a system intruder. Digital signatures can also be used.

- *Password crackers* check passwords against a dictionary (either a "regular" dictionary or a specialized one with easy-to-guess passwords) and also check if passwords are common permutations of the user ID. Examples of special dictionary entries could be the names of regional sports teams and stars; common permutations could be the user ID spelled backwards.

- *Integrity verification programs* can be used by such applications to look for evidence of data

---

[75] While penetration testing is a very powerful technique, it should preferably be conducted with the knowledge and consent of system management. Unknown penetration attempts can cause a lot of stress among operations personnel, and may create unnecessary disturbances.

tampering, errors, and omissions. Techniques include consistency and reasonableness checks and validation during data entry and processing. These techniques can check data elements, as input or as processed, against expected values or ranges of values; analyze transactions for proper flow, sequencing, and authorization; or examine data elements for expected relationships. These programs comprise a very important set of processes because they can be used to convince people that, if they do what they should not do, accidentally or intentionally, they will be caught. Many of these programs rely upon logging of individual user activities.

- *Intrusion detectors* analyze the system audit trail, especially log-ons, connections, operating system calls, and various command parameters, for activity that could represent unauthorized activity. Intrusion detection is covered in Chapters 12 and 18.

- *System performance monitoring* analyzes system performance logs in real time to look for availability problems, including active attacks (such as the 1988 Internet worm) and system and network slowdowns and crashes.

9.4.2.3 Configuration Management

From a security point of view, configuration management provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security. Some organizations, particularly those with very large systems (such as the federal government), use a configuration control board for configuration management. When such a board exists, it is helpful to have a computer security expert participate. In any case, it is useful to have computer security officers participate in system management decision making.

Changes to the system can have security implications because they may introduce or remove vulnerabilities and because significant changes may require updating the contingency plan, risk analysis, or accreditation.

9.4.2.4 Trade Literature/Publications/Electronic News

In addition to monitoring the system, it is useful to monitor external sources for information. Such sources as trade literature, both printed and electronic, have information about security vulnerabilities, patches, and other areas that impact security. The Forum of Incident Response Teams (FIRST) has an electronic mailing list that receives information on threats, vulnerabilities, and patches.[76]

9.5 Interdependencies

Assurance is an issue for every control and safeguard discussed in this handbook. Are user ID and access privileges kept up to date? Has the contingency plan been tested? Can the audit trail be tampered with? One important point to be reemphasized here is that assurance is not only for technical controls, but for operational controls as well. Although the chapter focused on information systems assurance, it is also important to have assurance that management controls are working well. Is the security program effective? Are policies understood and followed? As noted in the introduction to this chapter, the need for assurance is more widespread than people often realize.

Life Cycle. Assurance is closely linked to the planning for security in the system life cycle. Systems can be designed to facilitate various kinds of testing against specified security requirements. By planning for such testing early in the process, costs can be reduced; in some cases, without proper planning, some kinds of assurance cannot be otherwise obtained.

9.6 Cost Considerations

There are many methods of obtaining assurance that security features work as anticipated. Since assurance methods tend to be qualitative rather than quantitative, they will need to be evaluated. Assurance can also be quite expensive, especially if extensive testing is done. It is useful to evaluate the amount of assurance received for the cost to make a best-value decision. In general, personnel costs drive up the cost of assurance. Automated tools are generally limited to addressing specific problems, but they tend to be less expensive.

References

Borsook, P. "Seeking Security." *Byte*. 18(6), 1993. pp. 119-128.

Dykman, Charlene A. ed., and Charles K. Davis, asc. ed. *Control Objectives – Controls in an Information Systems Environment: Objectives, Guidelines, and Audit Procedures*. (fourth edition). Carol Stream, IL: The EDP Auditors Foundation, Inc., April 1992.

Farmer, Dan and Wietse Venema. "Improving the Security of Your Site by Breaking Into It." Available from FTP.WIN.TUE.NL. 1993.

Guttman, Barbara. *Computer Security Considerations in Federal Procurements: A Guide for*

---

[76] For information on FIRST, send e-mail to FIRST-SEC@FIRST.ORG.

Procurement Initiators, Contracting Officers, and Computer Security Officials. Special Publication 800-4. Gaithersburg, MD: National Institute of Standards and Technology, March 1992.

Howe, D. "Information System Security Engineering: Cornerstone to the Future." *Proceedings of the 15th National Computer Security Conference*, Vol 1. (Baltimore, MD) Gaithersburg, MD: National Institute of Standards and Technology, 1992. pp. 244-251.

Levine, M. "Audit Serve Security Evaluation Criteria." *Audit Vision.* 2(2). 1992, pp. 29-40.

National Bureau of Standards. *Guideline for Computer Security Certification and Accreditation.* Federal Information Processing Standard Publication 102. September 1983.

National Bureau of Standards. *Guideline for Lifecycle Validation, Verification, and Testing of Computer Software.* Federal Information Processing Standard Publication 101. June 1983.

National Bureau of Standards. *Guideline for Software Verification and Validation Plans.* Federal Information Processing Standard Publication 132. November 1987.

Nuegent, W., J. Gilligan, L. Hoffman, and Z. Ruthberg. *Technology Assessment: Methods for Measuring the Level of Computer Security.* Special Publication 500-133. Gaithersburg, MD: National Bureau of Standards, 1985.

Peng, Wendy W., and Dolores R. Wallace. *Software Error Analysis.* Special Publication 500-209. Gaithersburg, MD: National Institute of Standards and Technology, 1993.

Peterson, P. "Infosecurity and Shrinking Media." *ISSA Access.* 5(2), 1992. pp. 19-22.

Pfleeger, C., S. Pfleeger, and M. Theofanos, "A Methodology for Penetration Testing." *Computers and Security.* 8(7), 1989. pp. 613-620.

Polk, W. Timothy, and Lawrence Bassham. *A Guide to the Selection of Anti-Virus Tools and Techniques.* Special Publication 800-5. Gaithersburg, MD: National Institute of Standards and Technology, December 1992.

Polk, W. Timothy. *Automated Tools for Testing Computer System Vulnerability.* Special Publication 800-6. Gaithersburg, MD: National Institute of Standards and Technology, December 1992.

President's Council on Integrity and Efficiency. *Review of General Controls in Federal Computer Systems.* Washington, DC: President's Council on Integrity and Efficiency, October 1988.

President's Council on Management Improvement and the President's Council on Integrity and Efficiency. *Model Framework for Management Control Over Automated Information System.* Washington, DC: President's Council on Management Improvement, January 1988.

Ruthberg, Zella G, Bonnie T. Fisher and John W. Lainhart IV. *System Development Auditor.* Oxford, England: Elsevier Advanced Technology, 1991.

Ruthburg, Zella, et al. *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach.* Special Publication 500-153. Gaithersburg, MD: National Bureau of Standards, April 1988.

Strategic Defense Initiation Organization. *Trusted Software Methodology.* Vols. 1 and II. SDI-S-SD-91-000007. June 17, 1992.

Wallace, Dolores, and J.C. Cherniasvsky. *Guide to Software Acceptance.* Special Publication 500-180. Gaithersburg, MD: National Institute of Standards and Technology, April 1990.

Wallace, Dolores, and Roger Fugi. *Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Product Management Standards.* Special Publication 500-165. Gaithersburg, MD: National Institute of Standards and Technology, September 1989.

Wallace, Dolores R., Laura M. Ippolito, and D. Richard Kuhn. *High Integrity Software Standards and Guidelines.* Special Publication 500-204. Gaithersburg, MD: National Institute of Standards and Technology, 1992.

Wood, C., et al. *Computer Security: A Comprehensive Controls Checklist.* New York, NY: John Wiley & Sons, 1987.

III. OPERATIONAL CONTROLS

Chapter 10

PERSONNEL/USER ISSUES

Many important issues in computer security involve human users, designers, implementors, and managers. A broad range of security issues relate to how these individuals interact with computers and the access and authorities they need to do their job. No computer system can be secured without properly addressing these security issues.[77]

This chapter examines issues concerning the staffing of positions that interact with computer systems; the administration of users on a system, including considerations for terminating employee access; and special considerations that may arise when contractors or the public have access to systems. Personnel issues are closely linked to logical access controls, discussed in Chapter 17.

10.1 Staffing

The staffing process generally involves at least four steps and can apply equally to general users as well as to application managers, system management personnel, and security personnel. These four steps are: (1) defining the job, normally involving the development of a position description; (2) determining the sensitivity of the position; (3) filling the position, which involves screening applicants and selecting an individual; and (4) training.

10.1.1 Groundbreaking – Position Definition

Early in the process of defining a position, security issues should be identified and dealt with. Once a position has been broadly defined, the responsible supervisor should determine the type of computer access needed for the position. There are two general principles to apply when granting access: *separation of duties* and *least privilege*.

Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment. In effect, checks and balances need to be designed into both the process as well as the specific, individual positions of personnel who will implement the process. Ensuring that such duties are well defined is the responsibility of management.

Least privilege refers to the security objective of granting users *only those accesses they need to*

---

[77] A distinction is made between users and personnel, since some users (e.g., contractors and members of the public) may not be considered personnel (i.e., employees).

perform their official duties. Data entry clerks, for example, may not have any need to run analysis reports of their database. However, least privilege does not mean that all users will have extremely little functional access; some employees will have significant access if it is required for their position. However, applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources. It is important to make certain that the implementation of least privilege does not interfere with the ability to have personnel substitute for each other without undue delay. Without careful planning, access control can interfere with contingency plans.

10.1.2 Determining Position Sensitivity

Knowledge of the duties and access levels that a particular position will require is necessary for determining the sensitivity of the position. The responsible management official should correctly identify position sensitivity levels so that appropriate, cost-effective screening can be completed.

Various levels of sensitivity are assigned to positions in the federal government. Determining the appropriate level is based upon such factors as the type and degree of harm (e.g., disclosure of private information, interruption of critical processing, computer fraud) the individual can cause through misuse of the computer system as well as more traditional factors, such as access to classified information and fiduciary responsibilities. Specific agency guidance should be followed on this matter.

It is important to select the appropriate position sensitivity, since controls in excess of the sensitivity of the position wastes resources, while too little may cause unacceptable risks.

10.1.3 Filling the Position -- Screening and Selecting

Once a position's sensitivity has been determined, the position is ready to be staffed. In the federal government, this typically includes publishing a formal vacancy announcement and identifying which applicants meet the position requirements. More sensitive positions typically require *preemployment* background screening; screening after employment has commenced (post-entry-on-duty) may suffice for less sensitive positions.

> In general, it is more effective to use separation of duties and least privilege to limit the sensitivity of the position, rather than relying on screening to reduce the risk to the organization.

Background screening helps determine whether a particular individual is suitable for a given position. For example, in positions with high-level fiduciary responsibility, the screening process will attempt to ascertain the person's trustworthiness and appropriateness for a particular position. In the federal government, the screening process is formalized through a series of background checks conducted through a central investigative office within the organization or through another organization (e.g., the Office of Personnel Management).

Within the Federal Government, the most basic screening technique involves a check for a criminal history, checking FBI fingerprint records, and other federal indices.[78] More extensive background checks examine other factors, such as a person's work and educational history, personal interview, history of possession or use of illegal substances, and interviews with current and former colleagues, neighbors, and friends. The exact type of screening that takes place depends upon the sensitivity of the position and applicable agency implementing regulations. Screening is not conducted by the prospective employee's manager; rather, agency security and personnel officers should be consulted for agency-specific guidance.

Outside of the Federal Government, employee screening is accomplished in many ways. Policies vary considerably among organizations due to the sensitivity of examining an individual's background and qualifications. Organizational policies and procedures normally try to balance fears of invasiveness and slander against the need to develop confidence in the integrity of employees. One technique may be to place the individual in a less sensitive position initially.

For both the Federal Government and private sector, finding something compromising in a person's background does not necessarily mean they are unsuitable for a particular job. A determination should be made based on the type of job, the type of finding or incident, and other relevant factors. In the federal government, this process is referred to as *adjudication*.

10.1.4 Employee Training and Awareness

Even after a candidate has been hired, the staffing process cannot yet be considered complete – employees still have to be trained to do their job, which includes computer security responsibilities and duties. As discussed in Chapter 13, such security training can be very cost-effective in promoting security.

Some computer security experts argue that employees must receive initial computer security training before they are granted any access to computer systems. Others argue that this must be a risk-based decision, perhaps granting only restricted access (or, perhaps, only access to their PC) until the required training is completed. Both approaches recognize that adequately trained employees are crucial to the effective functioning of computer systems and applications. Organizations may provide introductory training prior to granting any access with follow-up more extensive training. In addition, although training of new users is critical, it is important to

---

[78] In the federal government, separate and unique screening procedures are not established for each position. Rather, positions are categorized by general sensitivity and are assigned a corresponding level of background investigation or other checks.

recognize that security training and awareness activities should be ongoing during the time an individual is a system user. (See Chapter 13 for a more thorough discussion.)

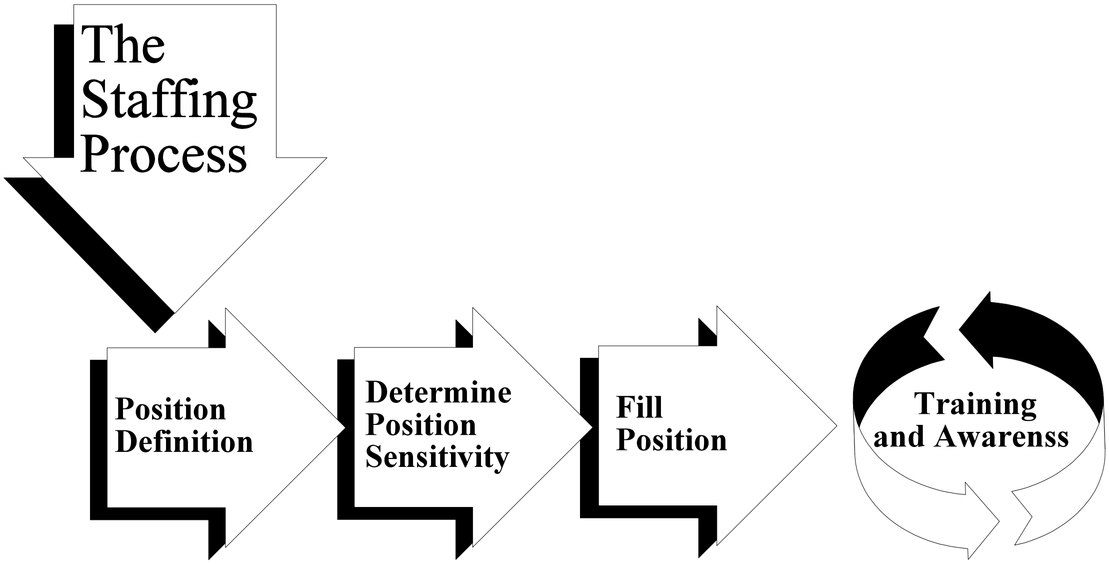


Figure 10.1

10.2 User Administration

Effective administration of users' computer access is essential to maintaining system security. *User account management* focuses on identification, authentication, and access authorizations. This is augmented by the process of *auditing* and otherwise periodically verifying the legitimacy of current accounts and access authorizations. Finally, there are considerations involved in the *timely modification or removal of access* and associated issues for employees who are reassigned, promoted, or terminated, or who retire.

10.2.1 User Account Management

User account management involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

User account management typically begins with a request from the user's supervisor to the system manager for a system account. If a user is to have access to a particular application, this request may be sent through the application manager to the system manager. This will ensure that the systems office receives formal approval from the "application manager" for the employee to be given access. The request will normally state the level of access to be granted, perhaps by function or by specifying a particular user profile. (Often when more than one employee is doing the same job, a "profile" of permitted authorizations is created.)

Systems operations staff will normally then use the account request to create an account for the new user. The access levels of the account will be consistent with those requested by the supervisor. This account will normally be assigned selected access authorizations. These are sometimes built directly into applications, and other times rely upon the operating system. "Add-on" access applications are also used. These access levels and authorizations are often tied to specific access levels within an application.

[redacted]

Next, employees will be given their account information, including the account identifier (e.g., user ID) and a means of authentication (e.g., password or smart card/PIN). One issue that may arise at this stage is whether the user ID is to be tied to the particular *position* an employee holds (e.g., ACC5 for an accountant) or the *individual employee* (e.g., BSMITH for Brenda Smith). Tying user IDs to positions may simplify administrative overhead in some cases; however, it may make auditing more difficult as one tries to trace the actions of a particular individual. It is normally more advantageous to tie the user ID to the individual employee. However, if the user ID is created and tied to a position, procedures will have to be established to change them if employees switch jobs or are otherwise reassigned.

When employees are given their account, it is often convenient to provide initial or refresher training and awareness on computer security issues. Users should be asked to review a set of rules and regulations for system access. To indicate their understanding of these rules, many organizations require employees to sign an "acknowledgment statement," which may also state causes for dismissal or prosecution under the Computer Fraud and Abuse Act and other applicable state and local laws.[79]

[redacted]

When user accounts are no longer required, the supervisor should inform the application manager and system management office so accounts can be removed in a timely manner. One useful secondary check is to work with the local organization's personnel officer to establish a procedure for routine notification of employee departures to the systems office. Further issues are discussed in the "Termination" section of this chapter.

It is essential to realize that *access and authorization administration is a continuing process*. New user accounts are added while others are deleted. Permissions change: sometimes permanently, sometimes temporarily. New applications are added, upgraded, and removed. Tracking this information to keep it up to date is not easy, but is necessary to allow users access to only those functions necessary to accomplish their assigned responsibilities – thereby helping to maintain the principle of *least privilege*. In managing these accounts, there is a need to balance timeliness of service and record keeping. While sound record keeping practices are necessary, delays in processing requests (e.g., change requests) may lead to requests for more access than is really necessary – just to avoid delays should such access ever be required.

Managing this process of user access is also one that, particularly for larger systems, is often decentralized. Regional offices may be granted the authority to create accounts and change user access authorizations or to submit forms requesting that the centralized access control function make the necessary changes. Approval of these changes is important – it may require the approval of the file owner and the supervisor of the employee whose access is being changed.

10.2.2 Audit and Management Reviews

From time to time, it is necessary to review user account management on a system. Within the area of user access issues, such reviews may examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth.

---

[79] Whenever users are asked to sign a document, appropriate review by organizational legal counsel and, if applicable, by employee bargaining units should be accomplished.

These reviews can be conducted on *at least* two levels:[80] (1) on an application-by-application basis or (2) on a systemwide basis. Both kinds of reviews can be conducted by, among others, in-house systems personnel (a self-audit), the organization's internal audit staff, or external auditors. For example, a good practice is for application managers (and data owners, if different) to review all access levels of all application users every month – and sign a formal access approval list, which will provide a written record of the approvals. While it may initially appear that such reviews should be conducted by systems personnel, they usually are not fully effective. System personnel *can* verify that users only have those accesses that their managers have specified. However because access requirements may change over time, it is important to involve the application manager, who is often the only individual in a position to know current access requirements.

Outside audit organizations (e.g., the Inspector General [IG] or the General Accounting Office) may also conduct audits. For example, the IG may direct a more extensive review of permissions. This may involve discussing the need for particular access levels for specific individuals or the number of users with sensitive access. For example, how many employees should really have authorization to the check-printing function? (Auditors will also examine non-computer access by reviewing, for example, who should have physical access to the check printer or blank-check stock.)

10.2.3 Detecting Unauthorized/Illegal Activities

Several mechanisms are used besides auditing[81] and analysis of audit trails to detect unauthorized and illegal acts. (See Chapters 9 and 18.) For example, fraudulent activities may require the regular physical presence of the perpetrator(s). In such cases, the fraud may be detected during the employee's absence. Mandatory vacations for critical systems and applications personnel can help detect such activity (however, this is not a guarantee, for example, if problems are saved for the employees to handle upon their return). It is useful to avoid creating an excessive dependence upon any single individual, since the system will have to function during periods of absence. Particularly within the government, periodic rescreening of personnel is used to identify possible indications of illegal activity (e.g., living a lifestyle in excess of known income level).

10.2.4 Temporary Assignments and In-house Transfers

One significant aspect of managing a system involves keeping user access authorizations up to date. Access authorizations are typically changed under two types of circumstances: (1) change in job role, either temporarily (e.g., while covering for an employee on sick leave) or

---

[80] Note that this is not an either/or distinction.

[81] The term *auditing* is used here in a broad sense to refer to the review and analysis of past events.

permanently (e.g., after an in-house transfer) and (2) termination discussed in the following section.

Users often are required to perform duties outside their normal scope during the absence of others. This requires additional access authorizations. Although necessary, such extra access authorizations should be granted sparingly and monitored carefully, consistent with the need to maintain separation of duties for internal control purposes. Also, they should be removed promptly when no longer required.

Permanent changes are usually necessary when employees change positions within an organization. In this case, the process of granting account authorizations (described in Section 10.2.1) will occur again. At this time, however, is it also important that access authorizations of the prior position be removed. Many instances of "authorization creep" have occurred with employees continuing to maintain access rights for previously held positions within an organization. This practice is inconsistent with the principle of least privilege.

10.2.5 Termination

Termination of a user's system access generally can be characterized as either "friendly" or "unfriendly." Friendly termination may occur when an employee is voluntarily transferred, resigns to accept a better position, or retires. Unfriendly termination may include situations when the user is being fired for cause, "RIFed,"[82] or involuntarily transferred. Fortunately, the former situation is more common, but security issues have to be addressed in both situations.

10.2.5.1 Friendly Termination

Friendly termination refers to the removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable. Since terminations can be expected regularly, this is usually accomplished by implementing a standard set of procedures for outgoing or transferring employees. These are part of the standard employee "out-processing," and are put in place, for example, to ensure that system accounts are removed in a timely manner. Out-processing often involves a sign-out form initialed by each functional manager with an interest in the separation. This normally includes the group(s) managing access controls, the control of keys, the briefing on the responsibilities for confidentiality and privacy, the library, the property clerk, and several other functions not necessarily related to information security.

In addition, other issues should be examined as well. The continued availability of data, for example, must often be assured. In both the manual and the electronic worlds, this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk,

---

[82] *RIF* is a term used within the government as shorthand for "reduction in force."

and how are they backed up. Employees should be instructed whether or not to "clean up" their PC before leaving. If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured. Authentication tokens must be collected.

Confidentiality of data can also be an issue. For example, do employees know what information they are allowed to share with their immediate organizational colleagues? Does this differ from the information they may share with the public? These and other organizational-specific issues should be addressed throughout an organization to ensure continued access to data and to provide continued confidentiality and integrity during personnel transitions. (Many of these issues should be addressed on an ongoing basis, not just during personnel transitions.) The training and awareness program normally should address such issues.

10.2.5.2 Unfriendly Termination

Unfriendly termination involves the removal of an employee under involuntary or adverse conditions. This may include termination for cause, RIF, involuntary transfer, resignation for "personality conflicts," and situations with pending grievances. The tension in such terminations may multiply and complicate security issues. Additionally, all of the issues involved in friendly terminations are still present, but addressing them may be considerably more difficult.

The greatest threat from unfriendly terminations is likely to come from those personnel who are capable of changing code or modifying the system or applications. For example, systems personnel are ideally positioned to wreak considerable havoc on systems operations. Without appropriate safeguards, personnel with such access can place logic bombs (e.g., a hidden program to erase a disk) in code that will not even execute until after the employee's departure. Backup copies can be destroyed. There are even examples where code has been "held hostage." But other employees, such as general users, can also cause damage. Errors can be input purposefully, documentation can be misfiled, and other "random" errors can be made. Correcting these situations can be extremely resource intensive.

Given the potential for adverse consequences, security specialists routinely recommend that system access be terminated as quickly as possible in such situations. If employees are to be fired, system access should be removed at the same time (or just before) the employees are notified of their dismissal. When an employee notifies an organization of a resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately terminated. During the "notice" period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications. In other cases, physical removal from their offices (and, of course, logical removal, *when logical access controls exist*) may suffice.

10.3 Contractor Access Considerations

Many federal agencies as well as private organizations use contractors and consultants to assist with computer processing. Contractors are often used for shorter periods of time than regular employees. This factor may change the cost-effectiveness of conducting screening. The often higher turnover among contractor personnel generates additional costs for security programs in terms of user administration.

10.4 Public Access Considerations

Many federal agencies have begun to design, develop, and implement public access systems for electronic dissemination of information to the public. Some systems provide electronic interaction by allowing the public to send information to the government (e.g., electronic tax filing) as well as to receive it. When systems are made available for access by the public (or a large or significant subset thereof), additional security issues arise due to: (1) increased threats against public access systems and (2) the difficulty of security administration.

While many computer systems have been victims of hacker attacks, public access systems are well known and have published phone numbers and network access IDs. In addition, a successful attack could result in a lot of publicity. For these reasons, public access systems are subject to a greater threat from hacker attacks on the confidentiality, availability, and integrity of information processed by a system. In general, it is safe to say that when a system is made available for public access, the risk to the system increases – and often the constraints on its use are tightened.

[redacted]

Besides increased risk of hackers, public access systems can be subject to insider malice. For example, an unscrupulous user, such as a disgruntled employee, may try to introduce errors into data files intended for distribution in order to embarrass or discredit the organization. Attacks on public access systems could have a substantial impact on the organization's reputation and the level of public confidence due to the high visibility of public access systems. Other security problems may arise from unintentional actions by untrained users.

In systems without public access, there are procedures for enrolling users that often involve some user training and frequently require the signing of forms acknowledging user responsibilities. In addition, user profiles can be created and sophisticated audit mechanisms can be developed to detect unusual activity by a user. In public access systems, users are often anonymous. This can complicate system security administration.

In most systems without public access, users are typically a mix of known employees or contractors. In this case, imperfectly implemented access control schemes may be tolerated. However, when opening up a system to public access, additional precautions may be necessary because of the increased threats.

10.5 Interdependencies

User issues are tied to topics throughout this handbook.

Training and Awareness discussed in Chapter 13 is a critical part of addressing the user issues of computer security.

Identification and Authentication and *Access Controls* in a computer system can only prevent people from doing what the computer is instructed they are not allowed to do, as stipulated by *Policy*. The recognition by computer security experts that much more harm comes from people doing what they are allowed to do, but should not do, points to the importance of considering user issues in the computer security picture, and the importance of *Auditing*.

Policy, particularly its compliance component, is closely linked to personnel issues. A deterrent effect arises among users when they are aware that their misconduct, intentional or unintentional, will be detected.

These controls also depend on manager's (1) selecting the right type and level of access for their employees and (2) informing system managers of which employees need accounts and what type and level of access they require, and (3) promptly informing system managers of changes to access requirements. Otherwise, accounts and accesses can be granted to or maintained for people who should not have them.

10.6 Cost Considerations

There are many security costs under the category of user issues. Among these are:

Screening -- Costs of initial background screening and periodic updates, as appropriate.[83]

Training and Awareness -- Costs of training needs assessments, training materials, course fees, and so forth, as discussed separately in Chapter 13.

User Administration -- Costs of managing identification and authentication which, particularly for large distributed systems, may be rather significant.

---

[83] When analyzing the costs of screening, it is important to realize that screening is often conducted to meet requirements wholly unrelated to computer security.

Access Administration -- Particularly beyond the initial account set-up, are ongoing costs of maintaining user accesses currently and completely.

Auditing -- Although such costs can be reduced somewhat when using automated tools, consistent, resource-intensive human review is still often necessary to detect and resolve security anomalies.

References

Fites, P., and M. Kratz. *Information Systems Security: A Practitioner's Reference*. New York, NY: Van Nostrand Reinhold, 1993. (See especially Chapter 6.)

National Institute of Standards and Technology. "Security Issues in Public Access Systems." Computer Systems Laboratory Bulletin. May 1993.

North, S. "To Catch a `Crimoid.'" *Beyond Computing*. 1(1), 1992. pp. 55-56.

Pankau, E. "The Consummate Investigator." *Security Management*. 37(2), 1993. pp. 37-41.

Schou, C., W. Machonachy, F. Lynn McNulty, and A. Chantker. "Information Security Professionalism for the 1990s." *Computer Security Journal*. 9(1), 1992. pp. 27-38.

Wagner, M. "Possibilities Are Endless, and Frightening." *Open Systems Today*. November 8 (136), 1993. pp. 16-17.

Wood, C. "Be Prepared Before You Fire." *Infosecurity News*. 5(2), 1994. pp. 51-54.

Wood, C. "Duress, Terminations and Information Security." *Computers and Security*. 12(6), 1993. pp. 527-535.

Chapter 11

PREPARING FOR CONTINGENCIES AND DISASTERS

A *computer security contingency* is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.[84]

To avert potential contingencies and disasters or minimize the damage they cause organizations can take steps early to control the event. Generally called *contingency planning*,[85] this activity is closely related to incident handling, which primarily addresses malicious technical threats such as hackers and viruses.[86]

[redacted]

Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organization.

This chapter presents the contingency planning process in six steps:[87]

1. *Identifying the mission- or business-critical functions.*

2. *Identifying the resources that support the critical functions.*

3. *Anticipating potential contingencies or disasters.*

4. *Selecting contingency planning strategies.*

---

[84] There is no distinct dividing line between disasters and other contingencies.

[85] Other names include disaster recovery, business continuity, continuity of operations, or business resumption planning.

[86] Some organizations include incident handling as a subset of contingency planning. The relationship is further discussed in Chapter 12, Incident Handling.

[87] Some organizations and methodologies may use a different order, nomenclature, number, or combination of steps. The specific steps can be modified, as long as the basic functions are addressed.

5. *Implementing the contingency strategies.*

6. *Testing and revising the strategy.*

11.1 Step 1: Identifying the Mission- or Business-Critical Functions

[redacted]

Protecting the continuity of an organization's mission or business is very difficult if it is not clearly identified. Managers need to understand the organization from a point of view that usually extends beyond the area they control. The definition of an organization's critical mission or business functions is often called a *business plan.*

Since the development of a business plan will be used to support contingency planning, it is necessary not only to identify critical missions and businesses, but also to *set priorities for* them. A fully redundant capability for each function is prohibitively expensive for most organizations. In the event of a disaster, certain functions will not be performed. If appropriate priorities have been set (and approved by senior management), it could mean the difference in the organization's ability to survive a disaster.

11.2 Step 2: Identifying the Resources That Support Critical Functions

[redacted]

After identifying critical missions and business functions, it is necessary to identify the supporting resources, the time frames in which each resource is used (e.g., is the resource needed constantly or only at the end of the month?), and the effect on the mission or business of the unavailability of the resource. In identifying resources, a traditional problem has been that different managers oversee different resources. They may not realize how resources interact to support the organization's mission or business. Many of these resources are *not* computer resources. Contingency planning should address all the resources needed to perform a function, regardless whether they directly relate to a computer.[88]

---

[88] However, since this is a computer security handbook, the descriptions here focus on the computer-related resources. The logistics of coordinating contingency planning for computer-related and other resources is an important consideration.

The analysis of needed resources should be conducted by those who understand how the function is performed and the dependencies of various resources on other resources and other critical relationships. This will allow an organization to *assign priorities* to resources since not all elements of all resources are crucial to the critical functions.

11.2.1 Human Resources

[redacted]

People are perhaps an organization's most obvious resource. Some functions require the effort of specific individuals, some require specialized expertise, and some only require individuals who can be trained to perform a specific task. Within the information technology field, human resources include both operators (such as technicians or system programmers) and users (such as data entry clerks or information analysts).

11.2.2 Processing Capability

Traditionally contingency planning has focused on processing power (i.e., if the data center is down, how can applications dependent on it continue to be processed?). Although the need for data center backup remains vital, today's other processing alternatives are also important. Local area networks (LANs), minicomputers, workstations, and personal computers in all forms of centralized and distributed processing may be performing critical tasks.

[redacted]

11.2.3 Automated Applications and Data

Computer systems run applications that process data. Without current electronic versions of both applications and data, computerized processing may not be possible. If the processing is being performed on alternate hardware, the applications must be compatible with the alternate hardware, operating systems and other software (including version and configuration), and numerous other technical factors. Because of the complexity, it is normally necessary to periodically verify compatibility. (See Step 6, Testing and Revising.)

11.2.4 Computer-Based Services

An organization uses many different kinds of computer-based services to perform its functions. The two most important are normally communications services and information services. Communications can be further categorized as data and voice communications; however, in many organizations these are managed by the same service. Information services include any source of information outside of the organization. Many of these sources are becoming automated, including on-line government and private databases, news services, and bulletin boards.

11.2.5 Physical Infrastructure

For people to work effectively, they need a safe working environment and appropriate equipment and utilities. This can include office space, heating, cooling, venting, power, water, sewage, other utilities, desks, telephones, fax machines, personal computers, terminals, courier services, file cabinets, and many other items. In addition, computers also need space and utilities, such as electricity. Electronic and paper media used to store applications and data also have physical requirements.

11.2.6 Documents and Papers

Many functions rely on vital records and various documents, papers, or forms. These records could be important because of a legal need (such as being able to produce a signed copy of a loan) or because they are the only record of the information. Records can be maintained on paper, microfiche, microfilm, magnetic media, or optical disk.

11.3 Step 3: Anticipating Potential Contingencies or Disasters

Although it is impossible to think of *all* the things that can go wrong, the next step is to identify a likely range of problems. The development of scenarios will help an organization develop a plan to address the wide range of things that can go wrong.

Scenarios should include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, can point to other possible, but less obvious, contingencies. The contingency scenarios should address each of the resources described above. The following are *examples* of some of the types of questions that contingency scenarios may address:

Human Resources: Can people get to work? Are key personnel willing to cross a picket line? Are there critical skills and knowledge possessed by one person? Can people easily get to an alternative site?

Processing Capability: Are the computers harmed? What happens if some of the computers are inoperable, but not all?

Automated Applications and Data: Has data integrity been affected? Is an application sabotaged? Can an application run on a different processing platform?

Computer-Based Services: Can the computers communicate? To where? Can people communicate? Are information services down? For how long?

Infrastructure: Do people have a place to sit? Do they have equipment to do their jobs? Can they occupy the building?

Documents/Paper: Can needed records be found? Are they readable?

11.4 Step 4: Selecting Contingency Planning Strategies

The next step is to plan how to recover needed resources. In evaluating alternatives, it is necessary to consider what controls are in place to prevent and minimize contingencies. Since no set of controls can cost-effectively prevent all contingencies, it is necessary to coordinate prevention and recovery efforts.

A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption.[89] *Emergency response* encompasses the initial actions taken to protect lives and limit damage. *Recovery* refers to the steps that are taken to continue support for critical functions. *Resumption* is the return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the organization will have to operate in the recovery mode.

---

[89] Some organizations divide a contingency strategy into emergency response, backup operations, and recovery. The different terminology can be confusing (especially the use of conflicting definitions of *recovery*), although the basic functions performed are the same.

[redacted]

The selection of a strategy needs to be based on practical considerations, including feasibility and cost. The different categories of resources should each be considered. Risk assessment can be used to help estimate the cost of options to decide on an optimal strategy. For example, is it more expensive to purchase and maintain a generator or to move processing to an alternate site, considering the likelihood of losing electrical power for various lengths of time? Are the consequences of a loss of computer-related resources sufficiently high to warrant the cost of various recovery strategies? The risk assessment should focus on areas where it is not clear which strategy is the best.

In developing contingency planning strategies, there are many factors to consider in addressing each of the resources that support critical functions. Some examples are presented in the sidebars.

11.4.1 Human Resources

To ensure an organization has access to workers with the right skills and knowledge, training and documentation of knowledge are needed. During a major contingency, people will be under significant stress and may panic. If the contingency is a regional disaster, their first concerns will probably be their family and property. In addition, many people will be either unwilling or unable to come to work. Additional hiring or temporary services can be used. The use of additional personnel may introduce security vulnerabilities.

Contingency planning, especially for emergency response, normally places the highest emphasis on the protection of human life.

11.4.2 Processing Capability

Strategies for processing capability are normally grouped into five categories: hot site; cold site; redundancy; reciprocal agreements; and hybrids. These terms originated with recovery strategies for data centers but can be applied to other platforms.

1. *Hot site* – A building already equipped with processing capability and other services.

2. *Cold site* – A building for housing processors that can be easily adapted for use.

3. *Redundant site* – A site equipped and configured exactly like the primary site. (Some organizations plan on having reduced processing capability after a disaster and use partial redundancy. The stocking of spare personal computers or LAN servers also provides some redundancy.)

4. *Reciprocal agreement* – An agreement that allows two organizations to back each other up. (While this approach often sounds desirable, contingency planning experts note that this alternative has the greatest chance of failure due to problems keeping agreements and plans up-to-date as systems and personnel change.)

5. *Hybrids* – Any combinations of the above such as using having a hot site as a backup in case a redundant or reciprocal agreement site is damaged by a separate contingency.

Recovery may include several stages, perhaps marked by increasing availability of processing capability. Resumption planning may include contracts or the ability to place contracts to replace equipment.

11.4.3 Automated Applications and Data

Normally, the primary contingency strategy for applications and data is *regular backup* and secure *offsite storage*. Important decisions to be addressed include how often the backup is performed, how often it is stored off-site, and how it is transported (to storage, to an alternate processing site, or to support the resumption of normal operations).

[redacted]

11.4.4 Computer-Based Services

Service providers may offer contingency services. Voice communications carriers often can reroute calls (transparently to the user) to a new location. Data communications carriers can also reroute traffic. Hot sites are usually capable of receiving data and voice communications. If one service provider is down, it may be possible to use another. However, the type of communications carrier lost, either local or long distance, is important. Local voice service may be carried on cellular. Local data communications, especially for large volumes, is normally more difficult. In addition, resuming normal operations may require another rerouting of communications services.

11.4.5 Physical Infrastructure

Hot sites and cold sites may also offer office space in addition to processing capability support. Other types of contractual arrangements can be made for office space, security services, furniture, and more in the event of a contingency. If the contingency plan calls for moving offsite, procedures need to be developed to ensure a smooth transition back to the primary operating facility or to a new facility. Protection of the physical infrastructure is normally an important part of the emergency response plan, such as use of fire extinguishers or protecting equipment from water damage.

11.4.6 Documents and Papers

The primary contingency strategy is usually backup onto magnetic, optical, microfiche, paper, or other medium and offsite storage. Paper documents are generally harder to backup than electronic ones. A supply of forms and other needed papers can be stored offsite.

11.5 Step 5: Implementing the Contingency Strategies

Once the contingency planning strategies have been selected, it is necessary to make appropriate preparations, document the strategies, and train employees. Many of these tasks are ongoing.

11.5.1 Implementation

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, *if* the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability.

It is important to keep preparations, including documentation, up-to-date. Computer systems change rapidly and so should backup services and redundant equipment. Contracts and agreements may also need to reflect the

[redacted]

changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization's architecture.

Preparation should also include formally designating people who are responsible for various tasks in the event of a contingency. These people are often referred to as the contingency response team. This team is often composed of people who were a part of the contingency planning team.

There are many important implementation issues for an organization. Two of the most important are 1) how many plans should be developed? and 2) who prepares each plan? Both of these questions revolve around the organization's overall strategy for contingency planning. The answers should be documented in organization policy and procedures.

How Many Plans?

Some organizations have just one plan for the entire organization, and others have a plan for every distinct computer system, application, or other resource. Other approaches recommend a plan for each business or mission function, with separate plans, as needed, for critical resources.

The answer to the question, therefore, depends upon the unique circumstances for each organization. But it is critical to coordinate between resource managers and functional managers who are responsible for the mission or business.

[redacted]

Who Prepares the Plan?

If an organization decides on a centralized approach to contingency planning, it may be best to name a *contingency planning coordinator*. The coordinator prepares the plans in cooperation with various functional and resource managers. Some organizations place responsibility directly with the functional and resource managers.

11.5.2 Documenting

The contingency plan needs to be written, kept up-to-date as the system and other factors change, and stored in a safe place. A written plan is critical during a contingency, especially if the person who developed the plan is unavailable. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge could immediately begin to execute the plan. It is generally helpful to store up-to-date copies of the contingency plan in several locations, including any off-site locations, such as alternate processing sites or backup data storage facilities.

11.5.3 Training

All personnel should be trained in their contingency-related duties. New personnel should be trained as they join the organization, refresher training may be needed, and personnel will need to practice their skills.

Training is particularly important for effective employee response during emergencies. There is no time to check a manual to determine correct procedures if there is a fire. Depending on the nature of the emergency, there may or may not be time to protect equipment and other assets. Practice is necessary in order to react correctly, especially when human safety is involved.

11.6 Step 6: Testing and Revising

[redacted]

A contingency plan should be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become dated as time passes and as the resources used to support critical functions change. Responsibility for keeping the contingency plan current should be specifically assigned. The extent and frequency of testing will vary between organizations and among systems. There are several types of testing, including reviews, analyses, and simulations of disasters.

A *review* can be a simple test to check the accuracy of contingency plan documentation. For instance, a reviewer could check if individuals listed are still in the organization and still have the responsibilities that caused them to be included in the plan. This test can check home and work telephone numbers, organizational codes, and building and room numbers. The review can determine if files can be restored from backup tapes or if employees know emergency procedures.

[redacted]

An *analysis* may be performed on the entire plan or portions of it, such as emergency response procedures. It is beneficial if the analysis is performed by someone who did *not* help develop the contingency plan but has a good working knowledge of the critical function and supporting resources. The analyst(s) may mentally follow the strategies in the contingency plan, looking for flaws in the logic or process used by the plan's developers. The analyst may also interview functional managers, resource managers, and their staff to uncover missing or unworkable pieces of the plan.

Organizations may also arrange *disaster simulations*. These tests provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can also provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost-beneficial it is to perform a disaster simulation.

11.7 Interdependencies

Since all controls help to prevent contingencies, there is an interdependency with all of the controls in the handbook.

Risk Management provides a tool for analyzing the security costs and benefits of various contingency planning options. In addition, a risk management effort can be used to help identify critical resources needed to support the organization and the likely threat to those resources. It is not necessary, however, to perform a risk assessment prior to contingency planning, since the identification of critical resources can be performed during the contingency planning process itself.

Physical and Environmental Controls help prevent contingencies. Although many of the other controls, such as logical access controls, also prevent contingencies, the major threats that a contingency plan addresses are physical and environmental threats, such as fires, loss of power, plumbing breaks, or natural disasters.

Incident Handling can be viewed as a subset of contingency planning. It is the emergency response capability for various technical threats. Incident handling can also help an organization prevent future incidents.

Support and Operations in most organizations includes the periodic backing up of files. It also includes the prevention and recovery from more common contingencies, such as a disk failure or corrupted data files.

Policy is needed to create and document the organization's approach to contingency planning. The policy should explicitly assign responsibilities.

11.8 Cost Considerations

The cost of developing and implementing contingency planning strategies can be significant, especially if the strategy includes contracts for backup services or duplicate equipment. There are too many options to discuss cost considerations for each type.

One contingency cost that is often overlooked is the cost of testing a plan. Testing provides many benefits and should be performed, although some of the less expensive methods (such as a review) may be sufficient for less critical resources.

References

Alexander, M. ed. "Guarding Against Computer Calamity." *Infosecurity News*. 4(6), 1993. pp. 26-37.

Coleman, R. "Six Steps to Disaster Recovery." *Security Management*. 37(2), 1993. pp. 61-62.

Dykman, C., and C. Davis, eds. *Control Objectives - Controls in an Information Systems Environment: Objectives, Guidelines, and Audit Procedures*, fourth edition. Carol Stream, IL: The EDP Auditors Foundation, Inc., 1992 (especially Chapter 3.5).

Fites, P., and M. Kratz, *Information Systems Security: A Practitioner's Reference*. New York, NY: Van Nostrand Reinhold, 1993 (esp. Chapter 4, pp. 95-112).

FitzGerald, J. "Risk Ranking Contingency Plan Alternatives." *Information Executive*. 3(4), 1990. pp. 61-63.

Helsing, C. "Business Impact Assessment." *ISSA Access*. 5(3), 1992, pp. 10-12.

Isaac, I. *Guide on Selecting ADP Backup Process Alternatives*. Special Publication 500-124. Gaithersburg, MD: National Bureau of Standards, November 1985.

Kabak, I., and T. Beam, "On the Frequency and Scope of Backups." *Information Executive*, 4(2), 1991. pp. 58-62.

Kay, R. "What's Hot at Hotsites?" *Infosecurity News*. 4(5), 1993. pp. 48-52.

Lainhart, J., and M. Donahue. *Computerized Information Systems (CIS) Audit Manual: A Guideline to CIS Auditing in Governmental Organizations*. Carol Stream, IL: The EDP Auditors Foundation Inc., 1992.

National Bureau of Standards. *Guidelines for ADP Contingency Planning*. Federal Information Processing Standard 87. 1981.

Rhode, R., and J. Haskett. "Disaster Recovery Planning for Academic Computing Centers."