Part II
Management Controls

Overview of Part II

This Handbook has divided security topics into three broad areas: management, operational, and technical, with the recognition that the various topics and controls rely upon each other in meeting their security objectives.

This section addresses security topics that can be characterized as managerial. They are techniques and concerns that must be addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization. The areas discussed here are not, in general, specific to a particular system -- as is seen with operational and technical controls.

This section of the Handbook addresses following computer security activities:

- Computer and Information Security Policy
- Security Program Management and Administration
- Risk Management
- Security in the System Life Cycle
- Assurance

Policy is the foundation of a computer security program. It is senior management's direction to create a security program, establish its goals, and assign responsibilities. Policy indicates management's (and consequently the organization's) commitment to security. In the Policy chapter, we discuss the different types of policy, their components, and how each documents important managerial decisions regarding the protection of system resources.

Having established the program through policy, management then directs its focus to program management and administration. The Security Program Management chapter presents an organization-wide approach to security. It discusses the structure of a security program, at both the centralized and system level.

The policy that management approves and the program that it establishes exist, fundamentally, to manage risk within the organization. Use of computers by an organization can increase or decrease overall risk. Risk, however, can never be totally eliminated. Therefore, it falls upon management's shoulders to manage risk. The Risk Management chapter discusses how that is done. This chapter discusses the two major benefits of risk management: measurement of risk and mitigating it through the selection of cost-effective controls.

The next chapter, rather than taking an organization-wide approach, discusses security and the management of risk from a system-specific point of view. The chapter, Security in the Computer System Life Cycle, examines the importance of addressing security at each stage of the life of a system -- from its initial design and requirements stages through its operation and, finally, its disposal. The chapter discusses the cost effectiveness of addressing security

early in the development of a system. It also discusses the many security-relevant decisions and analyses that happen during a system's life -- and how they fit together.

Assurance is the final topic considered in this section. Security assurance is the degree of confidence one has that security measures function as intended to protect the system. While assurance is often thought of as very technical (because of extensive, technical testing sometimes associated with obtaining it), assurance is actually more closely related to the topic of risk management -- for specific systems and their components. Assurance is closely linked to the process of accreditation, that is, the approval by management of a system to operate, a risk management function. The chapter discusses what assurance is and ways that it is obtained.

5 Computer and Information Security Policy

5.1 Introduction to Computer Security Policy

In the computer security context, the term "policy" means things. Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. It is also the specific rules established by the guardian of the system which are enforced by a system's technical controls as well as management and operational controls. In addition, policy may refer to entirely different matters, such as an organization's e-mail privacy policy or its policy for contingency planning.

Policy documents managerial decisions.

What all of these types of policy have in common is that they document and describe decisions taken by management. In making these decisions, managers face hard choices involving resource allocation, competing objectives, and organizational strategy related to protecting both technical and information resources as well as guiding employee behavior. Managers at all levels make choices that can result in policy, with the scope of the policy's applicability varying according to the scope of the manager's authority. In this chapter we use the term *policy* in a broad manner to encompass all of the types of policy described above -- regardless of the level of manager who sets the particular policy.

This chapter discusses four types of computer security policy:

program-level
program-framework
issue-specific, and
system-specific.

Managerial decisions on computer security issues vary greatly. In this chapter we have categorized them into four basic types of policy, which are discussed along with their components. *Program-level policy* is used to create an organization's computer security program. *Program-framework policy* establishes the organization's overall approach to computer security (i.e., its computer security framework). *Issue-specific policies* address specific issues of concern to the organization. Lastly, *system-specific policies* focus on decisions taken by management for a particular system.

Familiarity with various types of policy will aid managers in addressing computer security issues important to the organization. A comparison of an organization's computer security policies to the types described in this chapter will help provide management with an indication of the appropriateness and comprehensiveness of its policies. Effective policies ultimately result in the development and implementation of a better computer security program and better protection of systems and information.

5.2 The Four Types of Policy

Four types of policy will typically need to be developed to meet an organization's needs: *program-level, program-framework, issue-specific* and *system-specific*. Management uses program-level policy to:

- establish the security program,
- assign program management responsibilities,
- state organization-wide computer security purpose and objectives,
- provide a basis for compliance, and
- provide organization-wide direction on broad areas of program implementation.

Program-framework policies are made to:

- establish an organization's approach to implementing the important elements of a computer security program,
- specify management's decisions on those aspects of computer security where organization-wide oversight is necessary, and
- realize cost savings available through organization-wide implementation.

Issue-specific policies also need to be developed in order to:

- identify and define specific areas of concern,
- document management's decisions on the issue, and
- state the organization's position and expectations in relation to them.

Finally, policies are often needed to address issues specific to a certain system.[35] System-specific policies are developed and issued to:

- state the detailed security objectives of a specific system.

Program-level policy is typically issued by the head of the organization or another senior official, such as the top management officer. Program-framework policy may be issued by the computer security program manager, the IRM official, or another appropriate official. In general, for issue-specific and system-specific policy, the issuer is a senior official; the more global, controversial, or resource-intensive, the more senior the issuer.

Following are discussions of these four basic types of policy.

---

[35] A system refers to the entire collection of processes, both those performed manually and those using a computer (e.g., manual data collection and subsequent computer manipulation), which performs a function. This includes both application systems and support systems, such as a network.

5.2.1 Program-level Policy

Program-level policy is issued by management to *establish* its computer security program and its basic structure.

> Program-level policy establishes the security program and assigns program management and supporting responsibilities.

A management official, normally the head of the organization or the top-level management official, issues program-level policy to establish (or restructure) the organization's computer security program. This high-level policy defines the purpose of the program, its scope within the organization, assigns responsibilities for direct program implementation (to the computer security organization) as well as responsibilities to related offices (such as the IRM organization) and addresses compliance issues. The policy sets organizational strategic directions for security and assigns resources for its implementation. Components of program-level policy should include:

Purpose: Program policy establishes the organization computer security program. This includes defining the *goals* of the computer security program as well as its *management structure*. Security-related needs, such as integrity, availability, and confidentiality, can form the basis of organizational goals established in policy. For instance, in an organization responsible for maintaining large mission-critical databases, reduction in errors, data loss, or data corruption might be specifically stressed. In an organization responsible for maintaining confidential personal data, however, goals might emphasize stronger protection against unauthorized disclosure.

The program management structure should be organized to best address the goals of the program and respond to the particular operating and risk environment of the organization. Important issues for the structure of the computer security program include management and coordination of security-related resources, interaction with diverse communities, and the ability to relay issues of concern to upper management. The policy could also establish operational security offices for major systems, particularly those at high risk or most critical to organizational operations. (See the chapter on security program management and administration.)

Scope: Program-level policy should be clear as to which resources, (including facilities, hardware, and software) information, and personnel the program covers. In many cases, the program will encompass all systems and agency personnel, but this is not always true. In some instances, it may be appropriate for a policy to name specific assets, such as major sites and large systems.

Responsibilities: As noted in the earlier discussion of purpose, program-level policy performs the important function of establishing the computer security program and assigning program management responsibilities. In addition to the security program management responsibilities, the responsibilities of officials and offices throughout the organization must be addressed.

This includes the role of line managers, applications owners, users, and the data processing or IRM organization. This section of the policy statement, for example, would distinguish between the responsibilities of computer services providers and those of the mangers of applications using the provided services. It also can serve as the basis for establishing employee accountability, as discussed in "Compliance" below.

Overall, the program-level assignment of responsibilities should cover those activities and personnel who will be integral to the implementation and continuity of the computer security policy.

Compliance: Program-level policy typically will address two compliance issues. The first is general compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organization components. Often an oversight office (e.g., the Inspector General) is assigned responsibility for monitoring compliance including how well the organization is implementing management's priorities for the program. Secondly, program-level policy normally will also authorize the use of specified penalties and disciplinary actions for individuals who fail to comply with the organization's computer security policies. Since the security policy is a high level document, specific penalties for various infractions are normally not detailed here. However, the policy may authorize the creation of compliance structures which include violations and specific disciplinary action(s).[36]

When developing compliance policy, consideration should be given to the fact that violations of policy can be unintentional on the part of employees. For example, nonconformance can often be due to a lack of knowledge or training.

5.2.2 Program-framework Policy

Program-framework policy defines the organization's security program elements which form the framework for the computer security program and reflect decisions about priorities for protection, resource allocation, and assignment of responsibilities.

As introduced earlier, criteria for the types of areas to be addressed in the program-framework policy include, (but are not limited to):

- areas which need to be addressed for the entire organization;
- areas for which organization-wide oversight is necessary;
- areas which, through organization-wide implementation, can yield significant

[36] It is not necessary, however, to detail penalties already provided for by law, although they can be listed if the policy will also be used as a awareness or training document.

economies of scale; and

- areas for which there is some other advantage to the organization by having the issue addressed in a common manner.

The types of areas addressed by program-framework policy vary within each organization as does the way in which the policy is expressed. Some organizations issue policy directives, while others issue handbooks which include policy, regulations, standards, and guidance. (See sidebar discussion.) Many organizations develop policy on "key" areas of computer security, such as life cycle management, contingency planning, or network security.

It is important to keep in mind the criteria stated above for the types of areas that should be addressed in program-framework policy. If the policy (and its implementing standards and guidance) is too rigid, it could stifle cost-effective implementations and innovation.

As an example of program-framework policy, consider a typical organization policy on contingency planning. The organization might require that all contingency plans categorize criticality of processing according to a standard scale. This will assist the organization in the preparation of a master plan (for use if the organization's physical plant is destroyed) by facilitating prioritization across intra-organizational boundaries.

Policy in these areas normally applies throughout the organization and is usually independent of technology and the system or application. Program-framework policies may be comprised of components similar to those contained in program-level policy (i.e., purpose, scope, responsibilities, and compliance) -- but, because they address a wide variety of major elements may be in a very different format (e.g., in organizational handbook directives).

5.2.3 Issue-specific Policy

Issue-specific policies document management decisions in addressing particular activities, applications, systems, or technologies.

Whereas program-level and program-framework policy are intended to address broad aspects of computer security, issue-specific policies are developed to focus on areas of current relevance and concern (and sometimes controversy) to an organization. Management may find it appropriate, for example, to issue a policy on the appropriate use of a cutting-edge technology (whose security vulnerabilities are still largely unknown) within the organization. Issue-specific policies may also be appropriate when new issues arise, such as when implementing a recently-passed law requiring additional protection of particular information. Program-level policy is usually broad enough that it does not require much modification over time whereas issue-specific policies are likely to require more frequent revision as changes in technology and related factors take place. This is largely because as new technologies develop, some issues diminish in importance while new ones continually appear.

There are many areas for which issue-specific policy is appropriate. Two examples are explained below.

Both new technologies and the appearance of new issues often require the creation of issue-specific policies.

Example #1 - Internet Access: Many organizations are looking at the Internet as a means for expanding their research opportunities and communications. Unquestionably, there are many benefits offered by connecting to the Internet -- and some disadvantages. An Internet access policy may address who will have access, which types of systems may be connected to the network, what types of information may be transmitted via the network, additional requirements for user authentication for Internet-connected systems, and use of firewalls and trusted gateways, among others.

Example #2 - E-Mail Privacy: Users of computer e-mail systems have come to rely upon that service for informal communication with colleagues and others. However, since the system is typically owned by the employing organization, management may wish, from time-to-time, to monitor the employee's e-mail (e.g., if they are suspected of distributing viruses, sending offensive e-mail, or disclosing organizational secrets.) On the other hand, users may have an expectation of privacy, similar to that accorded U.S. mail. Policy in this area may address what level of privacy will be accorded e-mail and the circumstances under which it may or may not be read.

As suggested for program-level policy, a useful structure for issue-specific policy is to break the policy into its basic components, including the following:

Issue Statement: In order to formulate a policy on an issue, the issue must first be defined, with any relevant terms, distinctions, and conditions included. This section may also be used to state the goal or justification for the policy -- which can be helpful in gaining compliance with the policy. For example, an organization might want to develop an issue-specific policy on the use of "unofficial software," which might be defined to mean any software not approved, purchased, screened, managed, and owned by the organization. Additionally, the applicable distinctions and conditions might then need to be included, for instance, for software privately owned by employees but approved for use at work, and for software owned and used by other businesses under contract to the organization.

Besides the two examples presented, other potential candidates for issue-specific policies include: use of e-mail, protection of confidential/proprietary information communicated using e-mail, unauthorized software, acquisition of software, doing computer work at home, bringing in disks from outside the workplace, access to other employees' files, encryption of files and e-mail, rights of privacy, responsibility for correctness of data, suspected malicious code, and physical emergencies. This list is not all-inclusive nor meant to imply policies in each of these areas are required by all organizations.

Statement of the Organization's Position: Once the issue is stated and related terms and

conditions discussed, this section is used to clearly state the organization's position or stance (i.e., its decision) on the issue. To continue the example of developing an issue-specific policy on the use of unofficial software, this would mean stating whether use of unofficial software as defined is prohibited in all or some cases, whether or not there are further guidelines for approval and use, or whether case-by-case exceptions will be granted, by whom, and on what basis.

Applicability: Issue-specific policies also need to include statements of applicability. This means clarifying where, how, when, to whom, and to what a particular policy applies. For example, it could be that the hypothetical policy on unofficial software is intended to apply only to the organization's own on-site resources and employees and is not to be applicable to contractor organizations with offices at other locations. Additionally, the policy's applicability to employees travelling among different sites and/or working at home who need to transport and use disks at multiple sites might need to be clarified.

Roles and Responsibilities: Also usually included in issue-specific policies is the assignment of roles and responsibilities. This would mean, to continue the above example, that if the policy permits unofficial software privately owned by employees to be used at work with the appropriate approvals, then the approval authority granting such permission would need to be stated. Likewise, it would need to be clarified who would be responsible for ensuring that only approved software is used on organizational computer resources and, perhaps, for monitoring users in regard to unofficial software.

Some Helpful Hints on Policy

To be effective, policy requires visibility. Visibility aids implementation of policy by helping to ensure that knowledge of the policy is diffused throughout the organization. Management presentations, videos, panel discussions, guest speakers, question/answer forums, and newsletters, increase visibility. The organization's computer security training and awareness program can effectively notify users of new policies. It also provides new employees with necessary familiarity with the organization's policies.

Introduce computer security policies in a manner that ensures that management's unqualified support is clear, especially in environments where employees feel inundated with policies, directives, guidelines, and procedures. The organization's policy is the vehicle for emphasizing management's commitment to computer security and making clear their expectations for employee performance, behavior, and accountability.

Computer security policy should also be integrated into and consistent with other organizational policies (e.g., personnel policies). One way to help ensure this is to coordinate policies during development with other organizational offices.

Related to the assignment of roles and responsibilities is the inclusion of guidelines for procedures and compliance. The issue-specific policy on unofficial-software, for example, might include procedural guidelines for checking disks brought to work which had been used by employees at other locations.

Compliance: In dealing with compliance for issue-specific policy, it is generally appropriate

to describe, in some detail, the infractions which are unacceptable -- and state the respective penalizes. Penalties must be consistent with organizational personnel policies and practices and will need to be coordinated with appropriate officials and offices and, perhaps, employee bargaining units. It may also be desirable to task a specific office within the organization to monitor compliance.

Points of Contact and Supplementary Information: For any issue-specific policy, the appropriate individuals in the organization to contact for further information, guidance, and compliance should be indicated. Note that while the term "points of contact" could refer to either individual people or positions; however, since positions tend to change less often than the people occupying them, positions may be preferable. For example, for some issues the point of contact might be a line manager; for other issues it might be a facility manager, technical support person, or system administrator. For yet other issues, the point-of-contact might be a security program representative. Using the above example once more, employees would need to know whether the point of contact for questions and procedural information would be their immediate superior, a system administrator, or a computer security official.

5.2.4 System-Specific Policy

System-specific security policy includes two components: security objectives and operational security rules. It is closely tied to, and often difficult to separate from, system-specific policy implementation.

Program-level policy and issue-specific policy both address policy from a broad level, usually encompassing the entire organization. However, they do not provide sufficient details, for example, to be used in establishing an access control list. System-specific policy fills this need, drawing upon the more expansive program-level and program-framework policies. It is much more focused, since it addresses only one system.

There are many security policy decisions that may apply only at the system level -- and may vary from system to system within the same organization. While these decisions may appear to be too detailed to be policy, they can be extremely important with significant impacts on system usage and security. These types of decisions should be made by a *management official*, not by a technical system administrator. (Analysis of the impacts of these decisions, however, are often made by technical system administrators.) Some examples include:

- Who is allowed to read or modify data in the system?
- Under what conditions can data be read or modified?
- Are users allowed to dial into the computer system from home or while on travel?

In order to develop a cohesive and comprehensive set of security policies, a management process which derives security rules from security goals should be used. It is helpful to consider a two level model for system security policy: security objectives and operational

security rules, which together comprise the system-specific policy. Closely linked and often difficult to distinguish, however, is the implementation of the policy in technology.

5.2.4.1 Security Objectives

> Example of an objective: Only individuals in the accounting and personnel departments are authorized to provide or modify information used in payroll processing.

The first step in the management process is to define security objectives for the specific system. Although, this process may start with an analysis of the need for integrity, availability, and confidentiality, it cannot stop there. A security *objective* must be more specific; it should be concrete and well-defined. It also should be stated so that it is clear that the objective is achievable. This process will also draw upon other applicable organization policies, including program-level, program-framework, and issue-specific.

The security objectives should consist of a series of statements which describe meaningful actions about explicit resources. These objectives should be based on system functional or mission requirements, but should state the security actions which support the requirements.

5.2.4.2 Operational Security Rules

After management determines the security objectives, the rules for operating a system can be laid out. These rules, for example, would define authorized and unauthorized modification. Who, (by job category, by organization placement, or by name) can do what (e.g., modify, delete) to which specific classes and records of data, and under what conditions.

> Example: Personnel clerks can update fields for weekly attendance, charges to annual leave, employee addresses, and telephone numbers. Personnel specialists can update salary information. No one can update their own records.

Development of system-specific policy will require management to make decisions since it is unlikely that all desired security objectives will be able to be fully met. Management will face cost, operational, technical, and other constraints.

The degree of specificity needed for operational security rules varies greatly. The more detailed the rules are, *up to a point*, the easier it is to know when one has been violated. It is also, *up to a point*, easier to automate policy enforcement. However, overly detailed rules may make the job of instructing a computer to implement them difficult or impossible.

In addition to deciding the level of detail, management must also decide the degree of formality in documenting the system-specific policy. Once again, the more formal the documentation, the easier it is to enforce and to follow policy.

On the other hand, very detailed and formal policy at the system level can also be an administrative burden. In general, good practice suggests a detailed formal statement of the access privileges for a system. The reason for this area being highlighted is its complexity and its importance. Documenting access controls policy will make it substantially easier to follow and to enforce. (See the chapters on Personnel/user issues and Access Controls.) Areas which normally require a detailed and formal statement is the assignment of security responsibilities.

Policy decisions in other areas of computer security, such as those described in this Handbook, are often documented in the risk analysis, accreditation statements, or procedural manuals. However, any controversial, atypical or uncommon policies will also need formal statements. Atypical policies would include any areas where the system policy is different from organization policy or from normal practice within the organization, either more or less stringent. The documentation for a typical policy contains a statement explaining the reason for deviation from the organization's standard policy.

5.2.4.3 System-specific Policy Implementation

Technology plays an important -- but not sole -- role in enforcing system-specific policies. When technology is used to enforce policy, it is important not to neglect non-technology based methods. Technical system-based controls may limit, for example, the printing of confidential reports to a particular printer. However, corresponding physical security measures must be in place to limit access to the printer output or the desired security objective will not be achieved.

Technical methods frequently used to implement system-security policy are likely to include the use of *access controls*. However, there are other automated means of enforcing or supporting security policy that typically supplement access controls. For example, technology can be used to block telephone systems users from calling certain numbers. Intrusion detection software can alert system administrators to suspicious activity or take action to stop the activity. Personal computers can be configured to prevent booting from a floppy disk.

Technology-based enforcement of system-security policy has advantages and disadvantages. A computer system, properly designed, programmed, installed, configured, and maintained[37] consistently enforces policy within the computer system, although no computer can force users to follow all procedures. Management controls also play an important role -- and must not be neglected. In addition, deviations from the policy may sometimes be necessary and appropriate; such deviations may be difficult to implement easily with some technical controls. This situation occurs frequently if the security policy is too rigid.

[37]Doing all of these things properly is, unfortunately, the exception rather than the rule. Confidence in the system's ability to enforce system-specific policy is closely tied to assurance. (See the chapter on assurance.)

5.3 Interdependencies

Policy is related to many of the topics covered in this handbook. Policy is used to establish an organization's computer security program, and is therefore closely tied to program management and administration. Both program-level and system-specific policy may be established in any of the areas covered in this Handbook. For example, an organization may wish to have a consistent approach to incident handling for all its systems -- and would issue appropriate program-level policy to do so. On the other hand, it may decide that its applications are sufficiently independent of each other that application managers should deal with incidents on an individual basis.

This chapter has focused on the types and components of computer security policy; however, it is important to realize that *computer* security policies are often *extensions* of an organization's *information* security policies for handling information in other forms (e.g., paper documents). For example, an organization's e-mail policy would probably be tied to its broader policy on privacy of other forms of information about or belonging to employees. They may also be extensions of other policies, such as those about appropriate use of equipment and facilities.

5.4 Cost Considerations

There are a number of potential costs associated with developing and implementing computer security policies. Overall, the major cost of policy is the impact of the management decision which the policy documents. For example, the establishment of a computer security program, accomplished through policy, does not come at negligible cost.

Other costs may be those incurred through the policy development process. Numerous administrative and management activities may be required for drafting, reviewing, coordinating, clearing, disseminating, and publicizing policies. In many organizations successful policy implementation may require additional staffing and training -- and can take time. In general, the costs of computer security policy development and implementation to an organization will depend upon how much change needs to be accomplished in order to achieve a level of risk acceptable to management.

5.5 Summary

Formulating viable computer security policies is a challenge for an organization and requires communication and understanding of the organizational goals and potential benefits to be derived from policies. Through a carefully structured approach to policy development, which includes the delegation of program management responsibility and an understanding of program-level, program-framework, issue-specific, and system-specific policy components, an organization can reach a coherent set of policies. These will help realize a successful computer security program.

5.6 References

Howe, D. "Information System Security Engineering: Conerstone to the Future." *Proceedings of the 15th National Computer Security Conference*. Vol 1, 1992, pp. 244-251.

Lobel, J. "Establishing a System Security Policy." *Foiling the System Breakers*. New York: McGraw-Hill, 1986, pp. 57-95.

"Major Trends in Policy Development." *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, Office of Technology Assessment, U.S.Congres. 1987, p. 131-148.

Menkus, B. "Concerns in Computer Security." *Computers and Security*. 11(3), 1992. pp. 211-215.

O'Neill, M. and F. Henninge,Jr., "Understanding ADP System and Network Security Considerations and Risk Analysis." *ISSA Access*. 5(4), 1992. pp. 14-17.

Peltier, Thomas. "Designing Information Security Policies That Get Results." *Infosecurity News*. 4(2), 1993. pp. 30-31.

Smith, J. "Privacy Policies and Practices: Inside the Organizational Maze." *Communications of the ACM*. 36(12), 1993. pp. 104-120.

Sterne, Daniel. "On the Buzzword Computer Security Policy."

"Federal Policy Issues and Options." *Defending Secrets, Sharing Data: New Locks for Electronic Information*. Office of Technology Assessment, U.S.Congress. 1987, pp. 151-160.

6 Security Program Management

6.1 Purpose of Security Program Management

Computers and the information they process are a critical to many organizations' ability to perform their mission and business functions. Therefore, organizations should view information resources security as a management issue, treated like any other item of strategic importance. The purpose of a security program is to protect these vital assets. Accordingly, ensuring security requires the development of a comprehensive management approach.

The purpose of this chapter is to present security as a management function. An organization-wide approach to security program management is presented.[38] Because organizations differ vastly in size, complexity, management styles, and culture, it is not possible to describe one ideal security program. However, this chapter does describe some of the features and issues common to many organizations.

> OMB Circular A-130, "Management of Federal Information Resources," requires that federal agencies establish computer security programs.

6.2 Structure of a Security Program

Many organizations have security programs which are distributed throughout the organization with different elements performing different functions. While this is a desirable management structure, the distribution of the security function in many organizations is haphazard, based on chance. Ideally, the distribution of security functions should result from a planned and integrated management philosophy.

Figure 5-1 shows a management structure based on that of an actual Federal agency. The agency consists of five major units, each with several large computer facilities running multiple applications. This type of organization needs to manage security at the *agency* level, the *unit* level, the *computer facility* level, and the *application* level.

Managing computer security at multiple levels brings many benefits. Each level contributes to the overall security program with different types of expertise, authority and resources. In general, the higher levels (such as the headquarters or unit levels in the Agency described above) better understand the organization as a whole and exercise more authority. On the

[38] Note: This chapter addresses security program management, not the various activities such as risk analysis or contingency planning that make up an effective security program.

other hand, the lower levels (the computer facility and applications levels) are more familiar with the requirements, both technical and procedural, and problems of the systems and the users. The levels of security program management should be complementary; each can help the other be more effective.

Since many organizations have at least two level of security management, this chapter divides security program management into two levels: the *central* level and the *system* level. (Each organization, though, may have its own unique structure.) The central security program address the overall management of security within an organization or a major component of an organization. The system level security program addresses the management of security for a particular information processing system. Many organizations have *at least* these two levels and many organizations, such as the example above, have several more.

6.3 Central Program

The purpose of a *central security* program, as stated above, is the overall management of security within an organization. In the federal government, the organization could consist of a department, agency, installation or other major operating unit.

Two benefits of a central security program should be 1) increased economy and efficiency and 2) better enforcement and oversight.

A central security program provides two quite distinct types of benefits. The first type is increased efficiency and economy of security throughout the organization. The second type is the ability to provide enforcement and oversight. Both of these benefits are in keeping with the purpose of the Paperwork Reduction Act, as implemented in OMB Circular A-130.

> The Paperwork Reduction Act establishes a broad mandate for agencies to perform their information management activities in an efficient, effective, and economical manner.... Agencies shall assure an adequate level of security for all agency automated information systems, whether maintained in-house or commercially. (A-130, Section 5; Appendix III, Section 3.)

As with the management of all resources, central security management can be performed in many ways. The importance of sound management cannot be overemphasized.

6.3.1 Efficiency and Economy

A central security program can manage or coordinate the use of security-related resources across the entire organization. The most important of these resources are normally *information* and *financial resources*.

It is a truism to discuss both the overload of information available to modern managers and the utility of well-managed information. Most organizations, however, have trouble collecting information from myriad sources and effectively processing and distributing it within the organization. This section discusses some of the sources and uses of security *information*.

Within the Federal government, many organizations such as the Office of Management and Budget, the General Services Administration, the National Institute of Standards and Technology, and the National Telecommunications and Information Administration provide information on computer, telecommunications, or information resources. This information includes security-related policy, regulations, standards, and guidance. A portion of the information is channelled through the senior designated official for each agency (see FIRMR Part 201-2). Agencies are expected to have mechanisms in place to distribute information received by the senior designated official.

Security-related information is also available from private and Federal professional societies

and groups. These groups will often provide the information as a public service, although some private groups charge for it. However, even for information that is free or inexpensive, the costs associated with personnel gathering the information can be expensive. For instance, it is obvious that it is not cost effective for an organization to send *everyone* to *every* security conference.

Internal security-related information, such as which procedures were effective, virus infections, security problems and solutions need to be shared within an organization. Often this information is specific to the operating environment and culture of the organization.

A security program at the organization level can provide a way to collect the internal security-related information and distribute it as needed throughout the organization. Sometimes an organization can also share this information with external groups. Figure 5-2 shows a simplified version of this flow of information. For example, in many organizations, external interaction occurs at both the organization and system levels. However, the central security program should be aware of the interaction at the system level to aid in the sharing of information and to make sure that the organization has identified and utilized all important sources.

Figure 6-2

Another use of an effective conduit of information is to increase the central security program's ability to influence external and internal policy decisions. If the central security program office can represent the entire organization, then it is more likely to be listened to by upper management and external organizations. However, to be effective, there must be excellent communication between the system level security programs and the organization level. For example, if an organization were considering consolidating its mainframes into one

site (or considering distributing the processing currently done at one mainframe site), the central security program personnel could discuss the security implications and costs or cost savings. However, to speak authoritatively, the central computer security must actually know the security and cost impacts of the proposed change.

Besides being able to help an organization use information more cost effectively, a security program can also help an organization better spend its scarce security dollars. Organizations can develop expertise and then share it, reducing the need to contract out repeatedly for similar services. The central security program can help facilitate information sharing.

Example (based on Agency in Figure 1)

Each of the agency's five operating units developed a separate specialized expertise, and the organization as a whole shares the increased knowledge base. Operating Unit #1, which uses primarily UNIX, developed skills in UNIX security. Operating Unit #2, which uses primarily MVS, but has one UNIX machine, concentrated on MVS security but relies on Unit #1's skills for their one UNIX machine.

The central security program can also develop its own areas of expertise. Many security programs develop skills in contingency planning and risk analysis in order to help the entire organization perform these vital security functions.

Besides allowing an organization to share expertise, and therefore save money, a central security program can also use its position to consolidate requirements so the organization can negotiate discounts based on volume purchasing of security hardware and software.

6.3.2 Oversight

Besides helping an organization to improve the economy and efficiency of its security program, the central security program can also serve as an independent evaluation or enforcement function. The purpose of this oversight role is to ensure that organizational subunits are cost-effectively securing resources and following applicable policy. While the Office of Inspector General (OIG) and external organizations, such as the General Accounting Office (GAO), also perform a valuable evaluation role, they operate outside the regular management channels. The Life Cycle and Assurance Chapters further discuss the role of independent audit.

There are several reasons for having an oversight function within the regular management channel. First, since security is a part of the regular management of organization resources, it is a responsibility which cannot be abdicated to another organization. Second, it allows an organization to find and correct problems without the potential embarrassment of an IG or GAO audit or investigation. Third, the organization may find different problems than an outside organization. The organization better understands its assets, threats, systems and procedures than an external organization, and people involved in the audit may share information within the organization they may withhold from an outsider.

6.4 Central Security Program Elements & Considerations

In order for a *central security* program to be effective, it must be an established part of organization management. If system managers and applications owners do not need to consistently interact with the security program, then it can become an empty token of upper management's "commitment to security." The following paragraphs describe some of the means of becoming an established part of organization management and some of the indicators that a program has done so.

6.4.1 Stable Program Management Function

A well-established program will have a program manager recognized within the organization as the central security program manager. In addition, the program will be staffed with able personnel and links will be established between the program management function and security personnel in other parts of the organization. A security program is a complex function that needs a stable base from which to direct the management of security resources, such as information and financial resources. The benefits of an oversight function cannot be achieved if the security program is not recognized within an organization as having expertise and authority.

6.4.2 Stable Resource Base

A well-established program will have a stable resource base in terms of personnel, funds, and other support. Without a stable resource base, it is impossible to plan for and execute programs and projects effectively.

6.4.3 Existence of Policy

Policy provides the foundation for the central security program and is the means for documenting and promulgating important decisions about security. In addition to policy, a central security program should also publish standards, regulations, and guidelines which implement and expand on policy. These are also discussed in the Policy Chapter.

6.4.4 Published Mission and Functions Statement

A published mission statement grounds the central security program into the unique operating environment of the organization. The statement clearly establishes the function of the security program and defines responsibilities for both the security program and other related programs and entities. Without such a statement, it is impossible to develop evaluation criteria for the effectiveness of the security program.

6.4.5 Long-Term Security Strategy

A well-established program explores and develops long-term strategies to incorporate security

into the next generation of information technology. Since the computer and telecommunications field moves rapidly, it is essential to plan for future operating environments.

6.4.6 Compliance Program

An central security program must address whether the organization is in compliance with national policies and requirements as well as organization specific requirements. National requirements include those prescribed under the Computer Security Act of 1987, OMB Circular A-130, the FIRMR, and FIPS PUBs.

6.4.7 Liaison with Other Offices Within the Organization

Example: Agency IRM Offices engage in strategic and tactical planning for both information and information technology, in accordance with the Paperwork Reduction Act and OMB Circular A-130. Security should be an important component of these plans. The security needs of the agency should be reflected in the information technology choices and the information needs of the agency should be reflected in the security program.

There are many offices within an organization that potentially affect computer security. The IRM and traditional security offices (such as personnel, industrial, or physical security) are two obvious examples. However, computer security often overlaps with other offices such as Safety, Reliability, and Quality Assurance, Internal Control or the Inspector General. An effective program must have established relationships with these groups in order to integrate security into the management of an organization. The relationships must be more than just passing information; the offices must influence each other.

6.4.8 Liaison with External Groups

As discussed in this chapter, there are many sources of security information, such as NIST's Computer Security Program Managers' Forum, computer security bulletin board, and the Forum of Incident Response and Security Teams (FIRST). An established program will be knowledgeable of and take advantage of external sources of information. It will also be a provider of information.

6.5 System Level Security Program

The purpose of the *system level* security program is to ensure appropriate and cost-effective security for each system. A central security program, as explained above, addresses the entire spectrum of information resources security for an organization. The system level security programs implement security for each information system. This includes influencing decisions about what controls to implement, purchasing and installing technical controls, day-to-day security administration, evaluating system vulnerabilities, responding to security problems, and so forth. It encompasses all the areas discussed in this Handbook.

The system level security program is the local advocate for security. The system security officer is the person who must raise the issue of security with system managers and help develop solutions for security problems. For example, has the data owner made clear the security requirements of the system? Will bringing a new function online impact security? Is the system vulnerable to hackers and viruses? Has the contingency plan been tested? Raising these kinds of questions will force system managers and data owners to identify their security requirements and ensure that they are being addressed.

6.6 System Level Security Program Elements and Considerations

Like the central security program, there are many factors which influence how successful a *system level* security program is. Many of these are similar to the organization level. This section addresses some additional considerations.

6.6.1 System Level Security Policy

There are many policy issues that need to be addressed on a system-specific basis. System level policy address these issues. The issues can vary for each system, although access control and the designation of persons with security responsibility are likely to be needed for all systems. In order to develop a cohesive and comprehensive set of security policies, a management process which derives security rules from security goals should be used. This is discussed in the Policy Chapter.

6.6.2 Integration with System Operations

Characteristics of a Successful System Security Program:

System Level Security Policy
Integration with System Operations
Separation from Operations
System Security Plans

The system level security program must consist of people who understand the system. For security management to be effective, it must be integrated into the management of the system. Effective integration will assure that system managers and data owners consider security in the planning and operation of the system. The system level security manager must be able to participate in the selection and implementation of appropriate technical controls, security procedures, and must understand system vulnerabilities. The system level security program must be able to respond to system security problems in a timely manner.

For large systems, such as a mainframe data center, the security program will often include a manager and several staff positions in such areas as access control, user administration, and contingency and disaster planning. For small systems, such as an office-wide LAN, the security program may be an adjunct responsibility of the LAN administrator.

6.6.3 Separation from Operations

A natural tension often exists between security and operational elements. In many instances, operational components, which tend to be far stronger entities, seek to resolve this tension by having the security program embedded in computer operations. The typical result of this organizational strategy is a security program that lacks independence, has minimal authority, receives little management attention, and has few resources. As early as 1978, the General Accounting Office (GAO) identified this organizational mode as one of the principal basic weaknesses in federal agency computer security programs.[39] While it is possible for central security programs to face this problem, system level programs face this problem more often.

This conflict between the need to be a part of system management and independence has several solutions. The basis of many of the solutions is a link between the security program and upper management, often through the central security program. A key requirement of this setup is the existence of a reporting structure which does not include systems management. Another possibility is for the security program to be completely independent of system management and report directly to higher management. There are many hybrids and permutations such as co-location of security and systems management staff, but separate reporting (and supervisory) structures. Figure 5-3 presents an example of placement of the security program within a typical Federal agency.

Figure 6-3 (see attachment)

6.6.4 System Security Plans

The Computer Security Act mandates that agencies develop computer security and privacy

[39]GAO Report LCD 78-123, "Automated System Security -- Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data."

plans for sensitive systems. The purpose of this plan is to ensure that each Federal and Federal interest system has appropriate and cost-effective security. System level security personnel should be in a position to develop and implement security plans. The Security and System Life Cycle Chapter discusses the plans in more detail.

6.7 Central and System Level Security Program Interactions

The need for central and system level security programs to work together has been a major theme of this chapter. A system level program that is not integrated into the organizational program may have difficulty influencing significant areas affecting security.

The system level security program implements the policies, guidance, and regulations of the central security program. The system level office also learns from the information disseminated by the central program and uses the experience and expertise of the entire organization. The system level security program further distributes information to systems management as appropriate.

The communication, however, is not one way. The system level security program informs the central office about needs, problems, incidents, and solutions. The central security program can then represent the system to the organization's management and to external agencies and advocate programs and policies beneficial to the security of all the systems.

6.8 Interdependencies

Policy. Policy is the basis for the computer security program. The central security program(s) normally produces policy concerning general and organizational security issues (program framework policy) and often issue-specific policy. However, the system level security program normally produces some issue-specific policies and policies affecting only one system. The Policy Chapter provides additional guidance.

Life Cycle Management. The process of securing a system over its life cycle is the role of the system level security program. See Security and Life Cycle Management Chapter addresses these issues.

Independent Audit. The independent audit function described in the Assurance and Life Cycle Chapters should be complementary to the compliance function performed by a central security program.

General. The general purpose of the computer security program, to improve security, causes it to overlap with every control. Most controls will be addressed at the policy, procedural, or operational level by the central or system security program.

6.9 Cost Considerations

This chapter discussed how an organization-wide security program can manage security resources, including financial resources, more effectively. The cost considerations for a system level security program are more closely aligned with the overall cost savings in having security.

The most significant direct cost of a security program is personnel. In addition, many programs make frequent and effective use of consultants and contractors. A program also needs funds for training of personnel and travel to perform oversight, information collection and dissemination activities, and meet with personnel at other levels of security management.

6.10 Summary

Organizations, large and small, can benefit from the establishment of a computer security program that integrates central office and system level security efforts, is supported by senior management, and is publicized to all employees. Central and system level security programs must work together to achieve the common goal of protecting an organization's vital information resources.

6.11 References

"Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data. GAO Report LCD 78-123. General Accounting Office.

Computer Security Act of 1987. Public Law 100-235. U.S.Congress, 1988.

Federal Information Resources Management Regulations, especially 201-2. General Services Administration.

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

Helsing, C., M. Swanson and M. Todd, *Executive Guide to the Protection of Information Resources*, Spec. Pub. 500-169.
National Institute of Standards and Technology. 1989.

Helsing, C., M. Swanson and M. Todd, *Management Guide for the Protection of Information Resources.* Spec. Pub 500-170. National Institute of Standards and Technology. 1989.

Information Resources Security: What Every Federal Manager Should Know. General Services Administration.

Management of Federal Information Resources. OMB Circular A-130. Office of Management and Budget.

Managing an Organization Wide Security Program. Course taught by the Computer Security Institute.

Owen, R. Jr., "Security Management: Using the Quality Approach." *Proceedings of the 15th National Computer Security Conference*. Vol 2, 1992. pp. 584-592.

Spiegel, L. "Good LAN Security Requires Analysis of Corporate Data." *Infoworld*. 15(52), 1993. p. 49.

7 Risk Management

7.1 Introduction

Though people may not be aware of it, everyone performs acts of risk management daily. Actions as routine as buckling a car safety belt, carrying an umbrella when rain is forecast, or writing down a list of things to do rather than trusting to memory are acts of risk management: people have recognized various threats to their best interests and have taken precautions to guard against them or to minimize their effects.

Management is concerned with many types of risk. Computer security risk management addresses risks which arise from an organization's use of information technology.

Risk management is routinely performed in government and industry to limit a myriad of business and organizational risks. A common illustration of risk management is the development of investment strategies. To maximize the return on investments, businesses often must decide between aggressive (but high risk) and slow growth (but more secure) investment plans. Such decisions are made based on degrees of risk relative to potential benefits. These decisions require analysis of risk, consideration of alternatives, and, finally, implementation of what management determines to be the best plan.

This chapter discusses computer security risk management, which is one of the cornerstones of computer security. The fundamental assumption of risk management is that computers cannot be fully secure. There is always risk, whether it is from a trusted employee who defrauds the system or a fire that destroys critical resources.

The purpose of risk management is to improve security by performing two functions: the *measurement of risk* and the *selection of cost-effective controls*. The two functions of risk management are a logical outcome of this assumption that risk cannot be removed entirely. If risk cannot be removed, it must be reduced as cost-effectively as possible and it must be reduced to an acceptable level. This chapter will explain the two functions of risk management and describe the basic components of the risk management process.

7.1.1 Function #1: Measurement of Risk

Risk is the possibility that something bad will happen and it is associated with all computer systems. Management at some point must decide if the operation of the computer system is acceptable given the risk. In some cases, use of a computer system reduces overall risk; while in other cases it may increase risk. In general, use of computer systems reduce some risks while creating others.

For many managers, computer-based risk is not well understood for several reasons: 1) the type of risk may be different from risks previously associated with the organization or function; 2) the risk may be technical and hard to understand, or 3) the proliferation and decentralization of computing power can make it difficult to identify key assets that may be at risk.

> One example of a risk that often not well understood is email spoofing. Most people do not realize that it is possible for people to change the "from line" in an email message to make it look like it came from someone else.

It is important to both *identify* and *measure* risk. The identification of risk will show what safeguards are in place and how effective they are.

Measuring the risk makes it possible for a manager to decide whether the risk is too high or not. A manager may base the decision about the acceptability of risk on many factors including security, performance, legal constraints, and cost. The relative weights given to these factors is a management decision.

The acceptance of risk is closely linked with computer system *accreditation*, discussed in the Life Cycle and Assurance Chapters. Accreditation is the acceptance of risk by management resulting in a formal approval for the system to become operational or remain so.

If risk measurements are done consistently across an organization, they can be used to prioritize systems to be secured. In addition, the risk identification and measurement process can identify critical weaknesses that need immediate correction.

7.1.2 Function #2: Identification of Cost-effective Controls

The second function of computer security risk management is the identification of cost-effective controls. In designing (or reviewing) the security of a system, it may be obvious that some controls should be added and that others are too expensive (considering both monetary or non-monetary factors). For example, it may be clear to a particular manager in a particular situation that closing and locking the door to a room that contains local area network equipment is a needed control while a guard at the door would be too costly and too user-unfriendly. In addition, some controls may be required by organizational policy or directive. These controls are often referred to as baseline controls.

In every risk assessment, there will be many areas for which it will not be obvious what kind of controls are appropriate. Even considering only monetary issues, such as whether a control would cost more than the loss it is supposed to prevent, the selection of controls is difficult. However, a manager must consider many factors as well as monetary ones including the impact of controls and losses on:

- organizational policy, legislation, and regulation,

- safety, reliability, and quality requirements,
- system performance requirements,
- timeliness requirements,
- technical requirements, and
- cultural constraints.

Risk management can *help* a manager determine which are the most appropriate controls. Risk management is not, however, a magic wand which a manager can use to answer these very difficult questions. The quality of the output is dependent on the quality of the input. In some cases, the amount of work required to achieve high quality input will be too costly. In other cases, it may be impossible to achieve high quality input, especially for variables such as how often a threat appears or the effectiveness of a safeguard. Despite these drawbacks, risk management provides a very powerful tool for analyzing the risk associated with computer systems.

7.2 Risk Management: How Does It Work?

There are many different terms used to describe risk management and its elements. The definitions used in this paper are based on the NIST Risk Management Framework.

Risk management is the process of assessing risk, taking steps to reduce risk to a level acceptable to the accrediting official, and maintaining that level of risk. While there are many models and methods for risk management, there are several basic activities and processes that should be performed. Figure 1 shows the flow of risk management activities and processes. A major division in risk management (shown by the vertical line) is between *risk assessment* and *risk mitigation*. Both are critical parts of the risk management process. Risk assessment is the process of analyzing and measuring risk and is comprised of three basic activities: boundaries determination, analysis, and risk measure. Risk mitigation is the process of reducing risk and is comprised of two basic activities: acceptance testing and selection of cost-effective safeguards. Both processes are essential for risk management.

There is one other activity in risk management: uncertainty analysis. Risk management often

uses speculation, best guesses, incomplete data, and many unproven assumptions. The uncertainty analysis attempts to document this underlying problem so that the risk management results can be used more knowledgeably.

Although these activities are discussed in a particular sequence, it is not necessary that they be performed in this sequence. In particular, the selection of cost-effective safeguards and the risk acceptance test are likely to be performed either together or in reverse order. The uncertainty analysis can be performed throughout the risk management process.

7.2.1 Risk Assessment

Risk assessment is the process of analyzing and measuring risk and is comprised of three basic activities: boundaries determination, analysis, and risk measure.

7.2.1.1 Boundaries, Scope, and Methodology Determination

When beginning a risk management effort it is necessary to first identify the system under consideration, the part of the system that will be analyzed, and the methodology for the analysis including level of detail and formality. It is possible to perform risk management for an entire organization encompassing many systems.

The analysis can be focused on certain areas where either the amount of risk is unknown or known to be high. Different parts of a system can be analyzed in greater or less detail. Defining the scope and boundary can help ensure a cost-effective analysis.

> A risk assessment can focus on many different areas such as: technical and operational controls to be designed into a new application, the use of telecommunications, a data center, or an entire organization.

Factors that influence scope include what phase of the life cycle a system is in: more detail might be appropriate for a new system about to go online than for an existing system undergoing an upgrade. Another factor is the relative importance of the system under examination, for example, the more essential the system, the more thorough the risk analysis. A third factor may be magnitude and type of changes the system has undergone since the last risk analysis. The addition of new interfaces would warrant a different scope than would installing a new operating system.

Methodologies can be formal or informal, detailed or simplified, high level or low level, quantitative (computationally-based) or qualitative (based on descriptions or rankings) or a combination of the above. No single method is best for all users and all environments.

The definition of the boundary and scope (including methodology) will have major consequences in terms of the total amount of effort spent on the risk management effort and the type and usefulness of results which are produced. The boundary and scope should be selected in a way that will produce an outcome which is clear, specific, and useful to the

system and environment under scrutiny.

7.2.1.2 Analysis

There are many different components to risk. In order to understand risk, it is necessary to examine six different areas: 1) assets, 2) threats, 3) vulnerabilities, 4) safeguards, 5) consequences, and 6) likelihood. This examination normally includes gathering data about the area *and* synthesizing the information to make it useful.

Because it is possible to collect much more information than can be analyzed, steps must be taken to limit the information gathering and analysis. This process is called *screening*. A risk management effort should focus on those areas which result in the greatest consequence to the organization, i.e., cause the most harm. This can be done by ranking threats and assets in priority order.

The six areas listed above are the essential elements of risk. A brief description of each of them follows. A risk management methodology does not necessarily need to analyze each area separately. For example, assets and consequences may be analyzed together or threats and likelihoods.

Assets. These include the information, processing power, personnel, as well as the physical assets (such as the computer itself). Assets are analyzed to determine their value. The value of assets needs to be defined in terms of the consequences to the organization if the asset is disclosed, modified, destroyed or misused in any other way. This will include substantially more than just the replacement cost of hardware. Consequences are discussed below.

> Example: A system that processes payroll would value both the ability to run payroll and the payroll information itself.

The goal of asset valuation is to identify the most important assets, i.e., those whose loss, disclosure, modification, or misuse will cause the direst consequences to the organization. This will help to focus the risk assessment on the most critical assets.

Threats. A threat is an entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, viruses.

In order to analyze what threats exist, a threat categorization is normally performed which the analyst uses to help ensure that no threats are missed. This is called threat identification. In addition to identifying threats, they must also be analyzed to determine the likelihood of a threat occurring. The relative seriousness of threats should also be estimated. The threats of most concern are those with the potential to do the most harm to the most valuable assets.

In addition to looking at "big ticket" threats, the threat identification should investigate areas

that are poorly understood, new, or undocumented. If a facility has a well-tested physical access control system, less threat identification effort may be warranted for it than for unclear, untested software backup procedures.

The risk analysis should concentrate on realistic threats, meaning those most likely to occur and affect important assets. The Threat Chapter provides additional discussion. In some cases which threats are realistic cannot be known until after the threat analysis.

Vulnerabilities. A vulnerability is a condition or weakness in security procedures, technical controls, physical controls, or other controls that could be exploited by a threat. Vulnerabilities are often analyzed in terms of missing safeguards. Vulnerabilities contribute to risk because they "allow" a threat to harm the system.

Example: A vulnerability that could be exploited by the dishonest employee is a poor access control scheme that allowed the employee to access their own record.

The interrelationship of vulnerabilities, threats, and assets is critical to the analysis of risk. Some of these inter-relationships are pictured in the "brick wall" figure below. However, there are other inter-relationships such as the presence of a vulnerability inducing a threat. (For example, a normally honest employee might be tempted to alter data when the employee sees that a terminal has been left logged on.)

Safeguards. As noted above, safeguard and vulnerabilities are related since vulnerabilities are often expressed as the absence of safeguards. A safeguard is any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat. The safeguard analysis should include an examination of the effectiveness of the safeguard.

Example: The design and implementation of a new access control scheme is a safeguard as would be an audit trail which could detect people modifying their own records.

A safeguard analysis can also be done to identify new safeguards which could be implemented in the system. This is normally performed later in the risk management process. (It is discussed under Selection of Cost-effective Safeguards.)

Consequences. The consequence assessment estimates the amount of harm or loss that could occur due to a threat successfully exploiting a vulnerability. Consequences refers to the real harm that occurs, not just to the immediate impact. While near-term impacts usually result in disclosure, modification, destruction, or denial of

Example: The consequence of the dishonest employee modifying her record might be that all the employees start modifying their records with the employer losing thousands of dollars in stolen vacation time.

service, consequences are the more significant long-term consequences such as lost business, failure to perform the system's mission, loss of reputation, violation of privacy or injury or loss of human life.

The worse the consequence of a threat harming the system, the greater the risk.

Likelihood. Likelihood is an estimation of the frequency of a threat happening. A likelihood assessment must consider the presence, tenacity, and strengths of threats as well as the effectiveness of safeguards (or presence of vulnerabilities). In general, historical information about many threats is poor, particularly in regard to human threats; thus experience in this area is important. Some threat data, especially on physical threats such as fires or floods, is more complete. Care must be taken in using any statistical threat data; the source of the data or the analysis may be inaccurate or incomplete.

Example: The likelihood of people modifying their payroll records is much higher is they think they can get away with it.

Figure 2

The greater the likelihood of a threat occurring, the greater the risk.

7.2.1.3 Measures of Risk

After being collected, the data and estimates described above must be integrated and analyzed to produce a risk measure, which is a description of the kinds and degrees of risk to which the organization or system is exposed. The way risk is measured varies according to the risk analysis methodology chosen. The selection of the methodology should be made with the

production of a useful risk measure in mind.

The risk measure should be useful in the two basic functions of risk management: acceptance of residual risk and selection of safeguards. Therefore, to accomplish the first function, the risk measure must describe risk in a manner consistent with management understanding of risk. To accomplish the second function, the measure must assist in cost-benefit analysis by providing a meaningful description of the amount of benefit anticipated from various safeguards.

> The risk measure does not have to expressed as a number. It can be a description, graph, or any other form that is meaningful within an organization.

Risk is measured in either quantitative or qualitative terms (or a combination of the two). Quantitative measures are often expressed in terms of reduced expected monetary losses, such as annualized loss expectancies or single occurrences of loss. Qualitative measures are often expressed as high-medium-low or ranked on a scale of 1 to 10. The measure could also be a description of the risk.

The most important aspect of risk measurement is that it be meaningful for the given circumstances and organization. To be useful, the measurement should reflect what is truly important to the organization. Limiting the risk measurement activity to the most important risk is another way that the risk management process can be screened or focused to reduce the overall effort while still yielding useful results.

7.2.2 Risk Mitigation

This section on Risk Acceptance Test and the following section on Selection of Cost-effective Safeguards describe the second part of the risk management process: *risk mitigation*. Although there is flexibility in how the first part of the process (risk assessment) is conducted, the sequence of identifying boundaries, analyzing input and producing an output is quite natural. The process of risk mitigation has greater flexibility and the sequence will differ more depending on organizational culture and the purpose of the risk management activity.

7.2.2.1 Risk Acceptance Test

As discussed earlier in this chapter, one of the two primary functions of risk management is the identification and measurement of risk for the purpose of risk acceptance.

Risk acceptance can take into account various factors besides those addressed in the risk assessment. Some examples are listed in box. In addition, the risk acceptance should take into account limitations of the risk assessment. See the section below on uncertainty. The risk acceptance often uses the analysis of cost-effective safeguards since, in some cases, risk may have to be accepted because it is too expensive to mitigate it.

7.2.2.2 Selection of Cost-Effective Safeguards

Examples of Other Factors

Organizational policy
Political issues
System performance requirements
Technical constraints
Monetary constraints
Cultural constraints

The selection of cost-effective safeguards can be performed in many ways. One method is to use "what if" analysis. Under this method, the effect of adding various safeguards (and therefore reducing vulnerabilities) is tested to see what difference each alternative makes in the risk measure. Tradeoffs can then be made based on the cost of the safeguard and the benefit (in terms of reduced risk).

Another method is to categorize types of safeguards and recommend implementing them for various levels of risk. For example, high risk systems would implement stronger controls than low risk systems.

Other methods can rely on traditional benefit cost analysis. The benefit is calculated based on an expected decrease in future losses. The cost is based on the purchase and operating cost of safeguards.

As with other aspects of risk management, screening can be used to concentrate on the highest risk areas. One method is to examine risks with very severe consequence such as a very high single occurrence of loss (if a quantitative measure was used) or other important consequences (such as loss of life).

Figure 1 shows the selection of cost effective safeguards as a two step process. In the assessment portion of the figure, safeguard selection analysis is performed resulting in a recommendation. In the risk mitigation portion of the figure, the recommendation is accepted. (If it is not accepted, then more analysis work must be performed to reach an acceptable balance between risk and cost.) The selection of safeguards normally results in a requirement to obtain or implement the safeguards.

7.2.3 Uncertainty Analysis

There are two primary sources of uncertainty in the risk management process. The first source of uncertainty is a lack of confidence in the risk management model or methodology. The second source is a lack of sufficient information to determine the exact value of the elements of the risk model such as threat frequency, safeguard effectiveness, or consequences.

The risk management framework presented in this chapter is a generic description of risk management elements and their basic relationships. For a methodology to be useful, it must further refine the relationships and offer some means of screening information. In this process, assumptions may be made that do not accurately reflect the user's environment. This

is especially evident in the case of safeguard selection, where the number of relationships between assets, threats, vulnerabilities is potentially huge.

While uncertainty is always present it should not invalidate a risk assessment. Data and models, while imperfect, can be good enough for a given purpose.

Another source of uncertainty is the data itself. Data for the risk analysis normally comes from two sources: statistical data and expert analysis. Statistics and expert analysis can sound more authoritative than they really are. There are many potential problems with statistics such as the sample being too small, other parameters existing which affect the data but have not been accounted for, or the result may be stated in a misleading manner. In many cases, there may not be sufficient data. When expert analysis is used to make projections about future events, it should be recognized that the projection is subjective and is based on assumptions made by the expert.

7.3 Implementing Controls and Monitoring Effectiveness

Good documentation of risk assessments will make later risk assessments less time consuming and, if a question arises, will help explain why security decision were made.

Too frequently, organizations wrongly equate effective security with the performance of risk analysis alone, neglecting the essential further step of implementing risk mitigation measures. Merely knowing what the risks are does not reduce them. Moreover, to be effective, risk management must be a continuing process, requiring periodic assessment and improvement of safeguards, and reanalysis of risks.

The risk management process normally produces security requirements which are used to design, purchase, build or otherwise obtain the safeguards or change the system. The integration of risk management into the life cycle process is discussed in the Life Cycle Chapter. Risk management should be used to help define a system's initial and ongoing security requirements.

7.4 Interdependencies

Risk assessment often produces an important side benefit. It produces indepth knowledge about a system and often about an organization as risk analysts try to figure out how systems and functions are inter-related to determine threats, value assets, and understand consequences.

Risk management touches on every control and every chapter in this Handbook. It is, however, most closely related to Life Cycle. The requirement to perform risk management is often discussed in organizational policy and is an issue for organizational oversight. These issues are discussed in the Policy and Security Program Management chapters.

7.5 Cost Considerations

Risk management can get expensive very quickly if an expansive boundary and detailed scope are selected. It is very important to use screening techniques, as discussed in the chapter, to limit the overall effort. The goals of risk management must be kept in mind as a methodology is selected or developed. The methodology should concentrate on areas where identification of risk and the selection of cost effective safeguards are needed.

The cost of different methodologies can be significant. A "back of the envelope" analysis or high-medium-low ranking can often provide all the information needed. However, especially for the selection of expensive safeguards or the analysis of systems with unknown consequences, more indepth analysis may be warranted.

The building blocks of risk management presented in this chapter can be used creatively to develop methodologies that concentrate expensive analysis work where it is most needed.

7.6 Summary

No system or operational environment can ever be made completely risk free, nor can a risk assessment, which is ultimately based on many educated guesses, be completely precise and accurate. Effective risk management will reduce risks to acceptable levels at optimal cost, based on the best information obtainable.

7.7 References

Caelli, William, Dennis Longley, and Michael Shain. *Information Security Handbook.* Stockton Press, 1991.

Carroll, J.M. *Managing Risk: A Computer-Aided Strategy*, Butterworths Boston, 1984.

Jaworski, Lisa. "Tandem Threat Scenarios: A Risk Assessment Approach." *Proceedings of the 16th National Computer Security Conference*, Vol 1, 1993. pp. 155-164.

Katzke, Stuart. "A Framework for Computer Security Risk Management." *8th Asia Pacific Information Systems Control Conference Proceedings*, EDP Auditors Association, Inc., Singapore, October 12-14, 1992.

Gilbert, Irene. *Guide for Selecting Automated Risk Analysis Tools*. Spec. Pub. 500-174. National Institute for Standards and Technology, October 1989.

Guideline for Automatic Data Processing Risk Analysis. FIPS PUB 65. National Bureau of Standards. August 1979.

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

O'Neill, M. and F. Henninge,Jr., "Understanding ADP System and Network Security Considerations and Risk Analysis." *ISSA Access*. 5(4), 1992. pp. 14-17.

Proceedings, 4th International Computer Security Risk Management Model Builders Workshop, University of MD, National Institute for Standards and Technology, College Park, MD, August 6-8, 1991.

Proceedings, 3rd International Computer Security Risk Model Builders Workshop, Los Alamos National Laboratory, National Institute for Standards and Technology, National Computer Security Center, Santa Fe, NM, August 21-23, 1990.

Proceedings, 1989 Computer Security Risk Management Model Builders Workshop, AIT Corporation, Communications Security Establishment, National Computer Security Center, National Institute for Standards and Technology, Ottawa, Canada, June 20-22, 1989.

Proceedings, 1988 Computer Security Risk Management Model Builders Workshop, Martin Marietta, National Bureau of Standards, National Computer Security Center, Denver, CO, May 24-26, 1988.

Spiegel, L. "Good LAN Security Requires Analysis of Corporate Data." *Infoworld*. 15(52), 1993. p. 49.

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

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

8 Security in the Computer System Life Cycle

8.1 Introduction

Many computer systems evolve rather than progress through a formal life cycle. The purpose of this chapter is to show the relationship and purpose of various security-relevant events and analyses. The life cycle provides the context.

Like other aspects of information processing systems, security is most effective and efficient if managed throughout a computer system's life cycle, from initial planning through design, implementation, and operation until disposal.[40] Many security-relevant events and analyses occur during a system's life. This chapter explains the relationship among them and shows how they fit together. 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. This chapter examines:

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

8.2 What is the Computer System Life Cycle?

There are many models for the computer system life cycle, but most contain the following phases. Each phase can apply to an entire system or to a new component or module or to a system upgrade.

- *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

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

is almost always modified by the addition of hardware or software and by numerous other events.

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

Many people find the concept of a computer system life cycle confusing because many cycles occur within the broad framework of the 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. In addition, the computer system life cycle itself is merely one component of other life cycles.

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

As an example of how the computer system life cycle can be a part of a larger cycle, consider the *information cycle*. Normally information, such as personnel data, is used much longer than the life of one computer system. If an employee works for a company for 30 years and collects retirement for 20 more years, the employee's personnel record (information) will probably pass through many different computer systems owned by the company. In addition, parts of the information will also be used in other computer systems, such as those owned by the Internal Revenue Service and the Social Security Administration.

8.3 Benefits of Integrating Security in the Computer System Life Cycle

When security is integrated in the computer system life cycle, better, more cost-effective security can usually be obtained than if security is added to a system after a security breach, mishap, or audit. A reactive approach leads to haphazard security which can be expensive, minimally effective, or detrimental to system performance.

Security, like other aspects of a computer system, is best managed if planned for throughout the 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. This includes security features. In addition to including security in the early phases of the life cycle, it also must be incorporated into the later phases. Management of security during these phases helps ensure that security keeps up with changes to the system 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. When security is integrated into the computer system life cycle, better, more

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.

cost effective security can usually be obtained than if security is added to a system after a security breach, mishap, or audit. A reactive approach can lead to haphazard security which can be expensive, minimally effective or can significantly degrade system performance.

In addition to helping assure management that security is adequately considered in all phases, life cycle management helps *document* security-relevant decisions. This documentation benefits system management officials as well as oversight and independent audit groups. Systems management uses the documentation as a self-check and as a reminder why decisions were made so that the impact of a change 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 operating.

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. The purpose of these plans is to see that security is considered not only during system design and development but also throughout the operation and maintenance of the system and its disposal. Plans are discussed in more detail below.

8.4 Computer Security Plans and the Computer Security Act

The Computer Security Act of 1987 sets forth a statutory requirement for the preparation of computer security plans for all sensitive federal or federal-interest computer systems. These plans are known as Computer Security and Privacy Plans (CSPPs). 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 towards a CSPP 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 management. The benefit of having a distinct CSPP 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, OMB Bulletin 90-08, requires agencies to obtain independent review of CSPPs. This can 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" CSPP briefly describes the important security considerations for the

system and provides references to more detailed documents such as contingency plans, risk assessments, accreditation statements, or audit results. This enables the plan to be used as a management tool without requiring repetition of existing documents. For smaller systems, the CSPP may include all of the security documentation. As with other security documents, if a CSPP addresses specific vulnerabilities or other information which could compromise the system, the plan must be kept private.

The CSPP should be started at the beginning of the computer system life cycle and updated as the system progresses. However, a CSPP can be developed for a system at any point in the life cycle. In general, the plan should be updated 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.

8.5 Techniques to Address Security in the Computer System Life Cycle

This section describes the general security considerations and activities that occur at each phase of the computer system life cycle. As with other aspects of systems management, the level of detail and analysis for each activity described below is determined by many factors including size, complexity, system cost, and sensitivity. An overview of the process in pictured in Figure 7-1.

The life cycle described here can be applied to a brand new system or, more commonly, to a project to upgrade a part of an existing system. If the life cycle is applied to a project, it is important to recognize that the project can impact the entire system.

8.5.1 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; environmental, financial, political, or other constraints. The basic security aspects of a system should be developed along with the conceptual and early design of the system. This can be done through a *sensitivity assessment.*

Sensitivity Assessment. This 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. Factors such 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 must be examined when assessing sensitivity. In order to address these types of issues, the people who use or own the system or information must participate in conducting the assessment.

The definition of "sensitive" is often misconstrued. "Sensitive" is synonymous with important or valuable. Some sensitive data must be kept confidential, but much more is considered sensitive because of integrity or availability concerns. The more important a system is to the mission of the agency, the more sensitive it is. The Computer Security Act and OMB Circular A-130 clearly state that information is sensitive if modification or availability of the information is important.

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., Privacy Act or 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, security clearances)?
- What internal security standards, regulations, or guidelines apply to this system?

The sensitivity assessment starts an analysis of security which continues throughout the life cycle. The assessment results determines 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, either acquisitions or developments. 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 or will some controls become unnecessary?

8.5.2 Development / Acquisition

For most systems, this phase is more complicated than the initiation phase. Security activities can be divided into three parts: 1) determining security features, assurances, and operational practices; 2) incorporating these into design specifications; and 3) actually obtaining them. These divisions apply to systems that are designed and built in-house, to systems which are purchased, and to systems which use a combination of methods.

During this phase, the technical staff and the system sponsors must actively work together to ensure that the technical design reflects the security needs of the system. As with the development and incorporation of other system requirements, this process requires an open dialogue between the technical staff and the sponsors.

8.5.2.1 Determining Security Features, Assurances, and Operational Practices

System security requirements are expressed in terms of features, practices, and assurances.

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 benefit-cost tradeoffs.

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

Policy. As discussed in the Policy chapter, management needs to develop security policy for systems. This policy should address the total security of the system, not just the automated part of the system. Often choices about the functional needs of the system and benefit-cost tradeoffs require policy decisions. Policy requires management to make important choices about what assets require what kinds of protection.

Standards and Guidelines. International, national, and organization 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 algorithm should be used. Many organizations specify baseline controls for different types of systems, such as administrative, mission or business critical, or proprietary. If a system needs to interoperate with other systems, then give special care 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.

Benefit-cost. When considering security, benefit-cost 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 laws, policy, standards, and the functional needs of the system). Appropriate safeguards are those whose anticipated benefits outweigh their costs. Benefits and costs include monetary and non-monetary issues such as prevented losses, maintaining organization reputation, decreased user friendliness, or increased system administration.

Risk assessment, like benefit-cost analysis, is a decision-support tool. It helps managers select cost-effective safeguards by analyzing the assets, threats, and vulnerabilities. The extent of the risk assessment, like that other benefit-cost 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 Risk Management chapter.

Risk assessment can be performed during the requirements analysis phase of a procurement or the design phase of a system development cycle. Risk assessment should also be done during the development/acquisition phase of a system upgrade. The risk assessment may be performed once or multiple times, depending upon the project methodology (for either a procurement or a system development effort).

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.

8.5.2.2 Incorporating Security Features, Assurances, and Operational Practices into Specifications

Determining security features, assurances, and operational practices can yield significant security information and often voluminous requirements. This information must 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 system development methodology 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 on travel. In addition to developing specifications, figure out how the system will be tested or reviewed to determine whether the specifications have been met. This applies to both system developments and acquisitions.

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

8.5.2.3 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 security aspects of the system, monitoring the development process itself for security problems, responding to changes, and threat monitoring. Threats that may occur 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, solicitation documents, and the evaluation of proposed systems. Many systems use a combination of development and acquisition. In this case, security activities include both sets.

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

In federal government contracting, a person with security expertise can be a member of the source selection board to help evaluate security aspects of proposals.

In addition to obtaining the system, operational practices need to be developed. This refers 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 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.

Besides the technical and operational controls of a system, *assurance* must also 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. 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. See the Assurance chapter for more information.

8.5.3 Implementation

Many computer system life cycles do not specify a separate implementation phase. 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, as discussed below. The other activities described in this section, turning on the controls and testing, are often incorporated at the end of the development/acquisition phase.

8.5.3.1 Install/Turn On Controls

While obvious, this activity is often overlooked. When it is acquired, a system often comes with security features disabled. These need to be enabled and configured. For many systems this may be a complex task requiring significant skills. Systems which were custom developed may also need to have security features enabled and configured.

8.5.3.2 Security Testing

System security testing includes both the testing of the particular parts of the system which 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 the requirements and specifications. In order to provide more reliable technical information, certification is often performed by an independent reviewer. (If it is performed by the people who designed the system, there may be a disincentive to find errors.)

8.5.3.3 Accreditation

System security accreditation is the *formal approval* by the accrediting (management) official for system operation and an *explicit acceptance of risk*. 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 piece.

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 solution between security, 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. An annual re-evaluation will be conducted to determine if changes have occurred which affect the security of the system.

After the accrediting official decides on the acceptability of security safeguards, a formal accreditation statement should be issued. While most flaws in system security are not severe enough to remove an operational system from service or to prevent a new system from going operational, the flaws may require some restrictions on operation (e.g., limitations on dial-in access). In some cases, an interim accreditation may be granted to allow the system to operate but require a new review at the end of the interim period, presumably after security upgrades had been made.

8.5.4 Operation and Maintenance

Many security activities take place during the operational phase of a system's life. In general, these fall into three areas: security operations and administration; operational assurance; and periodic re-analysis of the security. Figure 7-2 diagrams the flow of security activities during the operational phase.

8.5.4.1 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 examples.

8.5.4.2 Operational Assurance

Security is *never* perfect when a system is implemented. 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 and, over time, procedures become outdated. Thinking risk is minimal, users tend to bypass security measures and procedures. As shown in Figure 7-2, "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 fixed), 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.

> Operational assurance examines whether a system is run 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.

In order 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. Audits can be divided into two types: self-audit and independent audit. Either method can examine technical, procedural, managerial, or other aspects of security. The audits often include the use of automated tools, security checklists, or a review of controls to see if they adequately protect the system.

Monitoring refers to an ongoing activity that examines either the system or users. 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. The actual act of keeping the audit trail is neither an audit nor monitoring. Daily or weekly review of the audit trail is generally monitoring while an historical review of several months of the trail is probably an audit.

Monitoring system security also involves a wide range of activities. System administrators often monitor for anomalies or variances from "normal" system operation which could indicate a problem. Automated tools which analyze the audit trail in real time, often using artificial intelligence, are being developed. Monitoring is also used to see if procedures are being followed.

More information on auditing and monitoring is included in the Assurance chapter. The Audit chapter provides information on the use of system-generated audit trails.

8.5.4.3 Change Management

> Security change management helps develop new security requirements.

Computer systems and the environments in which they operate change continually. System managers and users modify the system and incorporate new features, new procedures, and software updates. These changes are in response to various events such as user complaints, availability of new features and

services, or the discovery of new vulnerabilities.

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 the increase in network intrusion or the spread of personal computer viruses.

Security should also be considered during system upgrades and other planned changes and in determining the impact of unplanned changes. As shown in Figure 7.2, when a change occurs or is planned, a determination must be made whether the change is major or minor. A major change significantly affects the system, such as re-engineering the structure of 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 methods described below under major and minor change.

If the system has a configuration control board or other structure to manage technical system changes, assign a security specialist to the board to make determinations about whether changes will affect the security of the system.

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 or will occur. If the original analysis and system changes have been documented throughout the life cycle, the analysis will be much easier. Since these changes result in significant system acquisitions, development work, or changes in policy, the system should be re-accredited 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 which weighs the pros (benefits) and cons (costs). These limited risk assessment can be performed at meetings, on the backs of envelopes, or "on-the-fly." Even if the analysis is performed informally, decisions should still be appropriately documented. This process recognizes that even "small" decisions should be risk-based.

8.5.4.4 Periodic Re-Accreditation

Periodically, it is useful to formally re-examine the security of a system from a wider perspective. Is the security still sufficient? Are major changes needed? The analysis should address these types of questions.

The analysis leads to re-accreditation. The re-accreditation 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 of them need be performed periodically). The more extensive the 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 which result in major or minor changes. After changes have been made to the system, testing (including certification) may be needed. Management then accredits the system for continued operation if the risk is acceptable.

8.5.5 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 of retrieving the information in the future. Electronic information is generally easier to retrieve and store, but it is possible that the technology used to create the records will not be readily available in the future.

> 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.

Since electronic information is easy to copy and transmit, confidential information needs to be controlled throughout the computer system life cycle, so that managers can assure its proper disposition. The destruction of information from a storage medium (such as hard disk or tape) is called *sanitization*. There are three methods of sanitizing media: overwriting, degaussing (for magnetic media only), and destruction.

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 which cannot be sanitized without destruction. The disposition of software must be in keeping with its license or other agreements with the developer, if applicable. Some licenses are site-specific or contain other agreements which prevent the software from being transferred.

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

8.6 Interdependencies

Like many management controls, life cycle planning is interdependent with most other controls. All computer security controls, after all, happen during the computer system life cycle. Three main control areas which are closely linked to life cycle management 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, including system upgrades, and in periodic re-accreditation.

8.7 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 which is susceptible to many types of loss. In the second case, the cost of life cycle management should be *much smaller* than the reduction in losses. The major cost considerations for life cycle management are personnel costs and some delays as the system progresses through the life cycle for completion of analyses, reviews, and obtaining management approvals.

It is certainly possible to over-manage 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, sensitivity, and the risks associated with the system. In general, the higher the value of the system, the newer the system architecture, technologies, and practices, and the worse the impact if the system security fails, the more effort should be spent on life cycle management.

8.8 Summary

Life cycle management of the security of a system helps to ensure that security is considered in the system initiation, development or acquisition, implementation, operation and maintenance, and disposal. The life cycle discussed in this chapter provides a framework for the security-relevant events that happen throughout a system's life cycle.

8.9 References

A Framework for Security Risk Management in Information Technology Systems. Communications Security Establishment, Canada.

Disposition of Sensitive Automated Information. Computer System Laboraroy Bulletin.

National Institute of Standards and Technology. October, 1992.

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

Guideline for Computer Security Certification and Accreditation. FIPS PUB 102. National Institute of Standards and Technology. September 1983.

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

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

Ruthberg, et.al. *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach*. Spec. Pub. 500-153. National Institute of Standards and Technology. 1988.

CSL Bulletin, Sensitivity of Information. Computer System Laboraroy Bulletin. National Institute of Standards and Technology. Novermber, 1992.

Vickers Benzel, T. C. *Developing Trusted Systems Using DOD-STD-2167A*. IEEE, 1990.

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

9 Assurance

9.1 Introduction

Computer security assurance is the degree of confidence one has that the security measures work as intended to protect the system. This includes both the technical and operational safeguards. Like, the closely related areas of reliability and quality, assurance can be a difficult to analyze, but is something people look for and obtain though often without realizing what they have done. For example, people may routinely get product recommendations from colleagues but not think of it as obtaining assurance.

> Security assurance is the degree of confidence one has that the security adequately protects the system.

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. Since the security is supposed to protect the whole system, including the operating system, applications, telecommunications, etc., it is difficult to have assurance about the system as a whole if it is unknown whether the security safeguards work as intended.

Assurance is a challenging subject because it is hard to describe and even harder 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 responsible for the security of the system. This person is the *accrediting official*. Accreditation is discussed in Section 2.

There are many methods and tools for obtaining various degrees of assurance. For discussion purposes, this chapter categorizes assurance in terms of a general system life cycle. The chapter will first discuss planning for assurance and then discuss 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 quite fuzzy. While issues such as configuration management or audits are discussed under operational assurance, they can also be vital during a system's development. The discussion tends to focus more on technical issues during design and implementation assurance and a mixture of management, operational, and technical issues under operational assurance. The reader should keep in mind that the division is somewhat artificial and that there is substantial overlap.

9.2 Accreditation

9.2.1 Background

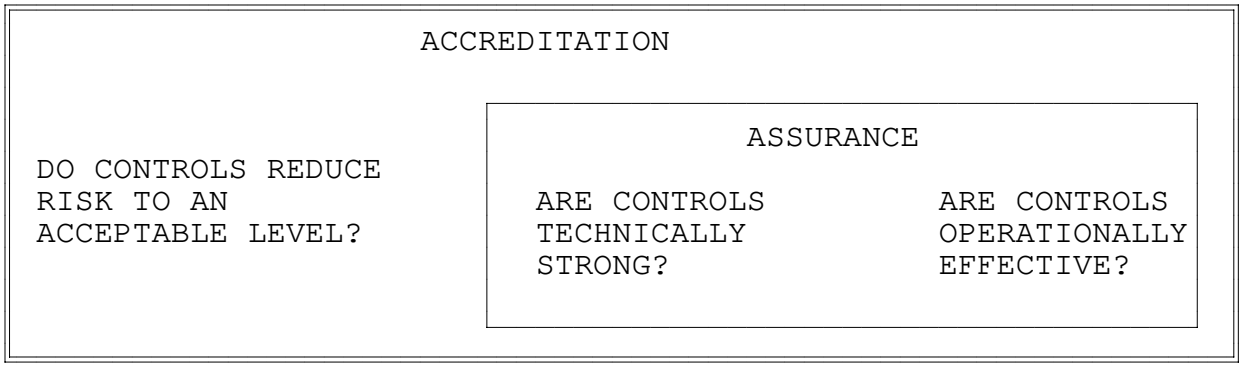
System security accreditation is the formal acceptance of the adequacy of the security of a system by a management official. The best way to view computer security accreditation is as a form of quality control. It forces managers and technical staff to work together to find solutions given security needs, 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 must be based on reliable information about the implementation of both technical and non-technical safeguards. These include:

- technical features (Do they operate as intended?)
- operational practices (Is the system run according to stated procedures?)
- overall security (Are there threats which the technical features and operational practices do not address?)
- remaining risks (Are these risks acceptable?)

Security accreditation should be performed before a computer system becomes operational with periodic re-accreditation performed after major system changes or significant time has elapsed. Even if a system was not initially accredited, the accreditation process can be initiated at any time. The Life Cycle chapter discusses accreditation. (Accreditation is required for federal systems, in accordance with OMB Circular A-130.)

9.2.2 Accreditation and Assurance

Assurance, therefore, is an extremely important -- but not the only -- element in accreditation. Assurance only 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 security requirements are the correct requirements, whether the level of quality is sufficiently high, and whether these requirements are well implemented. These activities are discussed in the Life Cycle and Risk Management chapters.



9.2.3 Selecting Assurance Methods

The accrediting official is the primary arbiter of how much and what types of assurance are needed for a system. It is the accrediting official who makes the final decision about the security of the system and therefore must feel confident about its security. In order for this decision to be an informed decision, the accrediting official must 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. This analysis may be derived from a risk assessment or other study, as deemed appropriate by the accrediting official. At the end of the accreditation process, the accrediting official will be the one to accept the remaining risk.

In selecting assurance methods, the need for assurance must 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. In addition, sometimes a combination of methods can be less costly than extensive testing. The determination of assurance methods must be coordinated with the accrediting official, who will make the final decision whether to accept the adequacy of the security and the residual risk.

The accrediting official, however, is not the only arbiter of assurance. Other officials who use the system should 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 impact the selection of methods. For instance, some of the methods may unduly restrict competition in federal information processing (FIP) resources acquisitions or may be contrary to the organization's privacy policies. Certain assurance methods may be required by organizational policy or directive.

9.3 Planning and Assurance

Assurance planning should begin during the planning phase of a system life cycle. This can be during the planning phase for a new system or for a system upgrade. Planning for assurance at the same time planning is done for other system requirements makes sense. If a

system is going to need extensive testing, it should be built to facilitate such testing.

> If a system or component is being purchased under federal procurement regulations, a plan must be developed prior to solicitation which explains how the government will evaluate the product.

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 assurance options may be much smaller than if the manager had planned for assurance earlier. The remaining assurance options may be more expensive, such as extensive testing, whereas a less expensive alternative may have been possible.

9.4 Design and Implementation Assurance

9.4.1 Background

Design and implementation assurance addresses whether the security features of a system, application, or component meets security requirements and specifications or whether they are they are well designed and well built, i.e., good quality. The source for security requirements and specifications is discussed in the Life Cycle Chapter. Design and implementation assurance examines whether the system is well-built, including its design, development, and installation.

Although design and implementation assurance is associated with the development/acquisition and implementation phase of the system life cycle, it should be considered throughout the life cycle as the system is modified, such as the addition of new capabilities or the maintenance and upgrading of software.

Design and implementation assurance must be looked at 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.

9.4.2 Methods

As stated above, 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 gaining design and implementation assurance.

9.4.2.1 Testing and Certification

Testing can be performed throughout the development cycle, after installation of the system, and throughout the operational phase of the system. Testing can address the quality of the

system as built, as implemented, or as operated. 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 a couple of test cases to indepth studies using metrics, automated tools, or detailed test cases.

Certification is a formal process for testing whether a component or system meets a specified set of security requirements. Certification is normally performed by an independent reviewer, (i.e., one not 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 is performed after system installation but prior to operating the system.

9.4.2.2 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 interoperatibility or strength of security provided. NIST publishes a list of validated products quarterly.

9.4.2.3 Use of Advanced or Trusted Development

In the development of both COTS products and 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.

9.4.2.4 Use of Reliable Architectures

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

9.4.2.5 Use of Reliable Security

Ease of safe use can include a system defaulting to a secure mode.

One factor in reliable security is the concept of *ease of safe use* which postulates that system which is easier to secure will be more likely to be secure. System 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 tested software may be less likely to contain bugs.

9.4.2.6 Evaluations

An evaluation is a analysis of a product, normally including product 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 consortiums. 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 reflects needed security features, the rigor of 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.

9.4.2.7 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 the requirements.

Assurance documentation can address the security for either the system or for specific components. System level documentation should describe the system 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 the applications; it describes the system as *integrated* and *implemented in a particular environment*. Component documentation will generally be an off-the-shelf product, whereas system documentation will generally be developed by the system designer or implementer.

9.4.2.8 Accreditation of Product to Operate in Similar Situation

Accreditations are 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.

9.4.2.9 Self-certification

A vendor, integrator, 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 this method does not provide an impartial review, 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 an independent evaluation or testing.

9.4.2.10 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 product 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.

9.4.2.11 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.

9.4.2.12 Distribution Assurance

It is often important to know that software has arrived unmodified. This is especially important if the software 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 an unreliable source (such as from a bulletin board).

9.5 Operational Assurance

9.5.1 Background

Design and implementation assurance addressed the quality of security features built into systems. Operational assurance addresses the quality of security procedures and practices. Security, unfortunately, 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. Strict adherence to procedures is rare and they become outdated. Errors in system administration are common. Users and administrators often think that nothing will happen to them or their system, so they shortcut security.

Operational assurance addresses whether the system is run according to requirements. It addresses whether technical features are being bypassed or have vulnerabilities and whether procedures are being followed. It does not address changes in the system security requirements. These changes could be caused by changes to the system, its operating environment, or its threats. Changes in the system security requirements are addressed in the

Life Cycle Chapter.

In order to maintain operational assurance, organizations use two basic methods: *system audits* and *monitoring*. These terms are used loosely and often overlap. A system audit is a one-time or periodic event to evaluate security. An audit can vary widely in scope. It could examine an entire system for the purpose of re-accreditation or investigate a single anomalous event. Monitoring refers to an ongoing activity that checks on the system, 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.

9.5.2 Audit

9.5.2.1 Background

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 the Life Cycle Chapter.) Less formal audits are often called security reviews.

Audits can be divided into two types: self-audit and independent audit. Both types of audits can provide excellent information about the security of a system. The essential difference between a self-audit and an independent audit is objectivity. Reviews done by system management staff, often called self-assessments, have an inherent conflict of interest. The system management staff may not have incentive to say that the computer system is poorly designed or sloppily operated. The independent auditor, by contrast, should have no professional stake in the system. Although the system management staff lack objectivity, 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. Independent audit may be performed by a professional audit staff in accordance with generally accepted auditing standards. These audits are generally quite rigorous.

> A person who performs an independent audit should be free from personal and external impairments to independence and should be organizationally independent.

Either type can examine technical, procedural, managerial, or other aspects of security. There are many methods and tools, some of which are described below, which can be used to audit a system. Note that the methods and tools overlap. Additional monitoring methods and tools are described in Section 5.3.2.

9.5.2.2 Methods/Tools

Automated tools. For even a small multi-user computer system, it is a very large job to manually review security features. Automated tools make it feasible to review even large computer systems for a variety of vulnerabilities and threats.

There are two types of automated tools: active and passive. Active tools find vulnerabilities by trying to exploit them. Passive tests 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, integrity of the system software, or whether the system is 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. If system administrators do not take advantage of the tools also, they are at a disadvantage. Many of the tools are simple to use; however, some programs (such as access control auditing tools for large mainframe systems) require specialized skill to use and interpret.

Internal Controls Audit. An auditor can review controls in place and make determinations whether the controls are strong, i.e., do they protect the data processed by the system. The auditor will often analyze both computer and non-computer based controls. Techniques used include inquiry, observation, and testing (of both the controls themselves and 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 federal internal controls audits.

Security Checklists. Within the government, the Computer Security and Privacy Plan (CSPP) provides a checklist against which the system can be audited. This plan, discussed in the Life Cycle Chapter, discusses the major security considerations for a system including management, operational and technical issues. One advantage of using the CSPPs is that the plan 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 must 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.

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

Penetration Testing. Penetration testing can use many methods to try and break into a system. In addition to using active automated tools described above, penetration testing can also be done "manually." The most useful type of penetration testing is to try 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 is a common vulnerability which penetration testing can target. Another method is "social engineering" which involves getting users or administrators to divulge information about the system, especially their passwords.

9.5.3 Monitoring

Many monitoring tools provide realtime security support.

9.5.3.1 Background

Security monitoring is an ongoing activity to look 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 realtime.

9.5.3.2 Methods

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

Automated tools. There are several types of automated tools which monitor a system for security problems. Some examples are:

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

- *Checksums*. 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. Digital signatures can also be used.

- *Password crackers*. A password cracker checks passwords against a dictionary (either a "regular" dictionary or a specialized one with easy-to-guess passwords) and also checks if the password is a common permutation of the userid. Examples of special dictionary entries could be the names of regional sports teams and stars; common permutations could be the userid spelled backwards.

- *Integrity verification programs*. Applications, such as database management systems, can use various programs to look for evidence of data tampering, errors, and omissions. Techniques include consistency and reasonable 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.

- *Intrusion detection*. This topic is covered in the Incident Handling and Audit Chapters. Intrusion detectors analyzes the system audit trail, especially logons, connections, operating system calls, and various command parameters for activity that could represent unauthorized activity.

- *System performance monitoring*. As with intrusion detection, these logs can be analyzed realtime to look for availability problems, including active attacks (such as the 1988 Internet worm) and system and network slowdowns and crashes.

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 adversely affect any of the system's properties, including its security. For this reason, it is helpful to have a computer security expert sit on the configuration control board, or be included in other mechanisms used for configuration management.

Changes to the system can have security implications both because they might introduce or remove vulnerabilities and because significant changes may require updating the contingency plan.

Trade Literature/Publications/Electronic News. In addition to monitoring the system, it is also useful to monitor external sources for information. Sources such as trade literature, both printed and electronic, have information about security vulnerabilities, patches, performance concerns, and other information which could impact security. FIRST, the Forum of Incident Response Teams, has an electronic mailing list which receives information on threats, vulnerabilities, and patches.[41]

Note: There is concern in the computer security community about publicizing security vulnerabilities because it could provide ammunition to hackers. However, system administrators need the information to secure their systems and the information is already spread rapidly in the hacker community.

9.6 Interdependencies

[41]For information on FIRST, send email to FIRST-SEC@FIRST.ORG.

Assurance is an issue for every control and safeguard discussed in this Handbook. Are userid 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 re-emphasized 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, assurance is more widespread than people often realize.

9.7 Cost Considerations

There are many methods of attaining assurance that the 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 to be received against the cost to make a best value decision. In general, personnel costs drive up the cost of assurance. Automated tools tend to be limited to addressing specific problems, but they tend to be less expensive.

9.8 Summary

Assurance is critical to the accreditation process. Since it is accrediting officials who accept risk, it is incumbent on them to demand appropriate assurance of both the technical and operational controls. The accrediting official can choose among the options to best meet their needs and budget constraints, since various kinds and levels of assurance can be achieved by many means.

9.9 References

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

Government Auditing Standards. Washington, DC: GAO.

Guideline for Computer Security Certification and Accreditation. FIPS PUB 102. National Institute of Standards and Technology, September, 1983.

Guideline for Lifecycle Validation, Verification, and Testing of Computer Software. FIPS PUB 101. National Institute of Standards and Technology, June, 1983.

Guideline for Software Verification and Validation Plans. FIPS PUB 132. National Institute of Standards and Technology, November, 1987.

Guttman, Barbara. *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*. Spec. Pub.

800-4. National Institute of Standards and Technology, March, 1992.

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

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

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

Nuegent, W., J. Gilligan, L. Hoffman and Z. Ruthberg, Technology *Assessment: Methods for Measuring the Level of Computer Security*, Spec. Pub. 500-133. National Institute of Standards and Technology, 1985.

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*. SP 800-5. National Institute of Standards and Technology, December, 1992.

Polk, W. Timothy. *Automated Tools for Testing Computer System Vulnerability*. Spec. Pub. 800-6. National Institute of Standards and Technology, December, 1992.

Ruthburg, Zella et. al. *Gudie to Auditing for Controls and Security: A System Development Life Cycle Approach*. Spec. Pub. 500-153. National Institute of Standards and Technology, April, 1988.

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

Wallace, Dolores and J.C. Cherniasvsky. *Guide to Software Acceptance.* Spec. Pub. 500-180. 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*. Spec. Pub. 500-165. National Institute of Standards and Technology, September, 1989.

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