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 establishes the security program and assigns program management and supporting responsibilities.

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

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.

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

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

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:

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.

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.

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.,