National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Generally Accepted Principles and Practices for Securing Information Technology Systems

Marianne Swanson

Barbara Guttman

September 1996

Table of Contents

1. Introduction

As more organizations share information electronically, a common understanding of what is needed and expected in securing information technology (IT) resources is required. This document provides a baseline that organizations can use to establish and review their IT security programs. The document gives a foundation that organizations can reference when conducting multi-organizational business as well as internal business. Management, internal auditors, users, system developers, and security practioners can use the guideline to gain an understanding of the basic security requirements most IT systems should contain. The foundation begins with generally accepted system security principles and continues with common practices that are used in securing IT systems.

1.1 Principles

Many approaches and methods can be used to secure IT systems; however, certain intrinsic expectations must be met whether the system is small or large or owned by a government agency or by a private corporation. The intrinsic expectations are described in this document as generally accepted system security principles. The principles address computer security from a very high-level viewpoint. The principles are to be used when developing computer security programs and policy and when creating new systems, practices or policies. Principles are expressed at a high level, encompassing broad areas, e.g., accountability, cost effectiveness, and integration.

1.2 Practices

The next level in the foundation is the common IT security practices that are in general use today. The practices guide organizations on the types of controls, objectives and procedures that comprise an effective IT security program. The practices show what should be done to enhance or measure an existing computer security program or to aid in the development of a new program. The practices provide a common ground for determining the security of an organization and build confidence when conducting multi-organizational business. This document provides the practices in a checklist format to assist organizations in reviewing their current policies and procedures against the common practices presented here. Organizations should use the practices as a starting point in order to develop additional practices based on their

own organizational and system requirements. The common practices should be augmented with additional practices based on each organization's unique needs. The practices described in this publication come from NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*. They are not intended to be definitive; as technology changes, so will the practices.

1.3 Relationship of Principles and Practices

This document describes eight principles and fourteen practices. Each of the principles applies to each of the practices. The nature of the relationship between the principles and the practices varies. In some cases, practices are derived from one or more principles; in other cases practices are constrained by principles. For example, the Risk Management Practice is directly derived from the Cost-Effectiveness Principle. However, the Comprehensive and Reassessment Principles place constraints on the Risk Management Practice.

While a mapping could be made to the specific relationships between the principles and the practices, it is probably not useful. The important point is that the principles provide the foundation for a sound computer security program.

1.4 Background

The National Performance Review (NPR) recommended as part of the National Information Infrastructure (NII) that the National Institute of Standards and Technology (NIST) develop generally accepted system security principles and practices for the federal government. These security principles and practices are to be applied in the use, protection, and design of government information and data systems, particularly front-line systems for delivering services electronically to citizens.

The need for rules, standards, conventions and procedures that define accepted security practices was outlined in the 1991 National Research Council document *Computers At Risk*. Their recommendation called for the development of a comprehensive set of generally accepted system security principles (GSSP) which would clearly articulate essential security features, assurances, and practices. Work began on implementing the *Computers At Risk* recommendation in 1992

by several national and international organizations with an interest in computer security. This document draws upon their on going efforts.

1.5 Audience

This document has two distinct uses. The chapter covering principles is to be used by all levels of management and by those individuals responsible for computer security at the system level and organization level. The principles are intended as a guide when creating program policy or reviewing existing policy. The common practices are intended as a reference document and an auditing tool. The goal of this document is to provide a common baseline of requirements that can be used within and outside organizations by internal auditors, managers, users and computer security officers. The concepts presented are generic and can be applied to organizations in private and public sectors.

1.6 Structure of this Document

This document is organized as follows: Chapter 2 presents the principles. Chapter 3 contains the common IT security practices. Chapter 4 provides references used in the development of this document.

1.7 Terminology

This document uses the terms information technology security and computer security interchangeably. The terms refer to the entire spectrum of information technology including application and support systems. Computer security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (including hardware, software, firmware, information data, and telecommunications).

2. Generally Accepted System Security Principles

As the name implies, the principles are generally accepted -- that which is most commonly being used at the present time to secure IT resources. The principles that this document offers are not new to the security profession. They are based on the premise that (most) everyone applies these when developing or maintaining a system and they have become generally accepted. This document uses the Organization for Economic Co-operation and Development's (OECD) *Guidelines for the Security of Information Systems* as the base for the principles. The OECD Guidelines were developed in 1992 by a group of international experts to provide a foundation from which governments and the private sector, acting singly and in concert, could construct a framework for securing IT systems. The *OECD Guidelines* are the current international guidelines which have been endorsed by the United States. A brief description of the nine OECD principles is provided in Figure 1. Using the spirit of the *Guideline*s, NIST developed principles which applies to federal systems.[1] In developing this set of principles, NIST drew upon the OECD Guidelines, added material, combined some principles, and rewrote others. Most of the rewriting and combining was done to provide clarity. The principles added by NIST are in keeping

OECD's *Guidelines for the Security of Information Systems* :

Accountability - The responsibilities and accountability of owners, providers and users of information systems and other parties...should be explicit.

Awareness - Owners, providers, users and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures...for the security of information systems.

Ethics - The Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interest of others are respected.

Multidisciplinary - Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints....

Proportionality - Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm....

Integration - Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.

Timeliness - Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.

Reassessment - The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

Democracy - The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

Figure 1. OECD Guidelines.

[1]The eight principles originally appeared as the "Elements of Computer Security" in the NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook.*

with the OECD principles but not directly stated. For example, NIST added the principle that Computer Security Support the Mission of the Organization. Prior to developing these principles, NIST thoroughly reviewed what is currently being accomplished in the IT Security principles area. With much consideration, a determination was made that the U.S. Government would benefit from its own set of principles.

The eight principles contained in this document provide an anchor on which the Federal community should base their IT security programs. These principles are intended to guide agency personnel when creating new systems, practices, or policies. They are not designed to produce specific answers. The principles should be applied as a whole, pragmatically and reasonably. Each principle is expressed as a one-line section heading and explained in the paragraphs that immediately follow.

2.1 Computer Security Supports the Mission of the Organization

The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake -- they are put in place to protect important assets and support the overall organizational mission. Security, therefore, is a means to an end and not an end in itself. For example, in a private-sector business, having good security is usually secondary to the need to make a profit. Security, then, *ought to* increase the firm's ability to make a profit. In a public-sector agency, security is usually secondary to the agency's providing services to citizens. Security, then, *ought to* help improve the service provided to the citizen.

To act on this, managers need to understand both their organizational mission and how each information system supports that mission. After a system's role has been defined, the security requirements implicit in that role can be defined. Security can then be explicitly stated in terms of the organization's mission.

The roles and functions of a system may not be restricted to a single organization. In an interorganizational system, each organization benefits from securing the system. For example, for electronic commerce to be successful, each participant requires security controls to protect their resources. However, good security on the buyer's system also benefits the seller; the buyer's system is less likely to be used for fraud or to be unavailable or otherwise negatively affect the seller. (The reverse is also true.)

2.2 Computer Security is an Integral Element of Sound Management

Information and IT systems are often critical assets that support the mission of an organization. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, or employees.

However, including security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed. Ultimately, organization managers have to decide what level of risk they are willing to accept, taking into account the cost of security controls.

As with other resources, the management of information and computers may transcend organizational boundaries. When an organization's information and IT systems are linked with external systems, management's responsibilities extend beyond the organization. This requires that management (1) know what general level or type of security is employed on the external system(s) or (2) seek assurance that the external system provides adequate security for their organization's needs.

2.3 Computer Security Should Be Cost-Effective

The costs and benefits of security should be carefully examined *in both monetary and non-monetary terms* to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending upon the particular IT system.

In general, security is a smart business practice. By investing in security measures, an organization can reduce the frequency and severity of computer security-related losses. For example, an organization may estimate that it is experiencing significant losses per year in inventory through fraudulent manipulation of its IT system. Security measures, such as an improved access control system, may significantly reduce the loss.

Moreover, a sound security program can thwart hackers and reduce the frequency of viruses. Elimination of these kinds of threats can reduce unfavorable publicity as well as increase morale and productivity.

Security benefits do have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software or fire-suppression systems. Additionally, security measures can sometimes affect system performance, employee morale, or retraining requirements. All of these have to be considered in addition to the basic cost of the control itself. In many cases, these additional costs may well exceed the initial cost of the control (as is often seen, for example, in the costs of administering an access control package). Solutions to security problems should not be chosen if they cost more, in monetary or non monetary terms, directly or indirectly, than simply tolerating the problem.

2.4 Systems Owners Have Security Responsibilities Outside Their Own Organizations

If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be *confident* that the system is adequately secure. This does not imply that all systems must meet any minimum level of security, but does imply that system owners should inform their clients or users about the nature of the security.

In addition to sharing information about security, organization managers "should act in a timely, coordinated manner to prevent and to respond to breaches of security" to help prevent damage to others.[2] However, taking such action should *not* jeopardize the security of systems.

2.5 Computer Security Responsibilities and Accountability Should Be Made Explicit

The responsibility and accountability[3] of owners, providers, and users of IT systems and other parties[4] concerned with the security of IT systems should be explicit.[5] The assignment of responsibilities may be internal to an organization or may extend across organizational boundaries.

Depending on the size of the organization, the computer security program may be large or small, even a collateral duty of another management official. However, even small organizations can prepare a document that states organization policy and makes explicit computer security responsibilities. This element does *not* specify that individual accountability must be provided for on all systems. For example, many information dissemination systems do not require user identification or use other technical means of user identification and, therefore, cannot hold users accountable.

---

[2] Organization for Economic Co-operation and Development, *Guidelines for the Security of Information Systems*, Paris, 1992.

[3] The difference between responsibility and accountability is not always clear. In general, *responsibility* is a broader term, defining obligations and expected behavior. The term implies a proactive stance on the part of the responsible party and a causal relationship between the responsible party and a given outcome. The term *accountability* generally refers to the *ability to hold* people responsible for their actions. Therefore, people could be responsible for their actions but not held accountable. For example, an anonymous user on a system is responsible for behaving according to accepted norms but cannot be held accountable if a compromise occurs since the action cannot be traced to an individual.

[4] The term *other parties* may include but is not limited to: executive management; programmers; maintenance providers; information system managers (software managers, operations managers, and network managers); software development managers; managers charged with security of information systems; and internal and external information system auditors.

[5] This principle implicitly states that people and other entities (such as corporations or governments) have responsibility and accountability related to IT systems which may be shared.

2.6 Computer Security Requires a Comprehensive and Integrated Approach

Providing effective computer security requires a comprehensive approach that considers a variety of areas both within and outside of the computer security field. This comprehensive approach extends throughout the entire information life cycle.

To work effectively, security controls often depend upon the proper functioning of other controls. Many such interdependencies exist. If appropriately chosen, managerial, operational, and technical controls can work together synergistically. On the other hand, without a firm understanding of the interdependencies of security controls, they can actually undermine one another. For example, without proper training on how and when to use a virus-detection package, the user may apply the package incorrectly and, therefore, ineffectively. As a result, the user may mistakenly believe that if their system has been checked once, that it will always be virus-free and may inadvertently spread a virus. In reality, these interdependencies are usually more complicated and difficult to ascertain.

The effectiveness of security controls also depends on such factors as system management, legal issues, quality assurance, and internal and management controls. Computer security needs to work with traditional security disciplines including physical and personnel security. Many other important interdependencies exist that are often unique to the organization or system environment. Managers should recognize how computer security relates to other areas of systems and organizational management.

2.7 Computer Security Should Be Periodically Reassessed

Computers and the environments in which they operate are dynamic. System technology and users, data and information in the systems, risks associated with the system, and security requirements are ever-changing. Many types of changes affect system security: technological developments (whether adopted by the system owner or available for use by others); connection to external networks; a change in the value or use of information; or the emergence of a new threat.

In addition, 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 procedures become outdated over time. These issues make it necessary to reassess periodically the security of IT systems.

2.8 Computer Security is Constrained by Societal Factors

The ability of security to support the mission of an organization may be limited by various factors, such as social issues. For example, security and workplace privacy can conflict. Commonly, security is implemented on an IT system by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. (In some cases, privacy may be mandated by law.)

Although privacy is an extremely important societal issue, it is not the only one. The flow of information, especially between a government and its citizens, is another situation where security may need to be modified to support a societal goal. In addition, some authentication measures may be considered invasive in some environments and cultures.

Security measures should be selected and implemented with a recognition of the rights and legitimate interests of others. This may involve balancing the security needs of information owners and users with societal goals. However, rules and expectations change with regard to the appropriate use of security controls. These changes may either increase or decrease security.

The relationship between security and societal norms is not necessarily antagonistic. Security can enhance the access and flow of data and information by providing more accurate and reliable information and greater availability of systems. Security can also increase the privacy afforded to an individual or help achieve other goals set by society.

3. Common IT Security Practices

The goal of this chapter is to assist the time-constrained security manager in reviewing their current policies and procedures against the common practices presented here. The list is not exhaustive; agencies should consider them as the minimum set. These practices are the ones currently employed in an effective computer security program. They do not take into account environmental or technological constraints, nor are they relevant to every situation. This chapter should be augmented with additional practices based on each agencies' unique requirements.

The practices serve as a companion to the NIST Special Publication, 800-12, *An Introduction to Computer Security: The NIST Handbook.* The *NIST Handbook* contains over 200 pages of assistance in securing computer-based resources. The document explains important concepts, cost considerations, and interrelationships of security controls. It provides a broad overview of computer security and is an excellent primer for anyone interested in computer security. The *NIST Handbook* provides the "why to" and served as the template for deriving the practices.

Each chapter of the *NIST Handbook* was carefully reviewed to determine which sections denoted a practice and which parts were explanation, detail, or example. The key points of each chapter along with a short explanation were placed into a practice format. Some disparity exists, however, in the way the practices are presented. In some sections, it was easy to provide a checklist of what should be considered when, for example, an agency is developing a contingency plan. It was much more difficult to design a checklist of practices for types of technical controls, such as audit trails. In the audit trail section, the reader will find more of a laundry list of what should be considered. Whether the section is a technical control or an operational or management control, each section is formatted as a practice.

Each section begins with a brief explanation of the control and a synopsis of the practice. The controls are then divided into subsections with practices listed below. Each practice appears with a small box placed to the left of it. In most cases, the practice is followed with a brief explanation or example. This section provides the "what" should be done, not the "why" or the "how." Several documents should be referenced for further information. The *NIST Handbook* should be used to obtain additional detail on any of the practices listed. The *NIST Handbook* will easily map to this chapter since the chapters are placed in the same order as the subsections.

The *handbook* also provides many references for further study. This document and the *NIST Handbook* are available electronically as follows:

Anonymous ftp: csrc.nist.gov (129.6.54.11) in the directory nistpubs/800-12
URL: http://csrc.nist.gov/nistpubs/800-12
Dial-up with modem: 301-948-5717

In the early development of this chapter, NIST considered obtaining a copyright release for an excellent practices document that originated in the United Kingdom. Copyright was not obtainable; however, the document was referenced while preparing this chapter. The *Code of Practice for Information Security Management* is written in a similar style and offers short concise practices in IT security. It is highly recommended that this document be obtained as an excellent source for additional information. The document is the British Standard 7799, *A Code of Practice for Information Security Management.* For ordering information, contact BSI Standards at the following:

BSI Standards
389 Cheswick High Road
London W4 4AL
United Kingdom
44-181-996-9000

3.1 Policy

The term *computer security policy* has more than one meaning. Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term policy is also used to refer to the specific security rules for particular systems. Additionally, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization's e-mail privacy policy or fax security policy.

Organizations should have the following three different types of policy: Program, Issue-Specific, and System Specific. (Some organizations may refer to these types with other names such as directives, procedures, or plans.)

3.1.1 Program Policy

An organization's *program policy* should:

- **Create and Define a Computer Security Program.** *Program policy should be clear as to which resources -- including facilities, hardware, and software, information, and personnel -- the computer security program covers.*

- **Set Organizational Strategic Directions.** *This may include defining the goals of the program. For instance, in an organization responsible for maintaining large mission-critical databases, reduction in errors, data loss, data corruption, and recovery might be specifically stressed.*

- **Assign Responsibilities.** Responsibilities should be assigned to the computer security organization for direct program implementation and other responsibilities should be assigned to related offices (such as the Information Resources Management organization).

- **Address Compliance Issues.** *Program policy typically addresses two compliance issues: 1) meeting the requirements to establish a program and the responsibilities*

assigned therein to various organizational components, and 2) the use of specified penalties and disciplinary actions.

3.1.2 Issue-Specific Policy

An organization's *issue-specific policies* should:

- **Address Specific Areas.** *Topics of current relevance and concern to the organization should be addressed. Management may find it appropriate, for example, to issue a policy on how the organization will approach e-mail privacy or Internet connectivity.*

- **Be Updated Frequently.** *More frequent modification is required as changes in technology and related factors take place. If a policy was issued, for example, on the appropriate use of a cutting-edge technology (whose security vulnerabilities are still largely unknown) within the organization, it could require updating.*

- **Contain an Issue Statement.** *The organization's position statement, applicability, roles and responsibilities, compliance, and point of contact should be clear.*

3.1.3 System-Specific Policy

An organization's *system-specific policies* should:

- **Focus on Decisions.** *The decisions taken by management to protect a particular system, such as defining the extent to which individuals will be held accountable for their actions on the system, should be explicitly stated.*

- **Be Made by Management Official.** *The decisions management makes should be based on a technical analysis.*

- **Vary From System to System.** *Variances will occur because each system needs defined security objectives based on the system's operational requirements, environment, and the*

manager's acceptance of risk. In addition, policies will vary based on differing needs for detail.

- **Be Expressed as Rules**. *Who (by job category, organization placement, or name) can do what (e.g., modify, delete) to which specific classes and records of data, and under what conditions.*

3.1.4 All Policies

All three types of policy should be:

- **Supplemented.** *Because policy may be written at a broad level, organizations also develop standards, guidelines, and procedures that offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Standards, guidelines, and procedures may be disseminated throughout an organization via handbooks, regulations, or manuals.*

- **Visible.** *Visibility aids implementation of policy by helping to ensure policy is fully communicated throughout the organization.*

- S**upported by Management.** *Without management support, the policy will become an empty token of management's "commitment" to security.*

- **Consistent.** *Other directives, laws, organizational culture, guidelines, procedures, and organizational mission should be considered.*

3.2 Program Management

Managing computer security at multiple levels brings many benefits. Each level contributes to the overall computer security program with different types of expertise, authority, and resources. In general, executive managers (such as those at the headquarters level) better understand the organization as a whole and have more authority. On the other hand, front-line managers (at the computer facility and applications levels) are more familiar with the specific requirements, both technical and procedural, and problems of the systems and the users. The levels of computer security program management should be complementary; each can help the other be more effective. Many organizations have at least two levels of computer security management; the *central* level and the *system* level.

3.2.1 Central Security Program

A *central security program* should provide distinct types of benefits: increased efficiency and economy of security throughout the organization and the ability to provide centralized enforcement and oversight. It should have the following:

- **Stable Program Management Function.** *The program management function should be stable and recognized within the organization as a focal point for computer security. However complex or simple the program management function is, it requires a stable base, including resources, to perform its activities.*

- **Existence of Policy.** *A program should be based on organizational policy and should create policy, standards, and procedures, as appropriate to address the computer security needs of the organization.*

- **Published Mission and Functions Statement**. *The statement should clearly establish the function of the computer security program and define responsibilities for the computer security program and other related programs and entities. It is often a part of organizational policy.*

- **Long-Term Computer Security Strategies.** *A program should explore and develop long-term strategies to incorporate computer security into the next generation of information technology.*

- **Compliance Program.** A *central computer security program needs to address compliance with national policies and requirements, as well as organization-specific requirements.*

- **Intraorganizational Liaison.** *Computer security often overlaps with other offices, such as safety, reliability and quality assurance, internal control, physical security, or the Office of the Inspector General. An effective program should have established relationships with these groups in order to integrate computer security into the organization's management.*

- **Liaison with External Groups.** *An established program should be knowledgeable of and take advantage of external sources of information. It should also provide information, as appropriate, to external groups.*

3.2.2 System-Level Program

While the central program addresses the entire spectrum of computer security for an organization, *system-level computer security programs* ensure appropriate and cost-effective security for each system. System-level computer security programs may address, for example, the computing resources within an operational element, a major application, or a group of similar systems (either technologically or functionally). They should have the following:

- **System-Specific Security Policy.** *The system policy should document the system security rules for operating or developing the system, such as defining authorized and unauthorized modifications.*

- **Life Cycle Management.** *Systems should be managed to ensure appropriate and cost-effective security. This specifically includes ensuring that security is authorized by*

appropriate management and that changes to the system are made with attention to security (also see Section 3.4).

- **Appropriate Integration with System Operations.** *The people who run the system security program should understand the system, its mission, its technology, and its operating environment. Effective security management needs to be integrated into the management of the system. However, if a computer security program lacks appropriate independence, it may have minimal authority, receive little management attention, and have few resources.*

3.3 Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management requires the analysis of risk, relative to potential benefits, consideration of alternatives, and, finally, implementation of what management determines to be the best course of action. Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one. An organization should consider the following when assessing risks.

3.3.1 Risk Assessment

Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic activities:

- **Determine the Assessment's Scope and Methodology.** *The first step in assessing risk is to identify the system under consideration, the part of the system that will be analyzed, and the analytical method including its level of detail and formality.*

- **Collecting and Analyzing Data.** *The many different components of risk should be examined. This examination normally includes gathering data about the threatened area and synthesizing and analyzing the information to make it useful. The types of areas are:*

  - *Asset Valuation. These include the information, software, personnel, hardware, and physical assets (such as the computer facility). The value of an asset consists of its intrinsic value and the near-term impacts and long-term consequences of its compromise.*

  - *Consequence Assessment. The consequence assessment estimates the degree of harm or loss that could occur.*

  - *Threat Identification. 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, and viruses. Threats should be identified and analyzed to determine the likelihood of their occurrence and their potential to harm assets.

- *Safeguard Analysis. Safeguard analysis should include an examination of the effectiveness of the existing security measures.*

- *Vulnerability Analysis. A vulnerability is a condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.*

- *Likelihood Assessment. Likelihood is an estimation of the frequency or chance of a threat happening. A likelihood assessment considers the presence, tenacity, and strengths of threats as well as the effectiveness of safeguards (or presence of vulnerabilities).*

Interpreting Risk Assessment Results. *The risk assessment must produce a meaningful output that reflects what is truly important to the organization. The risk assessment is used to support two related functions: the acceptance of risk and the selection of cost-effective controls.*

3.3.2 Risk Mitigation

Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management. Although there is flexibility in how risk assessment is conducted, the process of risk mitigation has greater flexibility than the sequence of events conducted in a risk assessment. The following activities are discussed in a specific sequence; however, they need not be performed in that sequence.

Select Safeguards. *The identification of appropriate controls is a primary function of computer security risk management. In selecting appropriate controls, the following factors should be considered:*

- *organizational policy, legislation, and regulation;*

- *safety, reliability, and quality requirements;*
- *system performance requirements;*
- *timeliness, accuracy, and completeness requirements;*
- *the life cycle costs of security measures;*
- *technical requirements; and*
- *cultural constraints.*

- **Accept Residual Risk.** *Management needs to decide if the operation of the IT system is acceptable, given the kind and severity of remaining risks. The acceptance of risk is closely linked with the authorization to use a IT system, often called accreditation. (Accreditation is the acceptance of risk by management resulting in a formal approval for the system to become operational or remain so.)*

- **Implementing Controls and Monitoring Effectiveness.** *The safeguards selected need to be effectively implemented. To continue to be effective, risk management needs to be an ongoing process. This requires a periodic assessment and improvement of safeguards and reanalysis of risks.*

3.3.3 Uncertainty Analysis

Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. An uncertainty analysis should be performed and documented so that the risk management results can be used knowledgeably. There are two primary sources of uncertainty in the risk management process: (1) a lack of confidence or precision in the risk management model or methodology, and (2) 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.

3.4 Life Cycle Planning

Security, like other aspects of an IT system, is best managed if planned for *throughout* the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal.

3.4.1 Security Plan

Organizations should ensure that security activities are accomplished during each of the phases.

- **Prepare a Security Plan.** *A security plan should be used to ensure that security is considered during all phases of the IT system life cycle.*

3.4.2 Initiation Phase

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

- **Conduct a Sensitivity Assessment.** *A sensitivity assessment looks at the sensitivity of the information to be processed and the system itself.*

3.4.3 Development/Acquisition Phase

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. The following steps should be considered during this phase:

- **Determine Security Requirements.** *During the first part of the development/ acquisition phase, security requirements should be developed at the same time system planners define the requirements of the system. 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).*

- **Incorporate Security Requirements Into Specifications.** *Determining security features, assurances, and operational practices can yield significant security information*

and often voluminous requirements. This information needs to be validated, updated, and organized into the detailed security protection requirements and specifications used by systems designers or purchasers.

- **Obtain the System and Related Security Activities.** *If the system is being built, security activities may include developing the system's security features, monitoring the development process itself for security problems, responding to changes, and monitoring threats. Threats or vulnerabilities that may arise during the development phase include Trojan horses, incorrect code, poorly functioning development tools, manipulation of code, and malicious insiders.*

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

    - *In addition to obtaining the system, operational practices need to be developed. These refer to human activities that take place around the system such as contingency planning, awareness and training, and preparing documentation.*

3.4.4 Implementation Phase

During implementation, the system is tested and installed or fielded. The following items should be considered during this phase:

- **Install/Turn-On Controls.** *While obvious, this activity is often overlooked. When acquired, a system often comes with security features disabled. These need to be enabled and configured.*

- **Security Testing.** *System security testing includes both the testing of the particular parts of the system that have been developed or acquired and the testing of the entire system. Security management, physical facilities, personnel, procedures, the use of commercial or in-house services (such as networking services), and contingency planning are*

examples of areas that affect the security of the entire system, but may have been specified outside of the development or acquisition cycle.

- **Accreditation.** *System security accreditation is the formal authorization by the accrediting (management) official for system operation and an explicit acceptance of risk. It is usually supported by a review of the system, including its management, operational, and technical controls.*

3.4.5 Operation/Maintenance Phase

During this phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. The following high-level items should be considered during this phase:

- **Security Operations and Administration.** *Operation of a system involves many security activities discussed in this publication. Performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software are some examples.*

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

- **Audits and Monitoring.** *To maintain operational assurance, organizations use two basic methods: system audits* and *monitoring. These terms are used loosely within the computer security community and often overlap. A system audit is a one-time or periodic event to evaluate security. Monitoring refers to an ongoing activity that examines either the system or the users. In general, the more "real-time" an activity is, the more it falls into the category of monitoring. Figure 2 describes the various forms of auditing and monitoring.*

Audit and Monitoring Techniques

Audit Types. Audits can be self-administered or independent (either internal or external). Both types can provide excellent information about technical, procedural, managerial, or other aspects of security. The essential difference between a self-audit and an independent audit is objectivity.

- Automated Tools. Automated tools can be used to help find a variety of vulnerabilities, such as improper access controls or access control configurations, weak passwords, lack of integrity of the system software, or not using all relevant software updates and patches. There are two types of automated tools: (1) active tools, which find vulnerabilities by trying to exploit them, and (2) passive tests, which only examine the system and infer the existence of problems from the state of the system.

- Internal Controls Audit. An auditor can review controls in place and determine whether they are effective. The auditor will often analyze both computer and noncomputer-based controls.

- Security Checklists. Checklists can be developed, which include national or organizational security policies and practices (often referred to as *baselines*).

- Penetration Testing. Penetration testing can use many methods to attempt a system break-in. In addition to using active automated tools as described above, penetration testing can be done "manually." For many systems, lax procedures or a lack of internal controls on applications are common vulnerabilities that penetration testing can target. Penetration testing is a very powerful technique; it should preferably be conducted with the knowledge and consent of system management.

Monitoring Types. There are many types and methods of monitoring a system or user. Some methods are deemed more socially acceptable and some are illegal. It is wise to check with agency legal council.

- Review of System Logs. A periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours.

- Automated Tools. Several types of automated tools monitor a system for security problems. Some examples are virus scanners, checksumming, password crackers, integrity verification programs, intrusion detectors, and system performance monitoring.

- Configuration Management/Managing Change. 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.

- Trade Literature/Publications/Electronic News. In addition to monitoring the system, it is useful to monitor external sources for information.

- Periodic Reaccreditation. Periodically, it is useful to formally reexamine the security of a system from a wider perspective. The analysis, which leads to reaccreditation, should address such questions as: Is the security still sufficient? Are major changes needed? The reaccreditation should address high-level security and management concerns as well as the implementation of the security.

Figure 2. Audit and Monitoring Techniques.

3.4.6 Disposal Phase

The disposal phase of the IT system life cycle involves the disposition of information, hardware, and software. The following items should be considered during this phase:

- **Information.** *Information may be moved to another system, archived, discarded, or destroyed. When archiving information, consider the method for retrieving the information in the future. While electronic information is generally easier to retrieve and store, the technology used to create the records may not be readily available in the future. Measures may also have to be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys. It is important to consider legal requirements for records retention when disposing of IT systems. For federal systems, system management officials should consult with their agency office responsible for retaining and archiving federal records.*

- **Media Sanitization.** *The removal of information from a storage medium (such as a hard disk or tape) is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by keyboard attack) and purging (rendering information unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, degaussing (for magnetic media only), and destruction.*

3.5 Personnel/User Issues

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

3.5.1 Staffing

An organization's staffing process should generally involve at least the following four steps which apply equally to general users as well as to application managers, system management personnel, and security personnel:

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

  Separation of duties *refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment.*

  Least privilege *refers to the security objective of granting users only those accesses they need to perform their official duties. Data entry clerks, for example, may not have any need to run analysis reports of their database.*

- **Determining Position Sensitivity.** *The responsible manager should determine the position sensitivity, based on the duties and access levels, so that appropriate cost-effective screening can be completed.*

- **Screening.** *Background screening helps determine whether a particular individual is suitable for a given position. In general, it is more effective to use separation of duties and least privilege to limit the sensitivity of the position, rather than relying on screening to reduce the risk to the organization.*

- **Employee Training and Awareness.** *Employees should be trained in the computer security responsibilities and duties associated with their jobs.*

3.5.2 User Administration

Organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access. The following should be considered:

- **User Account Management.** *Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.*

- **Audit and Management Reviews.** *It is necessary to periodically review user account management on a system. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.*

- **Detecting Unauthorized/Illegal Activities.** *Mechanisms besides auditing and analysis of audit trails should be used to detect unauthorized and illegal acts. Rotating employees in sensitive positions, which could expose a scam that required an employee's presence, or periodic rescreening of personnel are methods that can be used.*

Friendly Termination. *Friendly terminations should be accomplished by implementing a standard set of procedures for outgoing or transferring employees. This normally includes:*

- *removal of access privileges, computer accounts, authentication tokens,*
- *the control of keys,*
- *the briefing on the continuing responsibilities for confidentiality and privacy,*
- *return of property, and*
- *continued availability of data. In both the manual and the electronic worlds, this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk, and how are they backed up. Employees should be instructed whether or not to "clean up" their PC before leaving. If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.*

Unfriendly Termination. *Given the potential for adverse consequences, organizations should do the following:*

- *System access should be terminated as quickly as possible when an employee is leaving a position under less than friendly terms. If employees are to be fired, system access should be removed at the same time (or just before) the employees are notified of their dismissal.*
- *When an employee notifies an organization of a resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately terminated.*

- *During the "notice of termination" period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.*

- *In some cases, physical removal from the offices may be necessary.*

3.6 Preparing for Contingencies and Disasters

Contingency planning directly supports an organization's goal of continued operations. Organizations should practice contingency planning because it makes good business sense. Contingency planning addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. This broad perspective on contingency planning is based on the distribution of computer support throughout an organization. The following six steps describe the basic functions an organization should employ when developing contingency plans.

3.6.1 Business Plan

An organization should identify mission- or business-critical functions. The identification of critical functions is often called a *business plan.*

- **Identify Functions and Priorities.** *The business plan should identify functions and set priorities for them. In the event of a disaster, certain functions will not be performed. If appropriate priorities have been set (and approved by senior management), it could mean the difference in the organization's ability to survive a disaster.*

3.6.2 Identify Resources

An organization should identify the resources that support critical functions. Contingency planning should address all the resources needed to perform a function.

- **Analyze Resources Needed.** *The analysis of needed resources should be conducted by those who understand how the function is performed and the interdependencies among various resources. This allows an organization to assign priorities to resources since not all elements are crucial to the critical functions.*

- **Overlap of Areas.** *The identification of resources should cross managers' areas of responsibility.*

- **Common Resources Used**. *The following is a list of resources used by most organizations:*

  People
  Processing Capability (e.g., mainframes, personal computers)
  Computer-Based Services (e.g., telecommunications, world wide web)
  Data and Applications
  Physical Infrastructure
  Documents and Papers (e.g., documentation, blank forms, legal documents)

- **Time Frame Needed.** *In addition, an organization should identify the time frames in which each resource is used (e.g., is the resource needed constantly or only at the end of the month?), and the effect on the mission or business of the continued unavailability of the resource.*

3.6.3 Develop Scenarios

An organization should anticipate potential contingencies or disasters. The development of scenarios should help an organization develop a plan to address the wide range of things that can go wrong. The following items should be considered:

- **Identify Possible Scenarios.** *Although it is impossible to think of all the things that can go wrong, an organization should identify a likely range of problems. Scenarios should include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, can point to other possible, but less obvious, contingencies.*

- **Address Each Resource.** *The contingency scenarios should address each of the resources listed above.*

3.6.4 Develop Strategies

The selection of a contingency planning strategy should be based on practical considerations, including feasibility and cost. Risk assessment can be used to help estimate the cost of options

to decide on an optimal strategy. For example, is it more expensive to purchase and maintain a generator or to move processing to an alternate site, considering the likelihood of losing electrical power for various lengths of time? Whether the strategy is on-site or off-site, a contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption.

- **Emergency Response.** *Document the initial actions taken to protect lives and limit damage.*

- **Recovery.** *Plan the steps that are taken to continue support for critical functions.*

- **Resumption.** *Determine what is required in order to return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the organization will have to operate in the recovery mode.*

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

3.6.5 Test and Revise Plan

An organization should test and revise the contingency plan. A contingency plan should be tested periodically because there will undoubtedly be flaws in the plan and its implementation. The following items should be considered:

- **Keep Current.** *Responsibility for keeping the contingency plan current should be specifically assigned. Update the plan since it will become outdated as time passes and as the resources used to support critical functions change.*

- **Test.** *The extent and frequency of testing will vary between organizations and among systems.*

3.7 Computer Security Incident Handling

A computer security incident can result from a computer virus, other malicious code, or a system intruder, either an insider or an outsider. The definition of a computer security incident is somewhat flexible and may vary by organization and computing environment. An incident handling capability may be viewed as a component of contingency planning, because it provides the ability to react quickly and efficiently to disruptions in normal processing. Incident handling can be considered that portion of contingency planning that responds to malicious technical threats.

3.7.1 Uses of a Capability

An organization should address computer security incidents by developing an incident handling capability. The incident handling capability should be used to:

- **Provide Ability to Respond Quickly and Effectively.**

- **Contain and Repair Damage From Incidents.** *When left unchecked, malicious software can significantly harm an organization's computing, depending on the technology and its connectivity. Containing the incident should include an assessment of whether the incident is part of a targeted attack on the organization or an isolated incident.*

- **Prevent Future Damage.** *An incident handling capability should assist an organization in preventing (or at least minimizing) damage from future incidents. Incidents can be studied internally to gain a better understanding of the organization's threats and vulnerabilities.*

3.7.2 Characteristics

An incident handling capability should have the following characteristics:

- **Understanding of the Constituency It Will Serve.** *The constituency may be external as well as internal. An incident that affects an organization may also affect its trading*

partners, contractors, or clients. In addition, an organization's computer security incident handling capability may be able to help other organizations and, therefore, help protect the community as a whole.

- **Educated Constituency.** *Users need to know about, accept, and trust the incident handling capability or it will not be used. Through training and awareness programs, users can become knowledgeable about the existence of the capability and how to recognize and report incidents. Users trust in the value of the service will build with reliable performance.*

- **Centralized Communications.** *Successful incident handling requires that users be able to report incidents to the incident handling team in a convenient, straightforward fashion without the fear of attribution. An incident handling capability should provide a way for users to report incidents. A centralized communications point is very useful for accessing or distributing information relevant to the incident handling effort. For example, if users are linked together via a network, the incident handling capability can then use the network to send out timely announcements and other information.*

- **Expertise in the Requisite Technologies.** *The technical staff members who comprise the incident handling capability need specific knowledge. Technical capabilities (e.g., trained personnel and virus identification software) should be prepositioned, ready to be used as necessary.*

- **Ability to Communicate Effectively.** *This includes communicating with different types of users, who range from system administrators to unskilled users to management to law-enforcement officials.*

- **Links to Other Groups.** *Other groups assist in incident handling (as needed). The organization should have already made important contacts, both external and internal with other supportive sources (e.g., public affairs, legal, technical, managerial and state and local law enforcement) to aid in containment and recovery efforts. Intruder activity, whether hackers or malicious code, can often affect many systems located at many*

different network sites; handling the incidents can be logistically complex and can require information from outside the organization. By planning ahead, such contacts can be preestablished and the speed of response improved, thereby containing and minimizing damage.

3.8 Awareness and Training

An effective computer security awareness and training program requires proper planning, implementation, maintenance, and periodic evaluation. In general, a computer security awareness and training program should encompass the following seven steps:

- **Identify Program Scope, Goals, and Objectives.** *The scope of the program should provide training to all types of people who interact with IT systems. Since users need training which relates directly to their use of particular systems, a large organization-wide program needs to be supplemented by more system-specific programs.*

- **Identify Training Staff**. *It is important that trainers have sufficient knowledge of computer security issues, principles, and techniques. It is also vital that they know how to communicate information and ideas effectively.*

- **Identify Target Audiences.** *Not everyone needs the same degree or type of computer security information to do their jobs. A computer security awareness and training program that distinguishes between groups of people, presents only the information needed by the particular audienc*e, *and omits irrelevant information will have the best results.*

- **Motivate Management and Employees.** *To successfully implement an awareness and training program, it is important to gain the support of management and employees. Consider using motivational techniques to show management and employees how their participation in a computer security and awareness program will benefit the organization.*

- **Administer the Program.** *Several important considerations for administering the program include visibility, selection of appropriate training methods, topics, materials, and presentation techniques.*

- **Maintain the Program.** *Efforts should be made to keep abreast of changes in computer technology and security requirements. A training program that meets an organization's needs today may become ineffective when the organization starts to use a new application or changes its environment, such as by connecting to the Internet.*

- **Evaluate the Program.** *An evaluation should attempt to ascertain how much information is retained, to what extent computer security procedures are being followed, and general attitudes toward computer security.*

3.9 Security Considerations in Computer Support and Operations

Computer support and operations refers to system administration and tasks external to the system that support its operation (e.g., maintaining documentation). Failure to consider security as part of the support and operations of IT systems is, for many organizations, a significant weakness. Computer security system literature includes many examples of how organizations undermined their often expensive security measures because of poor documentation, no control of maintenance accounts, or other shoddy practices. The following practices are what an organization's support and operation should include:

- **User Support.** *In general, system support and operations staff should provide assistance to users such as with a help desk. Support staff need to be able to identify security problems, respond appropriately, and inform appropriate individuals.*

- **Software Support.** *Controls should be placed on system software commensurate with the risk. The controls should include:*

  - *policies for loading and executing new software on a system. Executing new software can lead to viruses, unexpected software interactions, or software that may subvert or bypass security controls.*

  - *use of powerful system utilities. System utilities can compromise the integrity of operating systems and logical access controls.*

  - *authorization of system changes. This involves the protection of software and backup copies and can be done with a combination of logical and physical access controls.*

  - *license management. Software should be properly licensed and organizations should take steps to ensure that no illegal software is being used. For example, an organization may audit systems for illegal copies of copyrighted software.*

- **Configuration Management.** *Configuration management should ensure that changes to the system do not unintentionally or unknowingly diminish security. The goal is to know how changes will affect system security.*

- **Backups.** *It is critical to back up software and data. Frequency of backups will depend upon how often data changes and how important those changes are. Program managers should be consulted to determine what backup schedule is appropriate. Backup copies should be tested to ensure they are usable. Backups should be stored securely.*

- **Media Controls.** *A variety of measures such as marking and logging, should be used to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media. The extent of media control depends upon many factors, including the type of data, the quantity of media, and the nature of the user environment.*

- **Documentation.** *All aspects of computer support and operations should be documented to ensure continuity and consistency. Security documentation should be designed to fulfill the needs of the different types of people who use it. The security of a system also needs to be documented, including security plans, contingency plans, and security policies and procedures.*

- **Maintenance.** *If someone who does not normally have access to the system performs maintenance, then a security vulnerability is introduced. Procedures should be developed to ensure that only authorized personnel perform maintenance. If a system has a maintenance account, it is critical to change factory-set passwords or otherwise disable the accounts until they are needed. If maintenance is to be performed remotely, authentication of the maintenance provider should be made.*

- **Standardized Log-on Banner.** *Prior to user authentication, the system should display a banner warning that use of the system is restricted to authorized people.*

3.10 Physical and Environmental Security

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics. In doing so, it can help prevent interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

- **Physical Access Controls.** *Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network (LAN) server.*

  - *Physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation.*

  - *It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.*

- **Fire Safety Factors.** *Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data, the risk to human life, and the pervasiveness of the damage. Smoke, corrosive gases, and high humidity from a localized fire can damage systems throughout an entire building. Consequently, it is important to evaluate the fire safety of buildings that house systems.*

- **Failure of Supporting Utilities.** *Systems and the people who operate them need to have a reasonably well-controlled operating environment. Consequently, failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities will*

usually cause a service interruption and may damage hardware. Organizations should ensure that these utilities, including their many elements, function properly.

- **Structural Collapse.** *Organizations should be aware that a building may be subjected to a load greater than it can support. Most commonly this is a result of an earthquake, a snow load on the roof beyond design criteria, an explosion that displaces or cuts structural members, or a fire that weakens structural members.*

- **Plumbing Leaks.** *While plumbing leaks do not occur every day, they can be seriously disruptive. An organization should know the location of plumbing lines that might endanger system hardware and take steps to reduce risk (e.g., moving hardware, relocating plumbing lines, and identifying shutoff valves) .*

- **Interception of Data.** *Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. Organizations should be aware that there are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.*

- **Mobile and Portable Systems.** *The analysis and management of risk usually has to be modified if a system is installed in a vehicle or is portable, such as a laptop computer. The system in a vehicle will share the risks of the vehicle, including accidents and theft, as well as regional and local risks. Organizations should use:*

  - *Secure storage of laptop computers when they are not in use.*

  - *Encrypt data files on stored media, when cost-effective, as a precaution against disclosure of information if a laptop computer is lost or stolen.*

3.11 Identification and Authentication

Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability.[6] Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

3.11.1 Identification

Identification is the means by which a user *provides* a claimed identity to the system. The most common form of identification is the user ID. The following should be considered when using user IDs:

- **Unique Identification.** *An organization should require users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.*

- **Correlate Actions to Users.** *The system should internally maintain the identity of all active users and be able to link actions to specific users. (See audit trails below.)*

- **Maintenance of User IDs.** *An organization should ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deleting former users.*

- **Inactive User IDs.** *User IDs that are inactive on the system for a specific period of time (e.g., 3 months) should be disabled.*

[6] Not all types of access control require identification and authentication.

3.11.2 Authentication

Authentication is the means of establishing the *validity* of this claim. There are three means of authenticating a user's identity *which can be used alone or in combination*: something the individual *knows* (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual *possesses* (a token -- e.g., an ATM card or a smart card); and something the individual *is* (a biometric -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint). The following should be considered:

- **Require Users to Authenticate.** *An organization should require users to authenticate their claimed identities on IT systems. It may be desirable for users to authenticate themselves with a single log-in. This requires the user to authenticate themselves only once and then be able to access a wide variety of applications and data available on local and remote systems.*

- **Restrict Access to Authentication Data.** *An organization should restrict access to authentication data. Authentication data should be protected with access controls and one-way encryption to prevent unauthorized individuals, including system administrators, or hackers from obtaining the data.*

- **Secure Transmission of Authentication Data.** *An organization should protect authentication data transmitted over public or shared data networks. When authentication data, such as a password, is transmitted to an IT system, it can be electronically monitored. This can happen on the network used to transmit the password or on the IT system itself. Simple encryption of a password that will be used again does not solve this problem because encrypting the same password will create the same ciphertext; the ciphertext becomes the password.*

- **Limit Log-on Attempts.** *Organizations should limit the number of log-on attempts. Many operating systems can be configured to lock a user ID after a set number of failed log-on attempts. This helps to prevent guessing of authentication data.*

- **Secure Authentication Data as it is Entered.** *Organizations should protect authentication data as it is entered into the IT system, including suppressing the display of the password as it is entered and orienting keyboards away from view.*

- **Administer Data Properly.** *Organizations should carefully administer authentication data and tokens including procedures to disable lost or stolen passwords or tokens and monitoring systems to look for stolen or shared accounts.*

3.11.3 Passwords

If passwords are used for authentication, organizations should:

- **Specify Required Attributes.** *Secure password attributes such as a minimum length of six, inclusion of special characters, not being in an online dictionary, and being unrelated to the user ID should be specified and required.*

- **Change Frequently.** *Passwords should be changed periodically.*

- **Train Users.** *Teach users not to use easy-to-guess passwords, not to divulge their passwords, and not to store passwords where others can find them.*

3.11.4 Advanced Authentication

Advanced authentication, such as a challenge-response system, generally requires more administrative overhead than passwords. If used, organizations should train users in the following:

- **How to Use.** *In the use of the authentication system including secrecy of PINs, passwords, or cryptographic keys, physical protection of tokens is also required.*

- **Why it is Used.** *To help decrease possible user dissatisfaction, users should be told why this type of authentication is being used.*

3.12 Logical Access Control

Access is the ability to do something with a computer resource (e.g., use, change, or view). Logical access controls are the system-based means by which the ability is explicitly enabled or restricted in some way. Logical access controls can prescribe not only who or what (e.g., in the case of a process) is to have access to a specific system resource but also the type of access that is permitted.

Organizations should implement logical access control based on policy made by a management official responsible for a particular system, application, subsystem, or group of systems. The policy should balance the often-competing interests of security, operational requirements, and user-friendliness. In general, organizations should base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions.

3.12.1 Access Criteria

Organizations should control access to resources based on the following access criteria, as appropriate:

- **Identity (user ID).** *The identity is usually unique in order to support individual accountability, but it can be a group identification or even anonymous.*

- **Roles.** *Access to information may also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access. The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization.*

- **Location.** *Access to particular system resources may be based upon physical or logical location. Similarly, users can be restricted based upon network addresses (e.g., users from sites within a given organization may be permitted greater access than those from outside).*

- **Time.** *Time-of-day and day-of-week/month restrictions are another type of limitation on access. For example, use of confidential personnel files may be allowed only during normal working hours.*

- **Transaction.** *Another criteria can be used by organizations handling transactions. For example, access to a particular account could be granted only for the duration of a transaction, e.g., in an account inquiry a caller would enter an account number and pin. A service representative would be given read access to that account. When completed, the access authorization is terminated. This means that users have no choice in the accounts to which they have access.*

- **Service Constraints.** *Service constraints refer to those restrictions that depend upon the parameters that may arise during use of the application or that are preestablished by the resource owner/manager. For example, a particular software package may be licensed by the organization for only five users at a time. Access would be denied for a sixth user, even if the user were otherwise authorized to use the application. Another type of service constraint is based upon application content or numerical thresholds. For example, an ATM machine may restrict transfers of money between accounts to certain dollar limits or may limit maximum ATM withdrawals to $500 per day.*

- **Access Modes.** *Organizations should consider the types of access, or access modes. The concept of access modes is fundamental to access control. Common access modes, which can be used in both operating or application systems, include read, write, execute, and delete. Other specialized access modes (more often found in applications) include create or search. Of course, these criteria can be used in conjunction with one another.*

3.12.2 Access Control Mechanisms

An organization should consider both internal and external access control mechanisms. *Internal* access controls are a logical means of separating what defined users (or user groups) can or cannot do with system resources. *External* access controls are a means of controlling interactions between the system and outside people, systems, and services. When setting up access controls, organizations should consider the following mechanisms:

- **Access control lists (ACLs).** *ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular system resource and the types of access they have been permitted.*

- **Constrained User Interfaces.** *Access to specific functions are restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types exist: menus, database views, and physically constrained user interface, e.g., an ATM.*

- **Encryption.** *Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management.*

- **Port Protection Devices.** *Fitted to a communications port of a host computer, a port protection device (PPD) authorizes access to the port itself, often based on a separate authentication (such as a dial-back modem) independent of the computer's own access control functions.*

- **Secure Gateways/Firewalls.** *Secure gateways block or filter access between two networks, often between a private network and a larger, more public network such as the Internet. Secure gateways allow internal users to connect to external networks while protecting internal systems from compromise.*

- **Host-Based Authentication.** *Host-based authentication grants access based upon the identity of the host originating the request, instead of the identity of the user making the request. Many network applications in use today use host-based authentication to determine whether access is allowed. Under certain circumstances, it is fairly easy to masquerade as the legitimate host, especially if the masquerading host is physically located close to the host being impersonated.*

Organizations should carefully administer access control. This includes implementing, monitoring, modifying, testing, and terminating user accesses on the system.

Organizations should avoid using passwords as a means of access control which can result in a proliferation of passwords that can reduce overall security. Password-based access control is often inexpensive because it is already included in a large variety of applications. However, users may find it difficult to remember additional application passwords, which, if written down or poorly chosen, can lead to their compromise. Password-based access controls for PC applications are often easy to circumvent if the user has access to the operating system (and knowledge of what to do).

3.13 Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Audit trails should be used for the following:

- **Individual Accountability.** *The audit trail supports accountability by providing a trace of user actions. While users cannot be prevented from using resources to which they have legitimate access authorization, audit trail analysis can be used to examine their actions.*

- **Reconstruction of Events.** *An organization should use audit trails to support after-the-fact investigations of how, when, and why normal operations ceased.*

- **Intrusion Detection.** *If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection. Intrusions can be detected in real time, by examining audit records as they are created or after the fact, by examining audit records in a batch process.*

- **Problem Identification.** *Audit trails may also be used as online tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring.*

3.13.1 Contents of Audit Trail Records

An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. Defining the scope and contents of the audit trail should be done carefully to balance security needs with possible performance, privacy, or other costs. In general, an event record should specify:

- **Type of Event.** *The type of event and its result, such as failed user authentication attempts, changes to users' security information, and organization- and application-specific security-relevant events.*

- **When the Event Occurred.** *The time and day the event occurred should be listed.*

- **User ID Associated With the Event.**

- **Program or Command Used to Initiate the Event.**

3.13.2 Audit Trail Security

Organizations should protect the audit trail from unauthorized access. The following precautions should be taken:

- **Control Online Audit Logs.** *Access to online audit logs should be strictly controlled.*

- **Separation of Duties.** *Organizations should strive for separation of duties between security personnel who administer the access control function and those who administer the audit trail.*

- **Protect Confidentiality.** *The confidentiality of audit trail information also needs to be protected if, for example, it records personal information about users.*

3.13.3 Audit Trail Reviews

Audit trails should be reviewed periodically. The following should be considered when reviewing audit trails:

- **Recognize Normal Activity.** *Reviewers should know what to look for to be effective in spotting unusual activity. They need to understand what normal activity looks like.*

- **Contain a Search Capability.** *Audit trail review can be easier if the audit trail function can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.*

- **Follow-up Reviews.** *The appropriate system-level or application-level administrator should review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.*

- **Develop Review Guidelines.** *Application owners, data owners, system administrators, data processing function managers, and computer security managers should determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities.*

- **Automated Tools.** *Traditionally, audit trails are analyzed in a batch mode at regular intervals (e.g., daily). Audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, can be used in a real-time, or near real-time fashion. Organizations should use the many types of tools that have been developed to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data.*

3.13.4 Keystroke Monitoring

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. If keystroke monitoring is used in audit trails, organizations should:

- **Have Written Policy.** *A policy, in concert with appropriate legal counsel, should be developed.*

- **Notify Users.** *Inform users if keystroke monitoring may take place.*

3.14 Cryptography

Cryptography is a branch of mathematics based on the transformation of data. It provides an important tool for protecting information and is used in many aspects of computer security. Cryptography is traditionally associated only with keeping data secret. However, modern cryptography can be used to provide many security services, such as electronic signatures and ensuring that data has not been modified. Several important issues should be considered when designing, implementing, and integrating cryptography in an IT system.

- **Select Design and Implementation Standards.** *Managers and users of IT systems must select among various standards when deciding to use cryptography. Their selection should be based on cost-effectiveness analysis, trends in the standard's acceptance, and interoperability requirements. In addition, each standard should be carefully analyzed to determine if it is applicable to the organization and the desired application.*

- **Decide on Hardware vs. Software Implementations.** *The trade-offs among security, cost, simplicity, efficiency, and ease of implementation need to be studied by managers acquiring various security products. Cryptography can be implemented in either hardware or software; each has related costs and benefits.*

- **Manage Keys.** *All keys need to be protected against modification, and secret keys and private keys need protection against unauthorized disclosure. Key management involves the procedures and protocols, both manual and automated, used throughout the entire life cycle of the keys. This includes the generation, distribution, storage, entry, use, destruction, and archiving of cryptographic keys.*

- **Secure Cryptographic Modules.** *The proper functioning of cryptography requires the secure design, implementation, and use of the cryptographic module. This includes protecting the module against tampering. Cryptography is typically implemented in a module of software, firmware, hardware, or some combination thereof. This module contains the cryptographic algorithm(s), certain control parameters, and temporary storage facilities for the key(s) being used by the algorithm(s).*

- **Comply with Export Rules.** *Users must be aware that the U.S. Government controls the export of cryptographic implementations. The rules governing export can be quite complex, since they consider multiple factors. In addition, cryptography is a rapidly changing field, and rules may change from time to time. Questions concerning the export of a particular implementation should be addressed to appropriate legal counsel.*

4. References

British Standards Institution. *British Standard 7799, A Code of Practice for Information Security.* 1995

Datapro. *The Quest for Generally Accepted System Security Principles (GSSP).* Delran NJ, October 1994

National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800-12. 1995.

National Institute of Standards and Technology. *Minimum Security Requirements for Multi-User Operating Systems.* NISTIR 5153. March 1993.

National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC, National Academy Press, 1991

Organization for Economic Co-operation and Development. *Guidelines for the Security of Information Systems.* Paris, 1992

Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force. *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information.* June 6, 1995