Special Publication 800-30 Rev A

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

Risk Management Guide for Information Technology Systems

Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa

NIST Special Publication 800-30 Rev A

Risk Management Guide for Information Technology Systems

Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa

C O M P U T E R S E C U R I T Y

U.S. DEPARTMENT OF COMMERCE

Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION

Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Arden L. Bement, Jr., Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. The Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-30
Natl. Inst. Stand. Technol. Spec. Publ. 800-30 Rev A, 58 pages (January 2004)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

Acknowledgements

Initial Release, October 2001:

The authors, Gary Stoneburner, from NIST and Alice Goguen and Alexis Feringa from Booz Allen Hamilton wish to express their thanks to their colleagues at both organizations who reviewed drafts of this document. In particular, Timothy Grance, Marianne Swanson, and Joan Hash from NIST and Debra L. Banning, Jeffrey Confer, Randall K. Ewell, and Waseem Mamlouk from Booz Allen provided valuable insights that contributed substantially to the technical content of this document. Moreover, we gratefully acknowledge and appreciate the many comments from the public and private sectors whose thoughtful and constructive comments improved the quality and utility of this publication.

Changes in Rev A

1. Consistency with other NIST publications:

   FIPS-199: Added reference to FIPS-199 and made impact level descriptions consistent with that reference. Included impact on individuals.

   SP 800-37: Change DAA to Authorizing Official

   SP 800-53: Change list of management, operational, and technical controls to match outline of 800-53. Also use terms "class" and "family".

2. Change CSA to FISMA

3. More consistent use of terms "threat-source", "threat", "flaw or weakness", and "vulnerability" in accordance with definitions given.

4. Reversed order of vulnerability analysis and threat analysis. Threat is threat-source/vulnerability pair, so although threat-source and vulnerability can be analyzed in parallel, threat analysis cannot be performed until after vulnerability analysis has been conducted.

5. Consolidated discussion on security controls in step 4 "Analyze Controls".

6. Improved threat examples.

7. Editorial changes.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems[1] to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT-related risk.

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the *organization and its ability to perform their mission*, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

1.1 AUTHORITY

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

1.2 PURPOSE

Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks.

---

1 The term "IT system" refers to a general support system (e.g., mainframe computer, mid-range computer, local area network, agencywide backbone) or a major application that can run on a general support system and whose use of information resources satisfies a specific set of user requirements.

In addition, this guide provides information on the selection of cost-effective security controls.[2] These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information.

Organizations may choose to expand or abbreviate the comprehensive processes and steps suggested in this guide and tailor them to their environment in managing IT-related mission risks.

1.3 OBJECTIVE

The objective of performing risk management is to enable the organization to accomplish its mission(s) (1) by better securing the IT systems that store, process, or transmit organizational information; (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and (3) by assisting management in authorizing (or accrediting) the IT systems[3] on the basis of the supporting documentation resulting from the performance of risk management.

1.4 TARGET AUDIENCE

This guide provides a common foundation for experienced and inexperienced, technical, and non-technical personnel who support or use the risk management process for their IT systems. These personnel include—

- Senior management, the mission owners, who make decisions about the IT security budget.
- Federal Chief Information Officers, who ensure the implementation of risk management for agency IT systems and the security provided for these IT systems
- The Authorizing Official, who is responsible for the final decision on whether to allow operation of an IT system
- The IT security program manager, who implements the security program
- Information system security officers (ISSO), who are responsible for IT security
- IT system owners of system software and/or hardware used to support IT functions.
- Information owners of data stored, processed, and transmitted by the IT systems
- Business or functional managers, who are responsible for the IT procurement process
- Technical support personnel (e.g., network, system, application, and database administrators; computer specialists; data security analysts), who manage and administer security for the IT systems

[2] The terms "safeguards" and "controls" refer to risk-reducing measures; these terms are used interchangeably in this guidance document.

[3] Office of Management and Budget's November 2000 Circular A-130 and the Government Information Security Reform Act of October 2000 require that an IT system be authorized prior to operation and reauthorized at least every 3 years thereafter.

- IT system and application programmers, who develop and maintain code that could affect system and data integrity
- IT quality assurance personnel, who test and ensure the integrity of the IT systems and data
- Information system auditors, who audit IT systems
- IT consultants, who support clients in risk management.

1.5 RELATED REFERENCES

This guide is based on the general concepts presented in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-27, *Engineering Principles for IT Security,* along with the principles and practices in NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*. This document is consistent with FIPS-199, *Standards for Security Categorization of Information and Information Systems*, NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*, and NIST SP 800-53 *Guide for the Selection and Specification of Security Controls for Information Systems*. In addition, this document is consistent with the policies presented in Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources"; the Government Information Security Reform Act of October 2000, and Title III of the E-Government Act, entitled the *Federal Information Security Management Act (FISMA)*.

1.6 GUIDE STRUCTURE

The remaining sections of this guide discuss the following:

- Section 2 provides an overview of risk management, how it fits into the system development life cycle (SDLC), and the roles of individuals who support and use this process.
- Section 3 describes the risk assessment methodology and the nine primary steps in conducting a risk assessment of an IT system.
- Section 4 describes the risk mitigation process, including risk mitigation options and strategy, approach for control implementation, control categories, cost-benefit analysis, and residual risk.
- Section 5 discusses the good practice and need for an ongoing risk evaluation and assessment and the factors that will lead to a successful risk management program.

This guide also contains six appendixes. Appendix A provides sample interview questions. Appendix B provides a sample outline for use in documenting risk assessment results. Appendix C contains a sample table for the safeguard implementation plan. Appendix D provides a list of the acronyms used in this document. Appendix E contains a glossary of terms used frequently in this guide. Appendix F lists references.

2. RISK MANAGEMENT OVERVIEW

This guide describes the risk management methodology, how it fits into each phase of the SDLC, and how the risk management process is tied to the process of system authorization (or accreditation).

2.1 IMPORTANCE OF RISK MANAGEMENT

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. Section 3 of this guide describes the risk assessment process, which includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. Section 4 describes risk mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. Section 5 discusses the continual evaluation process and keys for implementing a successful risk management program. The authorizing official is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing (or accrediting) the IT system for operation.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. Take the case of home security, for example. Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the homeowners have weighed the cost of system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need.

The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real-world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

2.2 INTEGRATION OF RISK MANAGEMENT INTO SDLC

Minimizing negative impact on an organization and need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems. Effective risk management must be totally integrated into the SDLC. An IT system's SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. In some cases, an IT system may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC. Table 2-1 describes the characteristics

of each SDLC phase and indicates how risk management can be performed in support of each phase.

Table 2-1 Integration of Risk Management into the SDLC

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	• Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	• The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	• The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	• Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	• Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

2.3 KEY ROLES

Risk management is a management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process.

- **Senior Management.** Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.
- **Chief Information Officer (CIO).** The CIO is responsible for the agency's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.
- **System and Information Owners.** The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. Typically the system and information owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.
- **Business and Functional Managers.** The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources.
- **ISSO.** IT security program managers and computer security officers are responsible for their organizations' security programs, including risk management. Therefore, they play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the IT systems that support their organizations' missions. ISSOs also act as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis.
- **IT Security Practitioners.** IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their IT systems. As changes occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.

- **Security Awareness Trainers (Security/Subject Matter Professionals).** The organization's personnel are the users of the IT systems. Use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

3. RISK ASSESSMENT

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, as discussed in Section 4.

Risk is a function of the ***likelihood*** of a given ***threat-source's*** exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization or on individuals.

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential impacts to individuals or to the organization, its mission, or its assets and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps, which are described in Sections 3.1 through 3.9—

- Step 1—System Characterization (Section 3.1)
- Step 2—Vulnerability Identification (Section 3.2)
- Step 3—Threat Identification (Section 3.3)
- Step 4—Control Analysis (Section 3.4)
- Step 5—Likelihood Determination (Section 3.5)
- Step 6—Impact Analysis (Section 3.6)
- Step 7—Risk Determination (Section 3.7)
- Step 8—Control Recommendations (Section 3.8)
- Step 9—Results Documentation (Section 3.9).

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed. Figure 3-1 depicts these steps and the inputs to and outputs from each step.

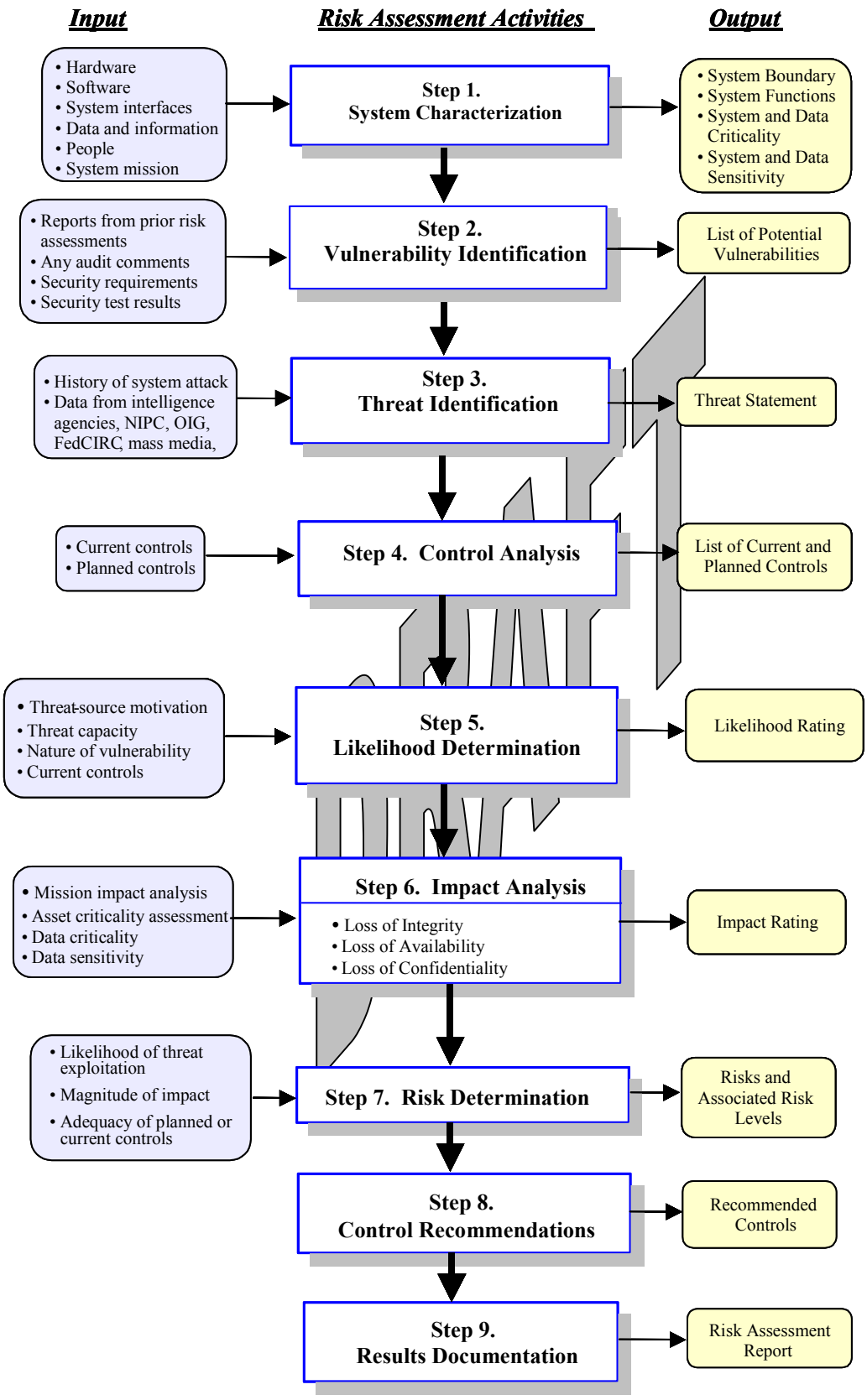

Figure 3-1. Risk Assessment Methodology Flowchart

3.1 STEP 1: SYSTEM CHARACTERIZATION

In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.

Section 3.1.1 describes the system-related information used to characterize an IT system and its operational environment. Section 3.1.2 suggests the information-gathering techniques that can be used to solicit information relevant to the IT system processing environment.

The methodology described in this document can be applied to assessments of single or multiple, interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.

3.1.1 System-Related Information

Identifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity.[4]

Additional information related to the operational environmental of the IT system and its data includes, but is not limited to, the following:

- The functional requirements of the IT system
- Users of the system (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)
- System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
- System security architecture

[4] The level of protection required to maintain system and data integrity, confidentiality, and availability.

- Current network topology (e.g., network diagram)
- Information storage protection that safeguards system and data availability, integrity, and confidentiality
- Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)
- Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
- Management controls used for the IT system (e.g., rules of behavior, security planning)
- Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment of the IT system (e.g., facility security, data center policies)
- Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

For a system that is in the initiation or design phase, system information can be derived from the design or requirements document. For an IT system under development, it is necessary to define key security rules and attributes planned for the future IT system. System design documents and the system security plan can provide useful information about the security of an IT system that is in development.

For an operational IT system, data is collected about the IT system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

3.1.2 Information-Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary:

- **Questionnaire.** To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system. The questionnaire could also be used during on-site visits and interviews.
- **On-site Interviews.** Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed). On-site visits also allow risk

assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system. Appendix A contains sample interview questions asked during interviews with site personnel to achieve a better understanding of the operational characteristics of an organization. For systems still in the design phase, on-site visit would be face-to-face data gathering exercises and could provide the opportunity to evaluate the physical environment in which the IT system will operate.

- **Document Review.** Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan[5], security policies) can provide good information about the security controls used by and planned for the IT system. An organization's mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.
- **Use of Automated Scanning Tool.** Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).

Information gathering can be conducted throughout the risk assessment process, from Step 1 (System Characterization) through Step 9 (Results Documentation).

Output from Step 1—Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundary

3.2 STEP 2: VULNERABILITY IDENTIFICATION

The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities; that is, flaws or weaknesses that could be exercised to result in a security breach or a violation of the system's security policy.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

[5] During the initial phase, a risk assessment could be used to develop the initial system security plan.

It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of the IT system and the phase it is in, in the SDLC:

- If the IT system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the vendors' or developers' security product analyses (e.g., white papers).
- If the IT system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.
- If the IT system is operational, the process of identifying vulnerabilities should include an analysis of the IT system security features and the security controls, technical and procedural, used to protect the system.

3.2.1 Vulnerability Sources

The technical and nontechnical vulnerabilities associated with an IT system's processing environment can be identified via the information-gathering techniques described in Section 3.1.2. A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific IT systems (e.g., a specific version of a specific operating system). The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities. Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

- Previous risk assessment documentation of the IT system assessed
- The IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports
- Vulnerability lists, such as the NIST I-CAT vulnerability database (http://icat.nist.gov)
- Security advisories, such as FedCIRC and the Department of Energy's Computer Incident Advisory Capability bulletins
- Vendor advisories
- Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
- Information Assurance Vulnerability Alerts and bulletins for military systems
- System software security analyses.

3.2.2 System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the IT system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test). Test methods include—

- Automated vulnerability scanning tool
- Security test and evaluation (ST&E)
- Penetration testing.[6]

The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], sendmail relaying). However, it should be noted that some of the *potential* vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements. Some of the "vulnerabilities" flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it. Thus, this test method may produce false positives.

ST&E is another technique that can be used in identifying IT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an IT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure that different facets of the IT system are secured. Penetration testing, when employed in the risk assessment process, can be used to assess an IT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes.

The results of these types of optional security testing will help identify a system's vulnerabilities.

Output from Step 2—A list of the system vulnerabilities (observations)[7] that could be exercised by potential threat-sources

[6] The NIST SP draft 800-42, *Network Security Testing Overview*, describes the methodology for network system testing and the use of automated tools.

[7] Because the risk assessment report is not an audit report, some sites may prefer to address the identified vulnerabilities as observations instead of findings in the risk assessment report.

3.3 STEP 3: THREAT IDENTIFICATION

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat (Section 3.5), one must consider potential vulnerabilities (Section 3.2), threat-sources (Section 3.3), and existing controls (Section 3.4).

Threat: The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

3.3.1 Threat-Source Identification

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources and associated vulnerabilities that are applicable to the IT system being evaluated.

Threat-Source: Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.

A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system. The common threat-sources can be classified as natural, human, or environmental.

Common Threat-Sources

- Natural —Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- Human —Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
- Environmental —Long-term power failure, pollution, chemicals, liquid leakage.

In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. For example, although the threat statement for an IT system located in a desert may not include "natural flood" because of the low likelihood of such an event's occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors. A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer's writing a Trojan horse program to bypass system security in order to "get the job done."

3.3.2 Motivation and Actions

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. Table 3-2 presents an overview of many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack. This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system break-ins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threat-sources that have the potential to harm an IT system and its data and that may be a concern where a vulnerability exists.

Table 3-2. Human Threat Sources: Threat-Source, Motivation, and Threat Actions

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat-source exercising a system vulnerability, as described in Section 3.5.

3.3.3 Threat Identification

The threat statement, or the list of potential threat-sources and associated system vulnerabilities, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available. Known threat-sources have been identified by many government and private sector organizations. Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats. Sources of information include, but are not limited to, the following:

- Intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Center)
- Federal Computer Incident Response Center (FedCIRC)
- Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.

Table 3-3 presents examples of threats (vulnerability/threat-source pairs). Notice that the table includes both specific and more general examples. Typically the threat list will combine general threats for breadth of coverage with specific threats for depth of coverage.

Table 3-3. Example Threats

Threat		Example Attack or Event
Vulnerability	**Threat-Source**	
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Criminals (with intent to gain financial advantage) with knowledge of or the ability to discover the vulnerability	Using telnet to XYZ server and browsing financial data with the *guest* ID to gain advantage in competitive procurement
A flaw in the security design of the system has been publicly announced and an exploit has been posted to the Internet	Hackers (motivated by desire for notoriety) with the capability to use publicly available exploits.	Using the public exploit, gain access to the system and perform unauthorized modification of system data to publicly display that they have obtained access
Data center uses water sprinklers to suppress fire and equipment is not protected from water damage	Fire, negligent persons	Water sprinklers are turned on in the data center and equipment is damaged

Output from Step 3—A threat statement containing a list of threat-sources and associated vulnerabilities that these threat-sources could exercise.

3.4 STEP 4: CONTROL ANALYSIS

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

Sections 3.4.1 through 3.4.3, respectively, discuss control methods, control categories, and the control analysis technique.

3.4.1 Control Methods

Security controls encompass the use of technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

Table 3-1 lists security controls organized by classes and families of security controls.

Table 3-1. Security Controls

Security Control Class	Security Control Family
Management Security	• Risk Assessment • Security Planning • System and Services Acquisition • Security Control Review • Processing Authorization
Operational Security	• Personnel Security • Physical and Environmental Protection • Contingency Planning and Operations • Configuration Management • Hardware and Software Maintenance • System and Data Integrity • Media Protection • • Incident Response • Security Awareness and Training
Technical Security	• Identification and Authentication • Logical Access Control • Accountability (including Audit Trails) • System and Communication Protection

3.4.2 Control Categories

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

- Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
- Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

Section 4.4 further explains these controls from the implementation standpoint. The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented).

3.4.3 Control Analysis Technique

During this step, the risk assessment personnel determine whether the security requirements stipulated for the IT system and collected during system characterization are being met by existing or planned security controls. Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy that security control requirement. The outcome of this process is the security requirements checklist. Sources that can be used in compiling such a checklist include, but are not limited to, the following government regulatory and security directives and sources applicable to the IT system processing environment:

- Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA)
- Federal Information Processing Standards Publications
- OMB November 2000 Circular A-130
- Privacy Act of 1974
- System security plan of the IT system assessed
- The organization's security policies, guidelines, and standards
- Industry practices.

The NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy.

The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and noncompliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner. The security requirements checklist can be used to validate security noncompliance as well as compliance. Therefore, it is essential to update such checklists to reflect changes in an organization's control environment (e.g., changes in security policies, methods, and requirements) to ensure the checklist's validity.

Output from Step 4—List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event

3.5 STEP 5: LIKELIHOOD DETERMINATION

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low. Table 3-4 below describes these three likelihood levels.

Table 3-4. Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Output from Step 5—Likelihood rating (High, Medium, Low)

3.6 STEP 6: IMPACT ANALYSIS

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1.1:

- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity.

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).

Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

- **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
- **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.
- **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts. Because of the generic nature of this discussion, this guide designates and describes only the qualitative categories—high, medium, and low impact (see Table 3.5).

Table 3-5. Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Medium	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Quantitative versus Qualitative Assessment

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to—

- An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year)
- An approximate cost for each occurrence of the threat-source's exercise of the vulnerability
- A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

Output from Step 6—Magnitude of impact (High, Medium, or Low)

3.7 STEP 7: RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of—

- The likelihood of a given threat-source's attempting to exercise a given vulnerability
- The magnitude of the impact should a threat-source successfully exercise the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix must be developed. Section 3.7.1 presents a standard risk-level matrix; Section 3.7.2 describes the resulting risk levels.

3.7.1 Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 3.6 below shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low). Depending on the site's requirements and the granularity of risk assessment desired, some sites may use a 4 x 4 or a 5 x 5 matrix. The latter can include a Very Low /Very High threat likelihood and a Very Low/Very High threat impact to generate a Very Low/Very High risk level. A "Very High" risk level may require possible system shutdown or stopping of all IT system integration and testing efforts.

The sample matrix in Table 3-6 shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example,

- The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low
- The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

3.7.2 Description of Risk Level

Table 3-7 describes the risk levels shown in the above matrix. This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Table 3-7. Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's authorizing official must determine whether corrective actions are still required or decide to accept the risk.

Output from Step 7—Risk level (High, Medium, Low)

[8] If the level indicated on certain items is so low as to be deemed to be "negligible" or non significant (value is <1 on risk scale of 1 to 100), one may wish to hold these aside in a separate bucket in lieu of forwarding for management action. This will make sure that they are not overlooked when conducting the next periodic risk assessment. It also establishes a complete record of all risks identified in the analysis. These risks may move to a new risk level on a reassessment due to a change in threat likelihood and/or impact and that is why it is critical that their identification not be lost in the exercise.

3.8 STEP 8: CONTROL RECOMMENDATIONS

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed in Section 4.6, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Output from Step 8—Recommendation of control(s) and alternative solutions to mitigate risk

3.9 STEP 9: RESULTS DOCUMENTATION

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.

A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report. Appendix B provides a suggested outline for the risk assessment report.

Output from Step 9—Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation

4. RISK MITIGATION

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the ***least-cost approach*** and implement the ***most appropriate controls*** to decrease mission risk to an acceptable level, with ***minimal adverse impact*** on the organization's resources and mission.

This section describes risk mitigation options (Section 4.1), the risk mitigation strategy (Section 4.2), an approach for control implementation (Section 4.3), control categories (Section 4.4), the cost-benefit analysis used to justify the implementation of the recommended controls (Section 4.5), and residual risk (Section 4.6).

4.1 RISK MITIGATION OPTIONS

Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options:

- **Risk Assumption.** To accept the potential risk and continue operating the IT system
- **Risk Avoidance.** To avoid the risk by eliminating the risk cause and/or consequence (e.g., add controls that prevent the risk from occurring, remove certain functions of the system, or shut down the system when risks are identified)
- **Risk Limitation.** To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls) or by authorizing operation for a limited time during which additional risk mitigation by other means is being put into place
- **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organization's mission and its IT systems, because of each organization's unique environment and objectives, the option used to mitigate the risk and the methods used to implement controls may vary. The "best of breed" approach is to use appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and nontechnical, administrative measures.

4.2 RISK MITIGATION STRATEGY

Senior management, the mission owners, knowing the potential risks and recommended controls, may ask, "When and under what circumstances should I take action? When shall I implement these controls to mitigate the risk and protect our organization?"

The risk mitigation chart in Figure 4-1 addresses these questions. Appropriate points for implementation of control actions are indicated in this figure by the word YES.

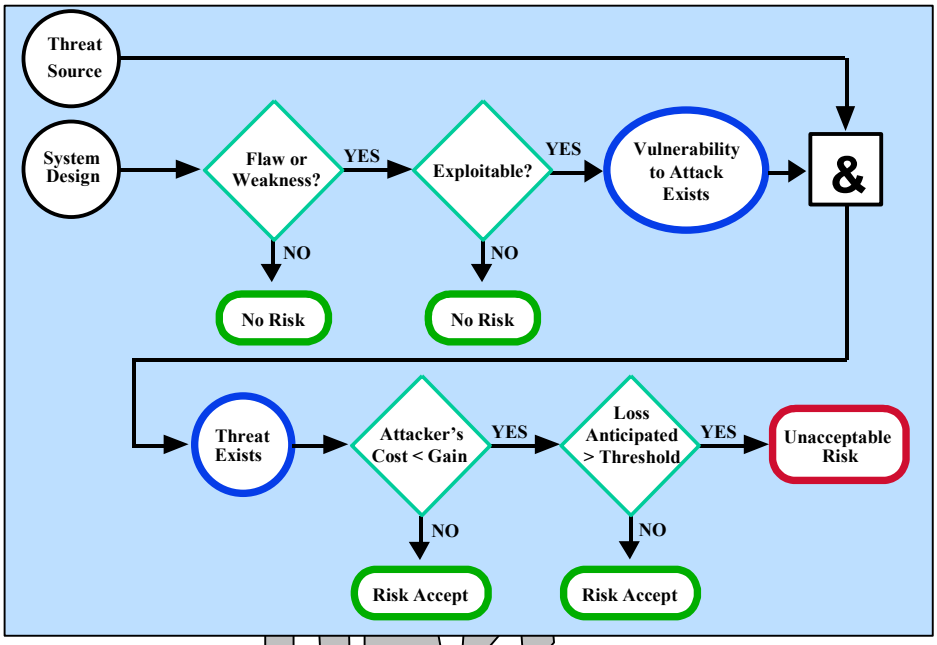

Figure 4-1. Risk Mitigation Action Points

This strategy is further articulated in the following rules of thumb, which provide guidance on actions to mitigate risks from intentional human threats:

- **When a flaw or weakness exists →** implement assurance techniques to remove the associated flaw or weakness and reduce the likelihood of others.
- **When a vulnerability (exploitable flaw or weakness) exists →** apply layered protections, architectural principles, and/or administrative controls to hinder or prevent the ability to exploit the flaw or weakness.
- **When the attacker's cost is less than the potential gain →** apply protections to decrease an attacker's motivation by increasing the attacker's cost or reducing the attacker's gain (for example, administrative protections such as limiting what is processed can significantly reduce attacker's gain).
- **When loss is too great →** apply design and architectural principles and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss. (Again, note that administrative choices such as limiting what is processed may provide the most effective risk mitigation.)

The strategy outlined above, with the exception of the second list item ("When the attacker's cost is less than the potential gain"), also applies to the mitigation of risks arising from natural,

environmental, and unintentional human threat-sources (e.g., system or user errors). (Because there is no "attacker," no motivation or gain is involved.)

4.3 APPROACH FOR CONTROL IMPLEMENTATION

When control actions must be taken, the following rule applies:

Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities.

The following risk mitigation methodology describes the approach to control implementation:

- Step 1—Prioritize Actions

  Based on the risk levels presented in the risk assessment report, the implementation actions are prioritized. In allocating resources, top priority should be given to risk items with unacceptably high risk rankings (e.g., risk assigned a Very High or High risk level). These vulnerability/threat pairs will require immediate corrective action to protect an organization's interest and mission.

  Output from Step 1—Actions ranking from High to Low

- Step 2—Evaluate Recommended Control Options

  The controls recommended in the risk assessment process may not be the most appropriate and feasible options for a specific organization and IT system. During this step, the feasibility (e.g., compatibility, user acceptance) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended control options are analyzed. The objective is to select the most appropriate control option for minimizing risk.

  Output from Step 2—List of feasible controls

- Step 3—Conduct Cost-Benefit Analysis

  To aid management in decision making and to identify cost-effective controls, a cost-benefit analysis is conducted. Section 4.5 details the objectives and method of conducting the cost-benefit analysis.

  Output from Step 3—Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls

- Step 4—Select Control

  On the basis of the results of the cost-benefit analysis, management determines the most cost-effective control(s) for reducing risk to the organization's mission. The controls selected should combine technical, operational, and management control elements to ensure adequate security for the IT system and the organization.

  Output from Step 4—Selected control(s)

- Step 5—Assign Responsibility

  Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is assigned.

  Output from Step 5—List of responsible persons

- Step 6—Develop a Safeguard Implementation Plan

  During this step, a safeguard implementation plan[9] (or action plan) is developed. The plan should, at a minimum, contain the following information:

  – Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report)
  – Recommended controls (output from risk assessment report)
  – Prioritized actions (with priority given to items with Very High and High risk levels)
  – Selected planned controls (determined on the basis of feasibility, effectiveness, benefits to the organization, and cost)
  – Required resources for implementing the selected planned controls
  – Lists of responsible teams and staff
  – Start date for implementation
  – Target completion date for implementation
  – Maintenance requirements.

  The safeguard implementation plan prioritizes the implementation actions and projects the start and target completion dates. This plan will aid and expedite the risk mitigation process. Appendix C provides a sample summary table for the safeguard implementation plan.

  Output from Step 6—Safeguard implementation plan

- Step 7—Implement Selected Control(s)

  Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk. Residual risk is discussed in Section 4.6.

  Output from Step 7—Residual risk

Figure 4-2 depicts the recommended methodology for risk mitigation.

[9] NIST Interagency Report 4749, *Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out.* December 1991.

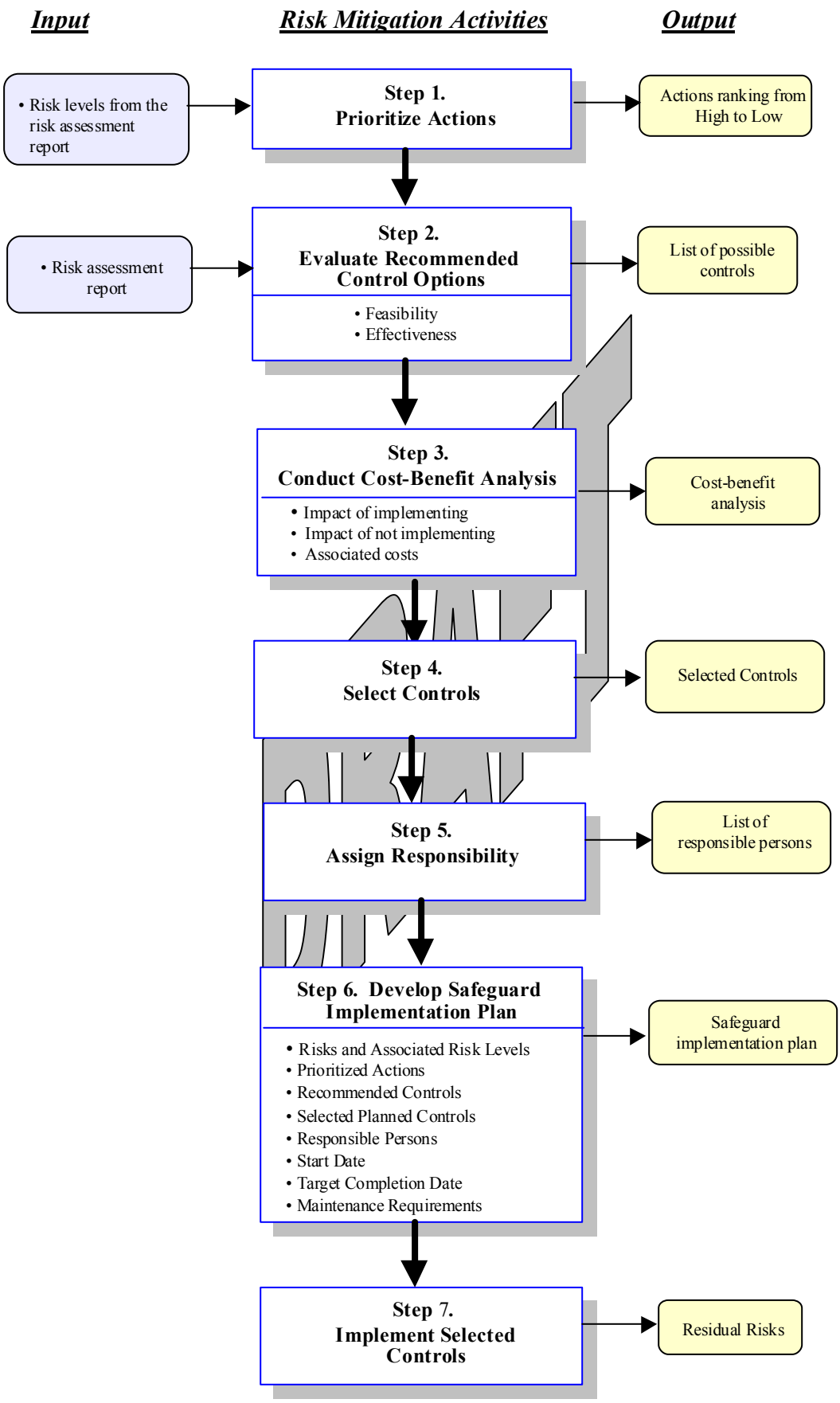

Figure 4-2. Risk Mitigation Methodology Flowchart

4.4 CONTROL CATEGORIES

In implementing recommended controls to mitigate risk, an organization should consider technical, management, and operational security controls, or a combination of such controls, to maximize the effectiveness of controls for their IT systems and organization. Security controls, when used appropriately, can prevent, limit, or deter threat-source damage to an organization's mission.

The control recommendation process will involve choosing among a combination of technical, management, and operational controls for improving the organization's security posture. The trade-offs that an organization will have to consider are illustrated by viewing the decisions involved in enforcing use of complex user passwords to minimize password guessing and cracking. In this case, a technical control requiring add-on security software may be more complex and expensive than a procedural control, but the technical control is likely to be more effective because the enforcement is automated by the system. On the other hand, a procedural control might be implemented simply by means of a memorandum to all concerned individuals and an amendment to the security guidelines for the organization, but ensuring that users consistently follow the memorandum and guideline will be difficult and will require security awareness training and user acceptance.

This section provides a high-level overview of some of the control categories. More detailed guidance about implementing and planning for IT controls can be found in NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems,* and NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook. A catalog of controls is found in NIST SP 800-53 and a more detailed discussion of technical controls is found in NIST SP 800-33.*

Sections 4.4.1 through 4.4.3 provide an overview of technical, management, and operational controls, respectively.

4.4.1 Technical Security Controls

Technical security controls for risk mitigation can be configured to protect against given types of threats. These controls may range from simple to complex measures and usually involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware. All of these measures should work together to secure critical and sensitive data, information, and IT system functions. Technical controls can be grouped into the following major categories, according to primary purpose:

- **Support** (Section 4.4.1.1). Supporting controls are generic and underlie most IT security capabilities. These controls must be in place in order to implement other controls.
- **Prevent** (Section 4.4.1.2). Preventive controls focus on preventing security breaches from occurring in the first place.
- **Detect and Recover** (Section 4.4.1.3). These controls focus on detecting and recovering from a security breach.

Figure 4-3 depicts the primary technical controls and the relationships between them.

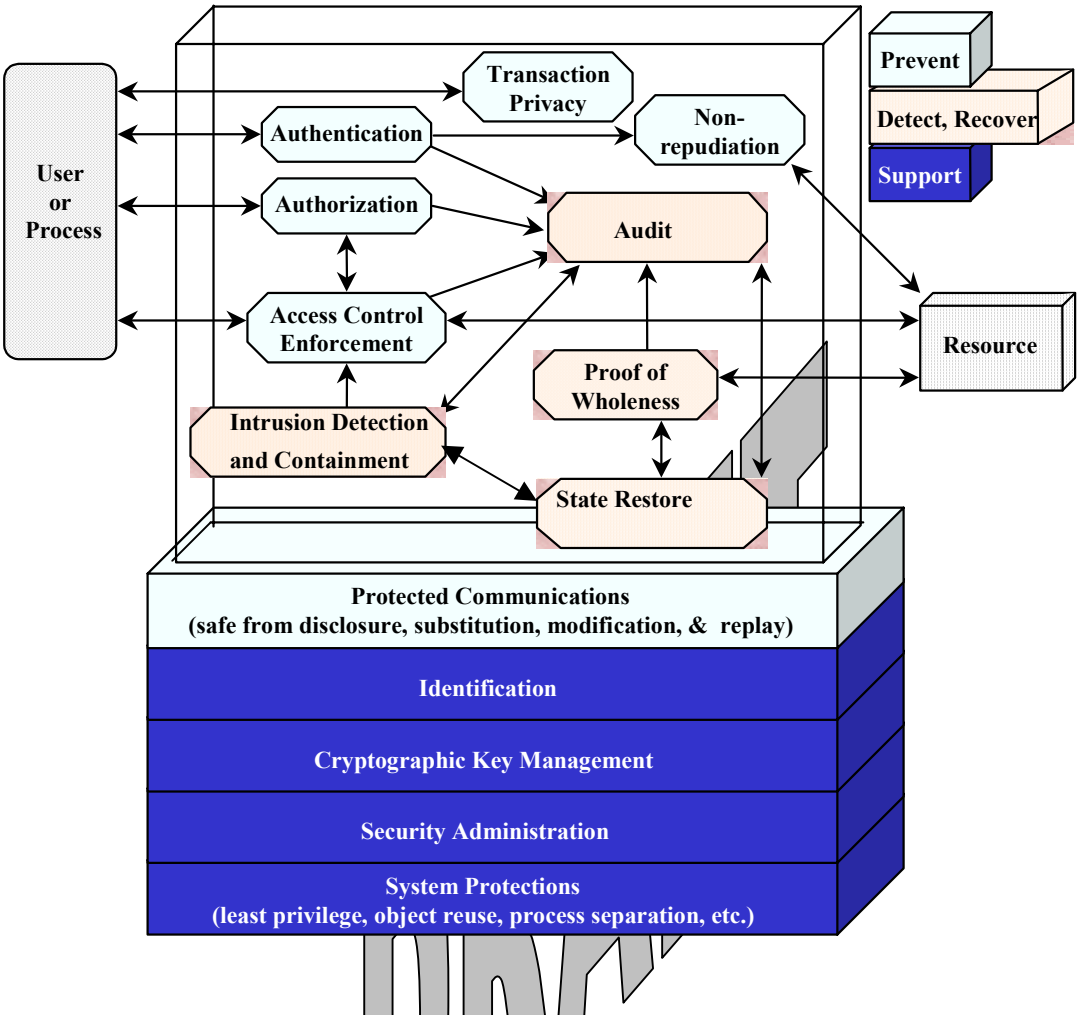

Figure 4-3. Technical Security Controls

4.4.1.1 *Supporting Technical Controls*

Supporting controls are, by their very nature, pervasive and interrelated with many other controls. The supporting controls are as follows:

- **Identification.** This control provides the ability to uniquely identify users, processes, and information resources. To implement other security controls (e.g., discretionary access control [DAC], mandatory access control [MAC], accountability), it is essential that both subjects and objects be identifiable.
- **Cryptographic Key Management.** Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. Cryptographic key management includes key generation, distribution, storage, and maintenance.
- **Security Administration.** The security features of an IT system must be configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment. System security can be built into operating system security or the application. Commercial off-the-shelf add-on security products are available.

- **System Protections.** Underlying a system's various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from the perspective both of the design processes used and of the manner in which the implementation was accomplished. Some examples of system protections are residual information protection (also known as object reuse), least privilege (or "need to know"), process separation, modularity, layering, and minimization of what needs to be trusted.

4.4.1.2 *Preventive Technical Controls*

These controls, which can inhibit attempts to violate security policy, include the following:

- **Authentication.** The authentication control provides the means of verifying the identity of a subject to ensure that a claimed identity is valid. Authentication mechanisms include passwords, personal identification numbers, or PINs, and emerging authentication technology that provides strong authentication (e.g., token, smart card, digital certificate, Kerberos).
- **Authorization.** The authorization control enables specification and subsequent management of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users).
- **Access Control Enforcement.** Data integrity and confidentiality are enforced by access controls. When the subject requesting access has been authorized to access particular processes, it is necessary to enforce the defined security policy (e.g., MAC or DAC). These policy-based controls are enforced via access control mechanisms distributed throughout the system (e.g., MAC sensitivity labels; DAC file permission sets, access control lists, roles, user profiles). The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security).
- **Nonrepudiation.** System accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Nonrepudiation spans both prevention and detection. It has been placed in the prevention category in this guide because the mechanisms implemented prevent the successful repudiation of an action (e.g., the digital certificate that contains the owner's private key is known only to the owner). As a result, this control is typically applied at the point of transmission or reception.
- **Protected Communications.** In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications control ensures the integrity, availability, and confidentiality of sensitive and critical information while it is in transit. Protected communications use data encryption methods (e.g., virtual private network, Internet Protocol Security [IPSEC] Protocol), and deployment of cryptographic technologies (e.g., Data Encryption Standard [DES], Triple DES, RAS, MD4, MD5, secure hash standard, and escrowed encryption algorithms such as Clipper) to minimize network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.

- **Transaction Privacy.** Both government and private sector systems are increasingly required to maintain the privacy of individuals. Transaction privacy controls (e.g., Secure Sockets Layer, secure shell) protect against loss of privacy with respect to transactions performed by an individual.

4.4.1.3 *Detection and Recovery Technical Controls*

Detection controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums. Recovery controls can be used to restore lost computing resources. They are needed as a complement to the supporting and preventive technical measures, because none of the measures in these other areas is perfect. Detection and recovery controls include—

- **Audit.** The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches.
- **Intrusion Detection and Containment.** It is essential to detect security breaches (e.g., network break-ins, suspicious activities) so that a response can occur in a timely manner. It is also of little use to detect a security breach if no effective response can be initiated. The intrusion detection and containment control provides these two capabilities.
- **Proof of Wholeness.** The proof-of-wholeness control (e.g., system integrity tool) analyzes system integrity and irregularities and identifies exposures and potential threats. This control does not prevent violations of security policy but detects violations and helps determine the type of corrective action needed.
- **Restore Secure State.** This service enables a system to return to a state that is known to be secure, after a security breach occurs.
- **Virus Detection and Eradication.** Virus detection and eradication software installed on servers and user workstations detects, identifies, and removes software viruses to ensure system and data integrity.

4.4.2 Management Security Controls

Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards, which are carried out through operational procedures to fulfill the organization's goals and missions.

Management security controls—preventive, detection, and recovery—that are implemented to reduce risk are described in Sections 4.4.2.1 through 4.4.2.3.

4.4.2.1 Preventive Management Security Controls

These controls include the following:

- Assign security responsibility to ensure that adequate security is provided for the mission-critical IT systems
- Develop and maintain system security plans to document current controls and address planned controls for IT systems in support of the organization's mission
- Implement personnel security controls, including separation of duties, least privilege, and user computer access registration and termination
- Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission.

4.4.2.2 Detection Management Security Controls

Detection management controls are as follows:

- Implement personnel security controls, including personnel clearance, background investigations, rotation of duties
- Conduct periodic review of security controls to ensure that the controls are effective
- Perform periodic system audits
- Conduct ongoing risk management to assess and mitigate risk
- Authorize IT systems to address and accept residual risk.

4.4.2.3 Recovery Management Security Controls

These controls include the following:

- Provide continuity of support and develop, test, and maintain the continuity of operations plan to provide for business resumption and ensure continuity of operations during emergencies or disasters
- Establish an incident response capability to prepare for, recognize, report, and respond to the incident and return the IT system to operational status.

4.4.3 Operational Security Controls

An organization's security standards should establish a set of controls and guidelines to ensure that security procedures governing the use of the organization's IT assets and resources are properly enforced and implemented in accordance with the organization's goals and mission. Management plays a vital role in overseeing policy implementation and in ensuring the establishment of appropriate operational controls.

Operational controls, implemented in accordance with a base set of requirements (e.g., technical controls) and good industry practices, are used to correct operational deficiencies that could be

exercised by potential threat-sources. To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing operational controls must be clearly defined, documented, and maintained. These operational controls include those presented in Sections 4.4.3.1 and 4.4.3.2 below.

4.4.3.1 Preventive Operational Controls

Preventive operational controls are as follows:

- Control data media access and disposal (e.g., physical access control, degaussing method)
- Limit external data distribution (e.g., use of labeling)
- Control software viruses
- Safeguard computing facility (e.g., security guards, site procedures for visitors, electronic badge system, biometrics access control, management and distribution of locks and keys, barriers and fences)
- Secure wiring closets that house hubs and cables
- Provide backup capability (e.g., procedures for regular data and system backups, archive logs that save all database changes to be used in various recovery scenarios)
- Establish off-site storage procedures and security
- Protect laptops, personal computers (PC), workstations
- Protect IT assets from fire damage (e.g., requirements and procedures for the use of fire extinguishers, tarpaulins, dry sprinkler systems, halon fire suppression system)
- Provide emergency power source (e.g., requirements for uninterruptible power supplies, on-site power generators)
- Control the humidity and temperature of the computing facility (e.g., operation of air conditioners, heat dispersal).

4.4.3.2 Detection Operational Controls

Detection operational controls include the following:

- Provide physical security (e.g., use of motion detectors, closed-circuit television monitoring, sensors and alarms)
- Ensure environmental security (e.g., use of smoke and fire detectors, sensors and alarms).

4.5 COST-BENEFIT ANALYSIS

To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.

The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. For example, the organization may not want to spend $1,000 on a control to reduce a $200 risk.

A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following:

- Determining the impact of implementing the new or enhanced controls
- Determining the impact of *not* implementing the new or enhanced controls
- Estimating the costs of the implementation. These may include, but are not limited to, the following:
  - Hardware and software purchases
  - Reduced operational effectiveness if system performance or functionality is reduced for increased security
  - Cost of implementing additional policies and procedures
  - Cost of hiring additional personnel to implement proposed policies, procedures, or services
  - Training costs
  - Maintenance costs
- Assessing the implementation costs and benefits against system and data criticality to determine the importance to the organization of implementing the new controls, given their costs and relative impact.

The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization. Just as there is a cost for implementing a needed control, there is a cost for not implementing it. By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forgo its implementation.

Cost-Benefit Analysis Example: System X stores and processes mission-critical and sensitive employee privacy information; however, auditing has not been enabled for the system. A cost-benefit analysis is conducted to determine whether the audit feature should be enabled for System X.

Items (1) and (2) address the intangible impact (e.g., deterrence factors) for implementing or not implementing the new control. Item (3) lists the tangibles (e.g., actual cost).

(1) Impact of enabling system audit feature: The system audit feature allows the system security administrator to monitor users' system activities but will slow down system performance and therefore affect user productivity. Also the implementation will require additional resources, as described in Item 3.

(2) Impact of not enabling system audit feature: User system activities and violations cannot be monitored and tracked if the system audit function is disabled, and security cannot be maximized to protect the organization's confidential data and mission.

(3) Cost estimation for enabling the system audit feature:

Cost for enabling system audit feature—No cost, built-in feature	$	0
Additional staff to perform audit review and archive, per year	$	XX,XXX
Training (e.g., system audit configuration, report generation)	$	X,XXX
Add-on audit reporting software	$	X,XXX
Audit data maintenance (e.g., storage, archiving), per year	$	X,XXX
Total Estimated Costs	$	XX,XXX

The organization's managers must determine what constitutes an acceptable level of mission risk. The impact of a control may then be assessed, and the control either included or excluded, after the organization determines a range of feasible risk levels. This range will vary among organizations; however, the following rules apply in determining the use of new controls:

- If control would reduce risk more than needed, then see whether a less expensive alternative exists
- If control would cost more than the risk reduction provided, then find something else
- If control does not reduce risk sufficiently, then look for more controls or a different control
- If control provides enough risk reduction and is cost-effective, then use it.

Frequently the cost of implementing a control is more tangible than the cost of not implementing it. As a result, senior management plays a critical role in decisions concerning the implementation of control measures to protect the organizational mission.

4.6 RESIDUAL RISK

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission.

Implementation of new or enhanced controls can mitigate risk by—

- Eliminating some of the system's vulnerabilities (flaws and weakness), thereby reducing the number of possible threat-source/vulnerability pairs
- Adding a targeted control to reduce the capacity and motivation of a threat-source

  For example, a department determines that the cost for installing and maintaining add-on security software for the stand-alone PC that stores its sensitive files is not justifiable, but that administrative and physical controls should be implemented to make physical access to that PC more difficult (e.g., store the PC in a locked room, with the key kept by the manager).

- Reducing the magnitude of the adverse impact (for example, limiting the extent of a vulnerability or modifying the nature of the relationship between the IT system and the organization's mission).

The relationship between control implementation and residual risk is graphically presented in Figure 4-4.

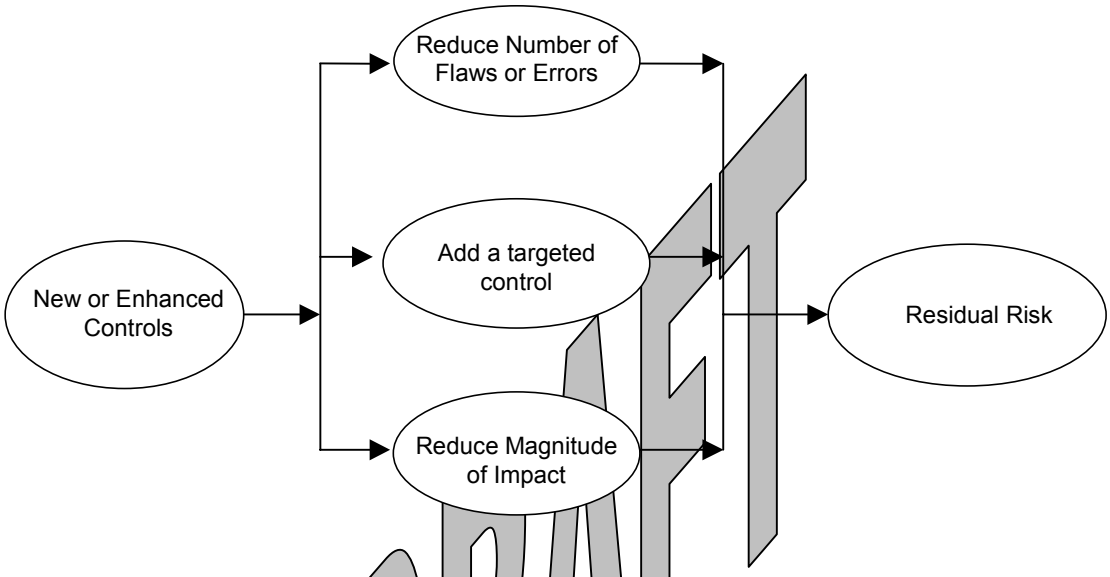

Figure 4-4. Implemented Controls and Residual Risk

The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.

As mandated by OMB Circular A-130, an organization's senior management or the authorizing official, who are responsible for protecting the organization's IT asset and mission, must authorize (or accredit) the IT system to begin or continue to operate. This authorization or accreditation must occur at least every 3 years or whenever major changes are made to the IT system. The intent of this process is to identify risks that are not fully addressed and to determine whether additional controls are needed to mitigate the risks identified in the IT system. For federal agencies, after the appropriate controls have been put in place for the identified risks, the authorizing official will sign a statement accepting any residual risk and authorizing the operation of the new IT system or the continued processing of the existing IT system. If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level.

5. EVALUATION AND ASSESSMENT

In most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

This section emphasizes the good practice and need for an ongoing risk evaluation and assessment and the factors that will lead to a successful risk management program.

5.1 GOOD SECURITY PRACTICE

The risk assessment process is on-going and risk management should be conducted and integrated in the SDLC for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization's business objectives or mission.

5.2 KEYS FOR SUCCESS

A successful risk management program will rely on (1) senior management's commitment; (2) the full support and participation of the IT team (see Section 2.3); (3) the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization; (4) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and (5) an ongoing evaluation and assessment of the IT-related mission risks.

APPENDIX A: SAMPLE INTERVIEW QUESTIONS

Interview questions should be tailored based upon where the IT system assessed is in the SDLC. Sample questions to be asked during interviews with site personnel to gain an understanding of the operational characteristics of an organization may include the following:

- Who are valid users?
- What is the mission of the user organization?
- What is the purpose of the system in relation to the mission?
- How important is the system to the user organization's mission?
- What is the system-availability requirement?
- What information (both incoming and outgoing) is required by the organization?
- What information is generated by, consumed by, processed on, stored in, and retrieved by the system?
- How important is the information to the user organization's mission?
- What are the paths of information flow?
- What types of information are processed by and stored on the system (e.g., financial, personnel, research and development, medical, command and control)?
- What is the sensitivity (or classification) level of the information?
- What information handled by or about the system should not be disclosed and to whom?
- Where specifically is the information processed and stored?
- What are the types of information storage?
- What is the potential impact on the organization if the information is disclosed to unauthorized personnel?
- What are the requirements for information availability and integrity?
- What is the effect on the organization's mission if the system or information is not reliable?
- How much system downtime can the organization tolerate? How does this downtime compare with the mean repair/recovery time? What other processing or communications options can the user access?
- Could a system or security malfunction or unavailability result in injury or death?

APPENDIX B: SAMPLE RISK ASSESSMENT REPORT OUTLINE

EXECUTIVE SUMMARY

I. Introduction

- Purpose
- Scope of this risk assessment

Describe the system components, elements, users, field site locations (if any), and any other details about the system to be considered in the assessment.

II. Risk Assessment Approach

Briefly describe the approach used to conduct the risk assessment, such as—

- The participants (e.g., risk assessment team members)
- The technique used to gather information (e.g., the use of tools, questionnaires)
- The development and description of risk scale (e.g., a 3 x 3, 4 x 4 , or 5 x 5 risk-level matrix).

III. System Characterization

Characterize the system, including hardware (server, router, switch), software (e.g., application, operating system, protocol), system interfaces (e.g., communication link), data, and users. Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort.

IV. Vulnerability Statement

Compile and list potential vulnerabilities applicable to the system assessed.

V. Threat-source Statement

Compile and list the potential threat-sources applicable to the system assessed.

VI. Risk Assessment Results

List the observations (vulnerability/threat-source pairs). Each observation must include—

- Observation number and brief description of observation (e.g., Observation 1: User system passwords can be guessed or cracked)
- A discussion of the threat-source and vulnerability pair
- Identification of existing mitigating security controls
- Likelihood discussion and evaluation (e.g., High, Medium, or Low likelihood)
- Impact analysis discussion and evaluation (e.g., High, Medium, or Low impact)
- Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)
- Recommended controls or alternative options for reducing the risk.

VII. Summary

Total the number of observations. Summarize the observations, the associated risk levels, the recommendations, and any comments in a table format to facilitate the implementation of recommended controls during the risk mitigation process.

APPENDIX C: SAMPLE SAFEGUARD IMPLEMENTATION PLAN SUMMARY TABLE

(1) Threat (Vulnerability/ Threat Pair)	(2) Risk Level	(3) Recommended Controls	(4) Action Priority	(5) Selected Planned Controls	(6) Required Resources	(7) Responsible Team/Persons	(8) Start Date/ End Date	(9) Maintenance Requirement/ Comments
Unauthorized users can telnet to XYZ server and browse sensitive company files with the *guest* ID.	High	• Disallow inbound telnet • Disallow "world" access to sensitive company files • Disable the *guest* ID or assign difficult-to-guess password to the *guest* ID	High	• Disallow inbound telnet • Disallow "world" access to sensitive company files • Disabled the *guest* ID	10 hours to reconfigure and test the system	John Doe, XYZ server system administrator; Jim Smith, company firewall administrator	9-1-2001 to 9-2-2001	• Perform periodic system security review and testing to ensure adequate security is provided for the XYZ server

(1) The threats (threat-source/vulnerability pair) are output from the risk assessment process
(2) The associated risk level of each identified threat is the output from the risk assessment process
(3) Recommended controls are output from the risk assessment process
(4) Action priority is determined based on the risk levels and available resources (e.g., funds, people, technology)
(5) Planned controls selected from the recommended controls for implementation
(6) Resources required for implementing the selected planned controls
(7) List of team(s) and persons who will be responsible for implementing the new or enhanced controls
(8) Start date and projected end date for implementing the new or enhanced controls
(9) Maintenance requirement for the new or enhanced controls after implementation.

APPENDIX D: ACRONYMS

AES	Advanced Encryption Standard
CSA	Computer Security Act
DAC	Discretionary Access Control
DES	Data Encryption Standard
FedCIRC	Federal Computer Incident Response Center
FTP	File Transfer Protocol
ID	Identifier
IPSEC	Internet Security Protocol
ISSO	Information system security officer
IT	Information Technology
ITL	Information Technology Laboratory
MAC	Mandatory Access Control
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PC	Personal Computer
SDLC	System Development Life Cycle
SP	Special Publication
ST&E	Security Test and Evaluation

APPENDIX E: GLOSSARY

TERM	DEFINITION
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or bypass.
Availability	The security goal that generates the requirement for protection against— • Intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data • Unauthorized use of system resources.
Confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.
Denial of Service	The prevention of authorized access to resources or the delaying of time-critical operations.
Due Care	Managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed.
Integrity	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

IT-Related Risk	The net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to— 1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information 2. Unintentional errors and omissions 3. IT disruptions due to natural or man-made disasters 4. Failure to exercise due care and diligence in the implementation and operation of the IT system.
IT Security Goal	See Security Goals
Risk	Within this document, synonymous with IT-Related Risk.
Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.
Risk Management	The total process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.
Security	Information system security is a system characteristic and a set of mechanisms that span the system both logically and physically.
Security Goals	The five security goals are integrity, availability, confidentiality, accountability, and assurance.
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
Threat-source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.
Threat Analysis	The examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

APPENDIX F: REFERENCES

Computer Systems Laboratory Bulletin. *Threats to Computer Systems: An Overview*. March 1994.

NIST Interagency Reports 4749. *Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out.* December 1991.

NIST Special Publication 800-12. *An Introduction to Computer Security: The NIST Handbook*. October 1995.

NIST Special Publication 800-14. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. September 1996. Co-authored with Barbara Guttman.

NIST Special Publication 800-18. *Guide For Developing Security Plans for Information Technology Systems*. December 1998. Co-authored with Federal Computer Security Managers' Forum Working Group.

NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. August 2001.

NIST Special Publication 800-27. *Engineering Principles for IT Security*. June 2001.

OMB Circular A-130. *Management of Federal Information Resources.* Appendix III. November 2000.

FIPS-199. *Standards for Security Categorization of Information and Information Systems*

NIST Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.