# Managing Enterprise Risk in Today's World of Sophisticated Threats

*A Framework for Developing Broad-Based, Cost-Effective Information Security Programs*

Dr. Ron Ross
National Institute of Standards and Technology

Public and private sector enterprises today are almost completely dependent upon their information technology infrastructures to accomplish their critical missions and carry out their corporate business strategies. In order to effectively compete in a fast-paced, highly complex, global economy, organizations are employing new, more powerful information technologies at an unprecedented rate, and in most instances, either ignoring or not fully understanding the increased exposure of their enterprise operations[1] and assets due to the aggressive use of that technology. Recent federal legislation enacted after the September 11, 2001, terrorist attacks, has identified the dependence on information technology and the protection of enterprise missions as a problem of national and economic security that transcends both government and industry.[2] This information technology dependence and urgent need to provide appropriate protection for critical national missions and assets is described in the Patriot Act of 2001, in its definition of U.S. critical infrastructures:

> "*...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters*…"

Critical infrastructures include the energy sector (electrical, nuclear, gas and oil, dams), transportation sector (air, road, rail, port, waterways), public health and emergency services sector, information and telecommunications sector, national defense sector, banking and finance sector, postal and shipping sector, agriculture, food, and water sector, and chemical sector. The fragility of the critical infrastructure is best illustrated by the great blackout of 2003 which left over 50 million people without electricity for an extended period of time after a series of cascading power plant failures across the northeastern United States and Canada. Since the critical infrastructures within the United States are over ninety percent owned and operated by nonfederal entities (including state, local, and tribal governments, private sector firms, and commercial industry), any potential solutions addressing the difficult and challenging protection problems must be broad-based and resonate with both the public and private sectors.

## *GETTING A HANDLE ON THE PROBLEM*

The principal cause of critical infrastructure fragility today can be attributed to *complexity* and *connectivity*. Critical infrastructures are made up of powerful information systems,[3] ranging from small personal digital assistants that manage individual email addresses and appointments to large supercomputers working on complex mathematical and scientific problems. Whether the information system is large or small, there is one common characteristic; the complexity of the hardware and software components that provide the ultimate capability to process, store, and transmit information. Today's information systems contain hardware and firmware devices with many hundreds of thousands of integrated circuits and associated microcode, and software

[1] Enterprise operations include mission, functions, and reputation.

[2] U.S. Patriot Act (Public Law 107-56), October 2001.

[3] An information system is a discrete set of information resources (including information, information technology, personnel, equipment, and funds) organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems and environmental control systems.

programs (including operating systems, middleware, and end-user applications) representing many millions of lines of source code. Understanding the protection issues associated with critical infrastructure information systems and applications requires a fundamental understanding of how the system components are put together and how the components interact while the systems are in operation. In addition to the basic complexity issues described above, government and business enterprises today depend on routinely sharing information and communicating with other organizations. The information systems in these enterprises are connected to the global economy through local and wide area networks using broadband, wireless, and dialup technologies. This ubiquitous connectivity presents serious problems for both government and private sector enterprises as they attempt to protect their operations and assets from an increasing number of sophisticated system and network-based threats worldwide.[4]

The classic dilemma facing organizations today in this fast-paced, highly-competitive, threat-laden world is how aggressively should they be employing the new information technologies to improve productivity and at the same time, maintaining the appropriate safeguards necessary to protect their most important enterprise missions? This is the business of managing enterprise risk. Managing enterprise risk is a fundamental departure from the risk avoidance approaches used by many organizations in the past. Risk management recognizes the need to operate in a highly complex and interconnected world using state-of-the-art information technology—technology that enterprises depend upon to accomplish critical business functions and successfully accomplish corporate-wide missions. Risk management is not an exact science; rather, it brings together the best collective judgments of the individuals responsible for the strategic planning and day-to-day operations of the business enterprises to provide an appropriate level of security for the information systems supporting the ongoing operations and assets of those enterprises. [5]

The commercial information technology products which can be routinely found in today's enterprise information systems, typically contain a significant number of flaws. This situation can be primarily attributed to the large, complex, and functionality-rich nature of the commercial products being developed and marketed. The problem of flaws in information technology products is exacerbated by the highly complex architectures being deployed within enterprises and the less than desirable system and security engineering practices being used to integrate the products into functioning information systems. Flaws in information technology products or in the resulting information systems that can be exploited by threat sources, are described as *vulnerabilities*. Threat sources exploit vulnerabilities in information technology products to compromise the information systems supporting critical enterprise missions. Compromises can be attributed to unauthorized disclosure of information (i.e., a *confidentiality* failure), unauthorized modification of information (i.e., an *integrity* failure), or denial of service (i.e., an *availability* failure). Each of these compromises to information or information systems can have an adverse *impact* on organizational operations, organizational assets, and individuals. The primary task in managing risk is to reduce the vulnerabilities in the information systems supporting the enterprise to an acceptable level. Every enterprise will have to accept some level of residual risk to the enterprise mission or business case. Finding that acceptable balance point is the key challenge to the senior leaders within the enterprise.

---

[4] Threat sources include nation states, terrorist groups, criminals, hackers, or any individuals or groups with intentions of compromising an information system and thus, causing harm to individuals or the enterprise.

[5] Information security will vary from organization to organization depending its mission or business case. An appropriate level of information security is defined to be the application of a sufficient number of information system safeguards (i.e., security controls) to protect the enterprise mission or business case. Acceptability of mission or business case risk may also differ among enterprises that interconnect and share information. A skilled information security professional can assist and advise senior leaders in assessing enterprise risk.

## *ESTABLISHING A COMPREHENSIVE INFORMATION SECURITY PROGRAM*

Managing the risk to enterprise missions associated with the operation of information systems begins with the development of an effective information security program. The Federal Information Security Management Act (FISMA)[6] states that an effective information security program includes:

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and address information security throughout the life cycle of each organizational information system;
- Plans for providing appropriate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization.

The most important aspect of effectively managing the risk to the organization's operations and assets associated with operating enterprise information systems is a fundamental *commitment* to information security on the part of the senior leadership of the organization. This commitment is the internalizing of information security as an essential mission need. Fundamental commitment to information security translates into ensuring sufficient resources (both dollars and people) are available to provide an appropriate level of security for the organization's information systems. Information security must be a top priority within the enterprise and structurally embedded within the infrastructure of the organization. This implies that every new initiative within the enterprise from the development of corporate strategies and programs to the acquisition of goods and services, incorporates information security considerations, preferably as early as possible in the system development life cycle process. Information security requirements must be considered at the same level of importance and criticality as the main stream functional requirements established by the enterprise.

[6] The E-Government Act (P.L. 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

***If the successful accomplishment of enterprise missions depends on information systems, including the information processed, stored, and transmitted by those systems, the systems must be dependable. To be dependable in the face of threats, the systems must be appropriately protected.***

Protection of enterprise missions can result only from the application of a balanced set of *security controls* for information systems supporting the organization's operations and assets. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. This includes the establishment of top-level information security policies, comprehensive procedures that provide the necessary detail to allow individuals within the enterprise to understand their security responsibilities and how to effectively implement the security policies, and an aggressive employment of security technologies including automated security support tools. This balanced approach, sometimes described as a *defense-in-depth* protection strategy, is absolutely essential in creating an information security program that is effective against an increasingly sophisticated and diverse set of threats. Adversaries will exploit weaknesses in an enterprise's information security program, so the balanced application of security safeguards and countermeasures using a defense-in-depth strategy provides the greatest assurance that the operations and assets of the organization are appropriately protected.

There are several important questions that should be answered by organizational officials when addressing the security considerations for their information systems:

- What security controls are needed to appropriately protect the information systems that support the operations and assets of the organization in order for that organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective[7] in their application?

## *THE RISK MANAGEMENT FRAMEWORK*

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of risk. The management of risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, policies, standards, or regulations. The following activities related to managing risk (also known as the NIST *Risk Management Framework*) are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the system development life cycle. Each of the activities in the Risk Management Framework has an associated NIST security standard and/or guidance document that can be used by organizations implementing the framework. The framework represents an iterative *security life cycle process* that focuses on managing risk to enterprise missions:

[7] Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

- ***Categorize*** the information system and the information resident within that system based on a Federal Information Processing Standards (FIPS) 199 impact analysis.[8]
- ***Select*** an initial set of minimum, baseline security controls (i.e., security control foundation) for the information system from NIST Special Publication 800-53, based on the FIPS 199 security categorization. Apply tailoring guidance as appropriate, to obtain the control set used as the starting point for the assessment of risk associated with the use of the system.[9]
- ***Supplement*** the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.[10]
- ***Document*** the agreed-upon set of security controls in the system security plan including the organization's rationale for any refinements or adjustments to the initial set of controls.[11]
- ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.[12]
- ***Assess*** the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.[13]
- ***Authorize*** information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable.[14]
- ***Monitor*** and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.[15]

---

[8] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, specifies mandatory security categories for information systems. Security categorization provides a corporate view of the criticality and sensitivity of the information system with respect to supporting enterprise missions or business case.

[9] NIST Special Publication 800-53, *Minimum Security Controls for Federal Information Systems*, provides guidance for selecting, specifying, and tailoring security controls for information systems.

[10] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance for conducting risk assessments and supplementing baseline security controls. This publication is being revised to align its risk management concepts more closely with the recently-developed NIST Risk Framework.

[11] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance for documenting security controls employed in information systems.

[12] NIST Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, provides guidance for implementing security configuration settings for information systems and linkage to the National Vulnerability Database, patching information, and automated support tools.

[13] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), provides guidance for assessing the effectiveness of security controls using standardized assessment methods and procedures.

[14] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidance on determining risk to organizational operations, organizational assets, and individuals.

[15] NIST Special Publications 800-37 and 800-53A provide guidance on the continuous monitoring of security controls in information systems.

Figure 1 illustrates the specific activities in the NIST Risk Management Framework and the information security standards and guidance documents associated with each activity.

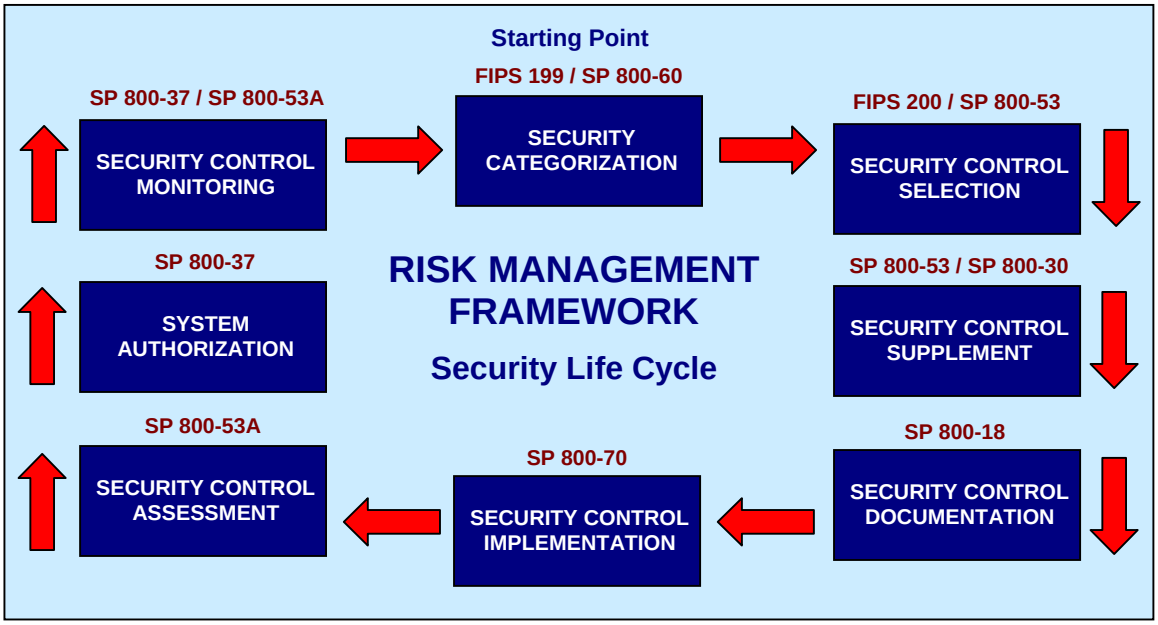


**FIGURE 1: THE NIST RISK MANAGEMENT FRAMEWORK**

## *THE FUNDAMENTAL CONCEPTS USED IN THE FRAMEWORK*

Applying the top-level NIST Risk Management Framework described above requires an understanding of some basic information security concepts. The process of selecting the appropriate security controls for an information system to protect the mission of the enterprise depends upon effectively categorizing the system with regard to its overall criticality/sensitivity and subsequently selecting the appropriate security controls for unique operational environments.

### Establishing Security Categories for Information Systems

FIPS 199, the mandatory federal security categorization standard, is predicated on a simple and well-established concept—determining appropriate priorities for organizational information systems according to mission impact and subsequently applying appropriate measures to protect those systems. The security controls applied to protect a particular information system should be commensurate with the potential impact on organizational operations, organizational assets, or individuals should there be a loss of confidentiality, integrity, or availability. FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information resident on those information systems.[16] The generalized format for expressing the security category (SC) of an information system is:

$$\mathbf{SC}_{\text{information system}} = \{(\mathbf{confidentiality}, \textit{impact}), (\mathbf{integrity}, \textit{impact}), (\mathbf{availability}, \textit{impact})\},$$

where the acceptable values for potential impact are low, moderate, or high.

[16] NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept is once again used to determine the overall impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security control baselines.[17] Thus, a *low-impact* system is defined as an information system in which all three of the security objectives are low. A *moderate-impact* system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a *high-impact* system is an information system in which at least one security objective is high.

Security categorization should be accomplished as an enterprise-wide activity with the involvement of senior-level organizational officials including, but not limited to, chief information officers, senior agency information security officers, authorizing officials (a.k.a. accreditation authorities), information system owners, and information owners. Many times, individual information system owners may tend to either over categorize or under categorize their systems if done in isolation without appropriate feedback and oversight from senior leaders within the organization. The involvement of senior leaders ensures that consistent, realistic security categorizations take place and appropriate security controls are employed to protect critical enterprise missions. The potential impact definitions for each security objective—confidentiality, integrity, and availability, are listed in Appendix A.

***Implementation Tip***

To determine the overall impact level of the information system:

- First, determine the different types of information that are processed, stored, or transmitted by the information system (e.g., financial information, contractor sensitive information, personally identifiable information, audit information, etc.). NIST Special Publication 800-60 provides guidance on a variety of information types commonly used by organizations.
- Second, using the impact levels in FIPS 199 and the recommendations of NIST Special Publication 800-60, categorize the confidentiality, integrity, and availability of each information type as low, moderate, or high impact.
- Third, determine the information system security categorization, that is, the highest impact level for each security objective (confidentiality, integrity, availability) from among the categorizations for the information types associated with the information system.
- Fourth, determine the overall impact level of the information system from the highest impact level among the three security objectives in the system security categorization.

## Minimum Security Requirements for Information Systems

FIPS 200 (a closely related security standard to FIPS 199) specifies minimum security requirements for information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.[18] The standard promotes the development, implementation, and operation of more secure information systems by

[17] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. Accordingly, the security controls in the control catalog are not categorized by security objective—rather, they are grouped into baselines to provide a general protection capability for classes of information systems based on impact level. The application of scoping guidance in NIST Special Publication 800-53 may allow selective security control baseline tailoring.

[18] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

establishing the starting point for determination of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements. The minimum security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of information systems and the information processed, stored, and transmitted by those systems. The security-related areas are:

- Access Control;
- Awareness and Training;
- Audit and Accountability;
- Certification, Accreditation, and Security Assessments;
- Configuration Management;
- Contingency Planning;
- Identification and Authentication;
- Incident Response;
- Maintenance;
- Media Protection;
- Physical and Environmental Protection;
- Planning;
- Personnel Security;
- Risk Assessment;
- Systems and Services Acquisition;
- System and Communications Protection; and
- System and Information Integrity.

The seventeen areas represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting information and information systems. The minimum security requirements for information systems are listed in Appendix B.

Organizations can meet the minimum security requirements in FIPS 200 by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53. The process of selecting the right security controls and assurance requirements for organizational information systems to achieve an appropriate level of information security is a multifaceted, risk-based activity involving management and operational personnel within the organization. Security categorization of information and information systems is the first step in the risk management process. Subsequent to the security categorization, organizations select an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in this standard. The selected set of security controls includes one of three, appropriately tailored security control baselines from NIST Special Publication 800-53 that are associated with the designated impact levels of the organizational information systems as determined during the security categorization process.

- For *low-impact* information systems, organizations, as a minimum, employ appropriately tailored security controls from the low baseline of security controls defined in NIST Special Publication 800-53 and ensure that the minimum assurance requirements associated with the low baseline are satisfied.
- For *moderate-impact* information systems, organizations, as a minimum, employ appropriately tailored security controls from the moderate baseline of security controls defined in NIST Special Publication 800-53 and ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.
- For *high-impact* information systems, organizations, as a minimum, employ appropriately tailored security controls from the high baseline of security controls defined in NIST Special Publication 800-53 and ensure that the minimum assurance requirements associated with the high baseline are satisfied.

### Tailoring the Baseline Security Controls to Support Operational Requirements

Once the overall impact level of the information system is determined, an initial set of security controls can be selected from the corresponding low, moderate, or high baselines listed in NIST Special Publication 800-53. Organizations have the flexibility to tailor the security control baselines in accordance with the terms and conditions set forth in Special Publication 800-53. Tailoring activities include:

- The application of appropriate *scoping guidance* to the initial baseline;
- The specification of *compensating security controls*, if needed; and
- The specification of *organization-defined parameters* in the security controls, where allowed.

To achieve a cost-effective, risk-based approach to providing appropriate information security organization-wide, security control baseline tailoring activities should be coordinated with and approved by senior-level officials within the organization (e.g., chief information officers, senior agency information security officers, authorizing officials, or authorizing officials' designated representatives). Tailoring guidance includes the application of scoping guidance and compensating controls, as well as the assignment of specific values to security control parameters in accordance with organizational security requirements.

#### *Scoping Guidance*

Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines. There are several areas described in greater detail in NIST Special Publication 800-53 that can potentially impact how the baseline security controls are applied by the organization. These considerations include:

- Operational/environmental-related considerations;
- Technology-related considerations;
- Scalability-related considerations;
- Physical Infrastructure-related considerations;
- Security objective-related considerations;
- Public access-related considerations;

- Policy/regulatory-related considerations; and
- Common security control-related considerations.

After the scoping guidance is applied in every applicable area, documented accordingly, and appropriate rationale provided for the scoping decisions, the remaining set of "fine-tuned" security controls in the baseline should more closely reflect the foundational, or starting point for the final determination of the security needs of the organization with regard to protecting the enterprise mission within the particular operational environment.

*Compensating Security Controls*

With the diverse nature of today's information systems, organizations may find it necessary, on occasion, to specify and employ compensating security controls. A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provides equivalent or comparable protection for an information system. A compensating control for an information system may be employed by an organization only under the following conditions:

- The organization selects the compensating control from NIST Special Publication 800-53, or if an appropriate compensating control is not available in the security control catalog, the organization adopts a suitable compensating control;
- The organization provides a complete and convincing rationale for how the compensating control provides an equivalent security capability or level of protection for the information system and why the related baseline security control could not be employed; and
- The organization assesses and formally accepts the risk associated with employing the compensating control in the information system.

The use of compensating security controls should be documented in the security plan for the information system and approved by the authorizing official. More than one compensating control may be required to provide the equivalent or comparable protection for a particular security control in NIST Special Publication 800-53. For example, an organization with significant staff limitations may have difficulty in meeting the separation of duty security control but may employ compensating controls by strengthening the audit and accountability controls and personnel security controls within the information system. Organizations should make every attempt to select compensating controls from the security control catalog in NIST Special Publication 800-53. Organization-defined compensating controls should be used only as a last resort when the security control catalog does not contain suitable compensating controls.

*Organization-Defined Security Control Parameters*

Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives. After the application of the scoping guidance and the selection of compensating security controls, organizations should review the list of security controls for assignment and selection operations and determine appropriate organization-defined values for the identified parameters. Where specified, minimum and maximum values for organization-defined parameters should be adhered to unless more restrictive values are prescribed by applicable laws, directives, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk. Organization-defined security control parameters should be documented in the security plan for the information system.

## Supplementing the Tailored Baseline

The tailored security control baseline should be viewed as the foundation or starting point in the selection of appropriate security controls for an information system. The tailored baseline represents, for a particular class of information system (derived from the FIPS 199 security categorization and modified appropriately for local conditions), the starting point for determining the needed level of security *due diligence* to be demonstrated by an organization toward the protection of its operations and assets. However, the final determination of the security controls necessary to provide an appropriate level of security for an information system is a function of the organization's assessment of risk and what is required to sufficiently mitigate the risks to organizational operations, organizational assets, or individuals. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, directives, policies, standards, or regulations.

The risk assessment at this stage in the security control selection process provides important inputs to determine the sufficiency of the security controls in the tailored baseline—that is, the security controls needed to protect the organization's operations (including mission, function, and reputation), the organization's assets, and individuals. Organizations are encouraged to make maximum use of the security control catalog in NIST Special Publication 800-53 to facilitate the process of enhancing security controls or adding controls to the tailored baseline. To assist in this process, the security control catalog contains numerous controls and control enhancements that are found only in higher-impact baselines or are not included in any of the baselines. The resulting set of agreed-upon security controls along with the supporting rationale for control selection decisions are documented in the security plan for the information system. Figure 2 summarizes the security control selection process, including the tailoring of the initial security control baseline and supplementation of the baseline based on the organization's assessment of risk.

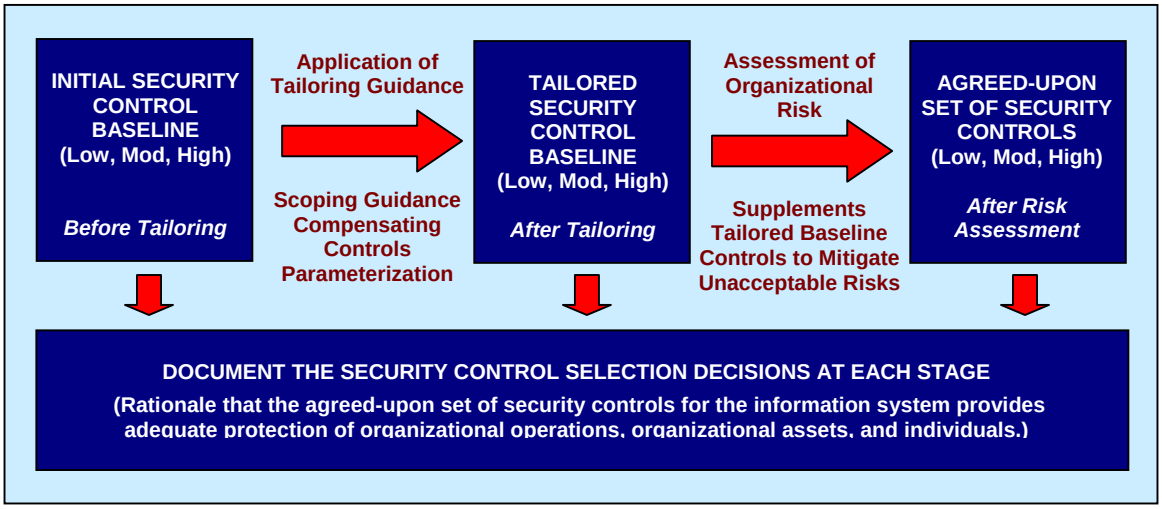


**FIGURE 2: SECURITY CONTROL SELECTION PROCESS**

## Implementing Security Controls and Determining Control Effectiveness

After an appropriate set of security controls is agreed upon by the organization, the controls are implemented within the information system. Configuration settings on all information technology products providing security capability to the information system are established and enforced, enterprise-wide. NIST Special Publication 800-70 describes the security configuration

checklist program and provides important linkages to the National Vulnerability Database and critical patching and update information for information technology products. Automated security support tools are also emerging to assist organizations in more effectively establishing linkages from the minimum security requirements in FIPS 200 and the specific security controls in NIST Special Publication 800-53 to the specific configuration settings in the information technology products providing the related security capabilities. These linkages are important in developing traceability from top-level information security policies and procedures to the actual security implementation within the hardware, software, and firmware components that make up the information systems supporting the enterprise.

Assessing security control effectiveness is a critical step in determining the remaining vulnerabilities in an information system—an assessment that is vital to an authorizing official in making a consistent, credible, risk-based decision on whether to place the information system into operation or continue its operation. NIST Special Publication 800-53A provides detailed assessment methods and procedures to organizations conducting assessments. The assessment methods and procedures provide a general framework for determining the effectiveness of individual security controls employed within the information system. Security assessments attempt to provide specific and credible evidence that the security controls are implemented correctly, operating as intended, and producing the desired effect with regard to meeting the enterprise's information security policy. As always, the assessment methods and procedures may require some specialization due to platform dependencies associated with certain technical security controls.

A complete assessment of the security controls in the information system will uncover any deficiencies in implemented controls or controls that may be missing altogether. Less than effective security controls result in residual vulnerabilities and risks that need to be addressed by the organization. The plan of action and milestones document associated with the information system addresses the noted deficiencies and provides a realistic roadmap on how those deficiencies are to be addressed by the information system owner. Specific actions taken by system owners to correct deficiencies take into account the importance of the information system in supporting enterprise missions as well as available resources. Collaboration with senior leaders ensures that the application of corporate-wide resources is applied in a balanced manner toward correcting deficiencies in the information system.

Once the information system is accredited (i.e., authorized for operation), it moves into a continuous monitoring phase, which requires tracking the security state of the system on an ongoing basis. Continuous monitoring is much more important today than in the past because of the dynamic nature of information systems, characterized by constantly changing hardware, software, and firmware components, new threats and vulnerabilities, and changing operational environments. The static certification and accreditation (C&A) processes that served organizations so well in the past are giving way to more dynamic processes that increasingly rely on the ongoing monitoring of security controls and making the near real-time adjustments to the security capabilities of the information system necessary to ensure continued protection of enterprise missions. NIST Special Publication 800-37 provides guidance on certifying and accrediting enterprise information systems.

## *PUTTING IT ALL TOGETHER*

All enterprise information systems, including operational systems, systems under development, and systems undergoing some form of modification or upgrade, are in some phase of what is commonly referred to as the system development life cycle.[19] There are many activities occurring during the life cycle of an information system dealing with the issues of cost, schedule, and performance. In addition to the functional requirements levied on an information system, security requirements must also be considered. When fully implemented, the information system must be able to meet its functional requirements and do so in a manner that is secure enough to protect the enterprise mission and business case. Organizations should have an enterprise-wide information security program and that program should be effectively integrated into the system development life cycle. The NIST Risk Management Framework described in this paper can be integrated into any phase of the system development life cycle. So, whether the enterprise maintains a host of legacy information systems or is bringing in state-of-the practice information technology, it is always the right time to consider information security issues.

And finally, it is of paramount importance that responsible officials within the enterprise understand the risks and other factors that could adversely affect organizational operations, organizational assets, or individuals. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated mission(s) or business case with an appropriate level of security—security commensurate with risk, including the magnitude of harm to individuals, the organization, or its assets resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

The NIST Risk Management Framework and the associated security standards and guidance provide a flexible and extensible approach toward bringing the appropriate level of protection to enterprise information systems based upon the unique mission requirements or business case of the enterprise. Whether protecting extremely critical or sensitive federal information systems or used voluntarily by private sector organizations to protect their corporate information technology assets, the Risk Management Framework can provide the right security solution for your enterprise. In the end, there is only one thing you need to remember—if your enterprise depends completely on your information technology infrastructure to accomplish your corporate mission and to fuel your enterprise operations, you must be prepared to *protect the technology*.

[19] There are typically five phases in the system development life cycle of an information system: (i) system initiation; (ii) system development and acquisition; (iii) system implementation; (iv) system operations and maintenance; and (v) system disposal. NIST Special Publication 800-64 provides guidance on the security considerations in the information system development life cycle.

## APPENDIX A

## Definitions of Potential Impact for Confidentiality, Integrity, and Availability

| FIPS 199 POTENTIAL IMPACT | | | |
|---|---|---|---|
| **Security Objective** | **LOW** | **MODERATE** | **HIGH** |
| **Confidentiality**<br>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.<br>[44 U.S.C., SEC. 3542] | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity**<br>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.<br>[44 U.S.C., SEC. 3542] | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability**<br>Ensuring timely and reliable access to and use of information.<br>[44 U.S.C., SEC. 3542] | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

## APPENDIX B

## Minimum Security Requirements for Information and Information Systems

**Access Control:** Organizations limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

**Awareness and Training:** Organizations: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

**Audit and Accountability:** Organizations: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

**Certification, Accreditation, and Security Assessments:** Organizations: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

**Configuration Management:** Organizations: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

**Contingency Planning:** Organizations establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

**Identification and Authentication:** Organizations identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

**Incident Response:** Organizations: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

**Maintenance:** Organizations: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

**Media Protection:** Organizations: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

**Physical and Environmental Protection:** Organizations: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

**Planning:** Organizations develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

**Personnel Security:** Organizations: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

**Risk Assessment:** Organizations periodically assess the risk to organizational operations (including mission, functions, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

**System and Services Acquisition:** Organizations: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

**System and Communications Protection:** Organizations: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

**System and Information Integrity:** Organizations: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

## APPENDIX C

## The Golden Rules for Effective Information Security

- Develop an enterprise-wide information security strategy and game plan;
- Get corporate “buy in” for the enterprise information security program—effective programs start at the top;
- Build information security into the infrastructure of the enterprise;
- Establish level of “due diligence” for information security;
- Focus initially on mission/business case impacts—bring in threat information only when specific and credible;
- Create a balanced information security program with management, operational, and technical security controls;
- Employ a solid foundation of security controls first, then build on that foundation guided by an assessment of risk;
- Avoid complicated and expensive risk assessments that rely on flawed assumptions or unverifiable data;
- Harden the target; place multiple barriers between the adversary and enterprise information systems;
- Be a good consumer—beware of vendors trying to sell “single point solutions” for enterprise security problems;
- Don’t be overwhelmed with the enormity or complexity of the information security problem—take one step at a time and build on small successes;
- Don’t tolerate indifference to enterprise information security problems; and
- Manage enterprise risk; don’t try to avoid it—use your information systems wisely.

## APPENDIX D

## References

**STANDARDS**


1. National Institute of Standards and Technology Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
2. National Institute of Standards and Technology Federal Information Processing Standards 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.


**GUIDELINES**


3. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
4. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.
5. National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.
6. National Institute of Standards and Technology Special Publication 800-53, Revision 1, *Minimum Security Controls for Federal Information Systems*, December 2006.
7. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006.
8. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
9. National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.
10. National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.


**WEB SITES**


11. NIST Computer Security Division: http://csrc.nist.gov
12. FISMA Implementation Project: http://csrc.nist.gov/sec-cert
13. NIST Security Configuration Checklist Program: http://checklists.nist.gov
14. National Vulnerability Database: http://nvd.nist.gov
15. NIST Cryptographic Module Validation Program: http://csrc.nist.gov/cryptval