RISK MANAGEMENT FRAMEWORK: HELPING ORGANIZATIONS IMPLEMENT EFFECTIVE INFORMATION SECURITY PROGRAMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The management of risks to information technology (IT) systems is a fundamental component of every organization's information security program. An effective risk management process enables an organization to protect its information assets and supports its ability to carry out its mission successfully. The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) has developed a Risk Management Framework that integrates the essential steps of the risk management process to support organizational managers in making informed decisions regarding the security of their information systems.

NIST's Risk Management Framework provides a structured process and information to help organizations identify the risks to their information systems, assess the risks, and take steps to reduce risks to an acceptable level. The Federal Information Security Management Act (FISMA) of 2002, Title III of the E-Government Act (Public Law 107-347), requires federal agencies to protect the information and information technology systems that support their operations and assets. NIST develops information security standards and guidelines to help federal agencies plan, implement, and manage comprehensive, risk-based, and balanced information security programs.

The Risk-Based Approach

The risk-based approach to the management of information systems is most effective when integrated into the system development life cycle (SDLC). The SDLC is a multistep process that starts with the initiation, analysis, design, development/acquisition, and implementation of an information system, and continues through the operation/maintenance and disposal of the system. NIST Special Publication (SP) 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, provides basic information on how to integrate information system security functionality and assurance into appropriate phases of the SDLC to support managing of risk throughout the life cycle of an information system.

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems,* discusses the development of security plans that provide an overview of the security requirements of the system and that describe the controls needed to meet those requirements. The security plan for a system also describes the responsibilities of all individuals who access the system and documents a structured process for planning for adequate, cost-effective security protection for a system.

Federal agencies implementing risk-based planning and management also must consider effectiveness, efficiency, and other requirements incorporated in current laws, directives, Executive Orders, policies, standards, or regulations. One consideration for federal agencies is the Federal Enterprise Architecture (FEA), which was established by the Office of Management and Budget (OMB) and the federal government's Chief Information Officer (CIO) Council to improve the performance of IT resources and agency investment strategies. The FEA is a business-based framework that helps agencies analyze and identify duplicative investments, gaps, and opportunities for collaboration among agencies. Information about the FEA is available from the OMB Web page http://www.whitehouse.gov/omb/e-gov/fea/.

The Risk Management Framework

Risk management is the process that information system managers apply to balance the operational and economic costs of protective measures for their information and information systems with the gains in capabilities and improved support of organizational mission that result from the use of efficient protection procedures. As part of the risk management process, organizations select and apply security controls for their information and information systems. The security controls are assessed and monitored to assure continued efficiency and effectiveness.

NIST's Risk Management Framework (RMF) points to specific publications and supplemental information to assist agencies in achieving adequate security for their IT systems. The RMF guides agencies through a series of steps, taking into account the risks such as the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. Easy access to the NIST standards and guidelines that pertain to the risk management process and general information about the Risk Management Framework is available from the NIST Web page http://csrc.nist.gov/groups/SMA/fisma/framework.html.

Risk Management Activities

The following activities compose the Risk Management Framework. These activities, which are fundamental to the management of organizational risk, can be applied to both new and legacy information systems within the context of the SDLC and the FEA:

· **Categorize** the information system and the information being processed, stored, and transmitted by the system, based on the potential impact to the organization should events occur to put the system and its information at risk. The organization assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability for the information and information systems that are needed by the organization to accomplish its mission, protect its assets and individuals**,** fulfill its legal responsibilities, and maintain its day-to-day functions.

Security categorization standards for information and information systems provide a common framework and understanding for documenting the potential impact to

organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) to information or the information system. Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, helps federal agencies determine the security category of their information systems. The categorization process also promotes effective management of information systems and consistent reporting by agencies to OMB and Congress.

NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, (Volumes 1 and 2), assists federal organizations in applying appropriate levels of information security based on the levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system.

· **Select** an appropriate set of security controls for the information system after determining the security categorizations as specified in FIPS 199 and the minimum security requirements as defined in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.* FIPS 200 specifies minimum security requirements for federal information and information systems for seventeen security-related areas that represent a broad-based, balanced information security program. The seventeen security-related areas encompass the management, operational, and technical aspects of protecting federal information and information systems. Further, FIPS 200 specifies that organizations meet the minimum security requirements by selecting an appropriately tailored set of baseline security controls based on an assessment of risk and local conditions, including the organization's specific security requirements, threat information, cost-benefit analyses, or special circumstances.

To address minimum security requirements, the organization selects security controls from NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems.* This publication provides a catalog of controls that organizations may select to protect their information systems in accordance with their missions and business requirements. An initial baseline set of security controls is determined based on the impact analysis conducted under the provisions of FIPS 199 and FIPS 200. Organizations can tailor and supplement the selection of baseline security controls, based on their assessment of risks. Guidance on tailoring the baseline controls is provided in NIST SP 800-53.

· **Implement** the security controls in the information system. NIST SP 800-70, *Security Configuration Checklists Program for IT Products*, presents information about security configuration checklists and their benefits, and explains how to use the NIST Checklist Program to find and retrieve checklists. Checklists of security settings are useful tools that have been developed to guide IT administrators and security personnel in selecting effective security settings that will reduce the risks and protect systems from attacks. A checklist, sometimes called a security configuration guide, lockdown guide, hardening guide, security technical implementation guide, or benchmark, is a series of instructions for configuring an IT product to an operational environment. Checklists can

be effective in reducing vulnerabilities to systems, especially for small organizations with limited resources. IT vendors often create checklists for their own products, but other organizations such as consortia, academic groups, and government agencies have also developed them. Information about the NIST Checklists Program is available from http://checklists.nist.gov/.

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, presents a broad overview of the elements of an information security program. The handbook summarizes NIST standards and guidelines, and provides information on topics such as requirements for security governance, planning issues, performance of systems, and risk management matters.

Many other NIST publications dealing with the implementation of security controls are available from the NIST Web page http://csrc.nist.gov/index.html.

· **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. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* includes useful information for this step of the Risk Management Framework.

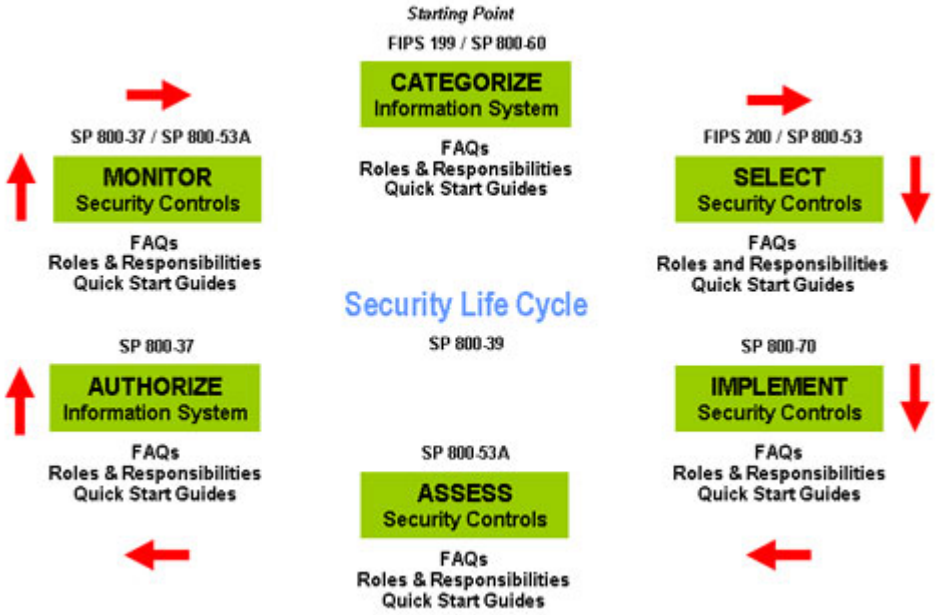
NIST SP 800-53A is a companion guide for NIST SP 800-53 and covers both the security control assessment and continuous monitoring steps in the Risk Management Framework. This guide helps organizations with the security assessment process, including how to build effective security assessment plans and how to manage assessment results. The procedures discussed give organizations flexibility in tailoring and supplementing the basic assessment processes to match the characteristics of the information system being assessed. While allowing for flexibility in the development of security assessment plans, NIST SP 800-53A also helps agencies achieve consistency of assessments through the application of a formal assessment framework and uniform assessment procedures.

· **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 determination that this risk is acceptable. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, discusses the steps leading to an official management decision by a senior agency official to authorize operation of an information system, accepting the risks to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Certification and accreditation of information systems are required activities for federal agencies.

· **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 changes, and reporting the security status of the system to

appropriate organization officials on a regular basis. Both NIST SP 800-53A and NIST SP 800-37 contain useful information for this step.

A chart of the six steps of the process is reproduced below. This chart is available from the NIST Web page http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html.



Users accessing the online version of this six-step chart can link to FIPS, SPs, Frequently Asked Questions (FAQs), Roles and Responsibilities, and Quick Start Guide documents for each step of the RMF. To access the respective documents for each step, users can place their cursor over the document and click the mouse button to link to that document. A menu appearing on the left side of the page, but not reproduced here, can also be used to access the FAQs, Roles and Responsibilities, and the Quick Start Guides for each step in the Risk Management Framework.

These steps provide a structured, yet flexible approach for managing the risks that result from the incorporation of information systems into the mission and business processes of the organization. The risk management concepts presented are broad in scope with the specific details of assessing risk and employing appropriate risk mitigation strategies provided by the supporting NIST security standards and guidelines. The FAQs, Roles and Responsibilities, and Quick Start Guides build on the standards and guidance, consolidate information from various NIST publications, and provide examples of ways that organizations can implement the standards and guidelines.

Upcoming Revisions of NIST Publications

Revision 3 of NIST SP 800-53, *Security Controls for Federal Information Systems and Organizations,* was announced by NIST in early June. This revision will provide a unified information security framework for the federal government and its contractors with the inclusion of security controls for both national security and nonnational security systems. This integrated approach will incorporate the best practices in information security from the Department of Defense, the intelligence community, and nondefense agencies, and will contain a broad-based and comprehensive set of safeguards and countermeasures for information systems.

The revision of SP 800-53 will include management, operational, and technical controls to be implemented in federal information systems that process, store, and transmit both national security and nonnational security information. The revised security control catalog will also include safeguards and countermeasures that are needed by organizations to address advanced cyber threats to vulnerabilities in federal information systems. The focus is on the management of risks in information systems on an enterprise-wide and near real-time basis. Systems that are operating in dynamic environments can be adversely affected by threats to organizational operations and assets, individuals, other organizations, and the Nation.

For details about the revision of SP 800-53, see http://csrc.nist.gov/publications/drafts/800-53/800-53-rev3-FPD-clean.pdf.

Another important publication, NIST SP 800-39, *Managing Risk From Information Systems: An Organizational Perspective,* is also nearly completed. NIST SP 800-39 discusses risk management concepts and the Risk Management Framework, bringing together the supporting security standards and guidelines that are necessary for managing risk related to information systems. The guide presents a comprehensive approach to the analysis of how agency information systems are tied to the agency mission and to the management of enterprise risk. Information about this publication is available from the NIST Web page http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf.

For More Information

The Risk Management Framework, available on the NIST Web page http://csrc.nist.gov/groups/SMA/fisma/framework.html, explains the steps of the risk management process and provides links to NIST publications.

Additional information about NIST's security programs is available from the Computer Security Resource Center http://csrc.nist.gov/.

The NIST contact for more information about the Risk Management Framework:

FISMA project leader:
Dr. Ron Ross
301-975-5390
ron.ross@nist.gov

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.