ITL BULLETIN FOR MARCH 2010

REVISED GUIDE HELPS FEDERAL ORGANIZATIONS IMPROVE THEIR RISK MANAGEMENT PRACTICES AND INFORMATION SYSTEM SECURITY

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Federal organizations are challenged to protect their information and information systems from mounting security threats. Persistent, sophisticated attacks and potential vulnerabilities in increasingly complex systems can weaken agency operations and compromise the confidentiality, integrity, and availability of information. Under the Federal Information Security Management Act (FISMA) of 2002, Title III of the E-Government Act (Public Law 107-347), and executive directives, the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) develops standards and guidelines to help federal organizations apply effective security techniques to protect information, systems, and assets.

To achieve adequate security, federal managers must actively manage the risks to their core missions and business functions, and to the information and information systems supporting those missions and functions. In managing risks, organizations 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 missions resulting from the use of efficient protection procedures. NIST developed the Risk Management Framework (RMF) to guide agencies through a structured process to identify the risks to the information systems, assess the risks, and take steps to reduce risks to an acceptable level.

NIST recently issued Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Developed in partnership with the Joint Task Force Transformation Initiative, the publication represents a new effort to build a unified information security framework for the information systems of the federal government and its contractors. The Joint Task Force includes participants from the Department of Defense (DOD), the Intelligence Community, and civil agencies of the federal government.

NIST Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

NIST SP 800-37, Revision 1, supports federal managers in both defense and civil agencies in making informed decisions about the security of their information systems. This publication is the second in a series of publications that are being developed by a Working Group of the Joint Task Force Transformation Initiative.

In August 2009, NIST issued the Working Group's first publication as NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. This guide provides a comprehensive catalog of security controls that can be used to protect both national security and non-national security information systems. Agencies are required to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability; to specify minimum security requirements for their systems; and to select security controls to satisfy minimum security requirements, based on a risk-based process.

In NIST SP 800-37, Revision 1, the Joint Task Force incorporated the traditional processes that the federal government uses to certify and accredit federal information systems into the Risk Management Framework. Federal organizations are required to certify and accredit their information systems through a series of steps that lead to an official management decision by a senior agency official to authorize the operation of an information system that implements security controls, based on the acceptance of the risks to agency operations, agency assets, or individuals.

The common foundation for information security described in NIST SP 800-37, Revision 1, enables information systems to be effectively managed in an environment of complex risks, increased vulnerabilities, and changing organizational missions. As a result, all federal agencies will have more uniform and consistent ways to manage the risks to organizational operations, assets, and information. Further, the use of the Risk Management Framework will facilitate information sharing and reciprocity of security authorization results.

The revised guide explains the basic concepts to be applied to the management of security risks to information systems. The publication emphasizes planning and building information security capabilities into information systems throughout the system life cycle; implementing up-to-date management, operational, and technical security controls; and maintaining awareness of the security condition of information systems though improved monitoring.

The specific tasks that organizations should perform in applying the Risk Management Framework are detailed, including the security certification and accreditation (now termed assessment and authorization) steps. Extensive appendices provide additional information on the RMF, including a reference list of relevant laws, policies, directives, instructions, standards and guidelines. Other sections of the appendices provide a glossary of terms used in the guide, acronyms, descriptions of the roles and responsibilities of participants in the risk management process, and a chart summarizing the steps in the RMF process.

SP 800-37, Revision 1, is available from the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html.

Managing Security Risks to Information Systems

The risk-based approach to the management of information systems is most effective when integrated into the organization's strategic planning processes. Leaders, managers, and staff members at all levels of an organization should be involved in the risk management process, and the process should be a basic component of the organization's planning and operations. NIST SP 800-37, Revision 1, discusses a three-tiered approach to risk management that addresses risk-related concerns at:

• Tier 1, the **organization**-level perspective with the development of a comprehensive governance structure and organization-wide risk management strategy;

• Tier 2, the **mission and business process** perspective of risk; and

• Tier 3, the **information system** perspective of risk, which is guided by the risk decisions at Tiers 1 and 2.

Figure 1 illustrates the three-tiered risk-based approach.

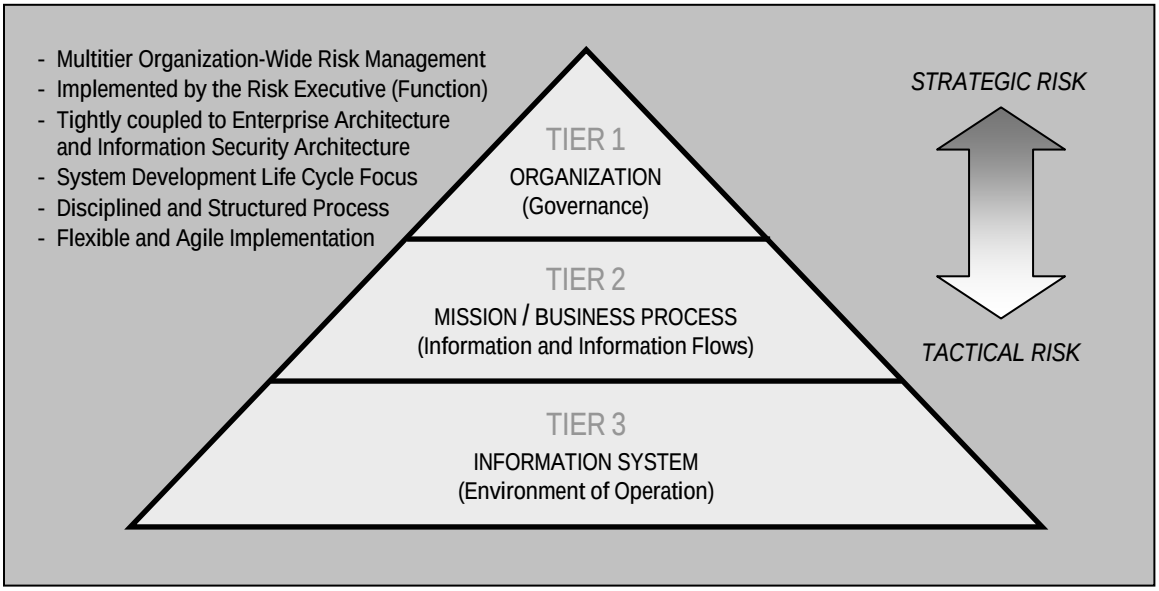

FIGURE 1

Information security requirements should be considered throughout the system development life cycle (SDLC), a multistep process that starts with the initiation, analysis, design, development/acquisition, and implementation of an information system, and that continues through the operation/maintenance and disposal of the system. The early integration of information security requirements into the system development life

cycle enables the organization to achieve cost-effective and efficient implementation of protective measures and more resilient systems.

The information security processes are not isolated from other management processes used by the organization to manage its information systems. Integrating security requirements into the organization's program, planning, and budgeting activities promotes the availability of needed resources and the completion of program and project milestones. Also, the integrated approach fosters closer cooperation among staff members responsible for the development and management of information systems and the information security professionals who advise senior managers on security controls. The security-related information generated during the SDLC can also be used for other security information requirements.

Organizations should establish practical and meaningful boundaries **for information systems**. When selecting security controls for a complex information system, organizations may want to consider decomposing a complex system into more manageable subsystems that can work together functionally and securely. Multiple subsystems with defined boundaries can result in a more effective application of security controls and in cost savings. The decomposition of the information system should be documented in the organization's security plan.

Information system boundaries are established when organizations categorize their systems, and they develop security plans. Boundaries that contain too many system components or architectural complexity make it difficult for organizations to carry out the risk management process. Boundaries that are too limited increase the number of systems that must be separately managed. This can inflate the total information security costs for the organization. The guide provides general guidelines to assist organizations in establishing appropriate system boundaries to achieve cost-effective solutions for managing information security-related risks.

Security controls for information systems should be allocated as system-specific, hybrid, or common controls. System-specific controls provide a security capability for a particular information system only; common controls provide a security capability for multiple information systems; and hybrid controls have both system-specific and common characteristics. These controls should be allocated to an information system consistent with the organization's enterprise architecture and information security architecture. The process should be an organization-wide activity. .

Common controls are more cost-effective, and they provide more consistent information security across the organization. The allocation of common controls can also simplify risk management activities. When security controls are allocated to an information system as system-specific controls, hybrid controls, or common controls, the organization assigns responsibility and accountability to specific organizational entities for the overall development, implementation, assessment, authorization, and monitoring of those controls. NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal*

Information Systems and Organizations, includes controls that are appropriate for the different types of allocations.

Risk Management Framework Tasks

Organizations should initiate their risk management tasks early in the system development life cycle to reinforce the security capabilities of the information system in a cost-effective manner. All risk management tasks other than continuous monitoring, should be completed before the system is placed into operation or after controls are added to an existing system. All security risks to information systems should be addressed on an ongoing basis through the execution of a continuous monitoring strategy. As part of the assessment and authorization process, the authorizing official must understand and accept the risks to the organization, to its assets, and to others, based on the implementation of a defined set of security controls and the security state of the information system.

The Risk Management Framework describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The six RMF steps are:

• Step 1. Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.

• Step 2. Select an initial set of baseline security controls for the information system based on the security categorization, tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

• **Step 3.** Implement the security controls and describe how the controls are employed within the information system and its environment of operation.

• **Step 4.** Assess the security controls using appropriate assessment 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.

• **Step 5.** Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

• **Step 6.** Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

The RMF applies primarily to Tier 3 in the risk management hierarchy. There is also some applicability at Tiers 1 and 2. NIST SP 800-37, Revision 1, provides a detailed

description for each specific task needed to carry out the six steps in the RMF. Each task description includes the following information:

- Individual or group with the primary responsibility for carrying out the task;
- Supporting roles of staff members who may be called upon to assist in completing the task;
- System development life cycle phase most closely associated with the task;
- Supplemental guidance to help explain how the task is executed; and
- Appropriate references for publications or Web sites with information related to the task.

A milestone checkpoint, which is provided for each step in the RMF, contains a series of questions to help the organization complete each step in the RMF before proceeding to the next step.

Organizations have flexibility in implementing the RMF tasks at appropriate phases of the system development life cycle. Organizations can apply RMF steps 1, 2, and 3 to legacy systems to confirm that the security categorization has been completed, that it is appropriate, and that the needed security controls have been selected and allocated for legacy systems. Security control weaknesses and deficiencies discovered in existing systems can be addressed in RMF Steps 3 through 6. When they have determined that there is a current security authorization in effect, organizations can move directly to the continuous monitoring step in the RMF. If a current security authorization is not in place, the organization continues with RMF Steps 4, 5, and 6.

The security categorization process influences the level of effort expended when implementing the RMF tasks. Information systems that support the most critical, sensitive operations and assets within the organization as indicated by the security categorization process, should receive the greatest level of attention and effort to strengthen information security and reduce risks. Most RMF tasks can be carried out by external providers with appropriate contractual agreements or other arrangements in place. See Appendix I of the guide for information on this issue.

A summary table of the RMF tasks is provided in Appendix E of the document.

For More Information

General information about the Risk Management Framework, and access to standards and guidelines that pertain to the RMF, are available from the NIST Web page http://csrc.nist.gov/groups/SMA/fisma/framework.html.

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

FISMA Implementation Project leader:
Dr. Ron Ross

301-975-5390
ron.ross@nist.gov

NIST publications that provide information and guidance on steps in the risk management process include:

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
NIST Special Publication (SP) 800-18, *Guide for Developing Security Plans for Federal Information Systems*
NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*
NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories,* (Volumes 1 and 2)
NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*
NIST SP 800-70, *Security Configuration Checklists Program for IT Products*
NIST SP 800-100, *Information Security Handbook: A Guide for Managers*

For information about these NIST standards and guidelines, as well as other security-related publications, see NIST's Web page http://csrc.nist.gov/publications/index.html.

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