ITL BULLETIN FOR AUGUST 2010

ASSESSING THE EFFECTIVENESS OF SECURITY CONTROLS IN FEDERAL INFORMATION SYSTEMS

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

Organizations throughout the federal government depend upon information systems to carry out their missions and to conduct business with the public. Disruptions to organizational operations, human and system errors, and hostile attacks on systems can seriously impair the ability of federal agencies to operate effectively.

Risks to the core missions and business operations of organizations change significantly as technology changes and as more people use information systems and networks to share information and engage in global commerce.

Under the Federal Information Security Management Act (FISMA) of 2002, Title III of the E-Government Act (Public Law 107-347), federal agencies must protect the information and information technology systems that support their operations and assets. FISMA emphasizes a risk-based policy for cost-effective security. The changing technology environment accentuates the importance of active, continuous management of risks.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) develops guides and recommendations to assist organizations in carrying out the critically important risk management process. NIST recently revised its guide to support organizations in assessing the effectiveness of the security controls that are implemented in federal information systems. The selection and assessment of appropriate security controls are important steps in the comprehensive process of managing risks and maintaining effective security of those information systems.

NIST Special Publication (SP) 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans,* June 2010

NIST SP 800-53A, Rev. 1, was developed by the Joint Task Force Transformation Initiative Interagency Working Group, which includes representatives from the Civil, Defense, and Intelligence Communities of the federal government. The revised guide updates an earlier guide for assessing security controls, and describes the fundamental concepts associated with security control assessments. Issues covered include the integration of assessments into the system development life cycle; the importance of an organization-wide strategy for conducting security control assessments; the development of assurance cases to help organizational officials determine the effectiveness of security

controls and the overall security of the information system; and the format and content of assessment procedures.

The revised guide discusses the process for assessing the security controls in organizational information systems and their environments of operation. The activities to be carried out by organizations and assessors include preparing for security control assessments; developing security assessment plans; conducting security control assessments; and analyzing assessment results. The guide provides a chart that summarizes the security control assessment process, including the activities carried out during pre-assessment, assessment, and post-assessment stages.

The appendices to the guide provide detailed assessment-related information including references, definitions and terms used in the guide, and an explanation of acronyms. A detailed description of assessment methods is provided, as well as penetration testing guidelines, and a master catalog of assessment procedures that can be used to develop plans for assessing security controls. The master catalog of assessment procedures (Appendix F) provides procedures for assessing the security controls defined in Appendix F of NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, which was published in August 2009. Also included in the appendices are an outline for the content of security assessment reports, and the definition, format, and use of assessment cases.

NIST SP 800-53A, Rev.1, updates assessment procedures for security controls and control enhancements, providing organizations with greater flexibility in selecting appropriate assessment methods for conducting various types of assessments, such as assessments supporting information system development, initial and ongoing security authorizations, and continuous monitoring. Organizations can adjust the assessment procedures to more closely match the characteristics of their information systems and environments of operation, and to meet the risk management needs of the organization.

NIST SP 800-53A, Rev. 1, is available from the NIST Web page: http://csrc.nist.gov/publications/PubsSPs.html.

Selection and Implementation of Security Controls

Federal 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, using a risk-based process.

The selection of security controls is an important component of providing needed security, and safeguarding the operations and assets of the organization. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity (including non-repudiation and authenticity), and availability of the system and its information. Once

implemented within an information system, security controls should be assessed to provide the information necessary to determine their ongoing effectiveness. This assessment examines 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.

Assessments of security controls enable organization officials to verify that the implementers and operators of information systems are meeting their stated security goals and objectives. The revised guide helps organizations conduct the assessment process as part of the overall risk management process. The process of assessing the effectiveness of security controls also provides useful input to the organization's risk management processes.

The assessing of security controls in federal information systems is an important step in managing organizational risk from the use of information systems. Federal organizations are required to assess the effectiveness of security controls implemented in information systems to provide the necessary information to support the official management decision by a senior agency official to authorize the operation of an information system based on the acceptance of the risks to agency operations, agency assets, or individuals.

Security Control Assessment and the Risk Management Framework

The security control assessment process discussed in NIST SP 800-53A, Rev.1, supports the larger strategic initiative of enterprise-wide, near real-time risk management, that is, managing risks from information systems in dynamic environments of operation.

NIST developed the Risk Management Framework (RMF) to guide agencies through a structured process to identify the mission and business risks associated with the operation and use of information systems, assess the risks, and take steps to reduce risks to an acceptable level.

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 missions 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.

Risk management tasks are initiated early in the system development life cycle to reinforce the security capabilities of the information system in a cost-effective manner. Most risk management tasks should be completed before the system is placed into operation or after controls are added to an existing system. All information system security-related risks should be addressed on an ongoing basis through the implementation of a continuous monitoring strategy. The assessment and authorization processes help the organization's authorizing official 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 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. 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.

NIST SP 800-53A, Rev. 1, is a companion guideline to NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*. NIST SP 800-53 covers Step 2 in the RMF, determining what security controls are needed and selecting appropriate security controls for managing the risks to the organization. NIST SP 800-53A covers Step 4 of the RMF, security control assessment, and Step 6 of the RMF, continuous monitoring; it provides guidance on the security assessment process, including how to build effective security assessment plans and how to analyze and manage assessment results.

The RMF points to specific publications and supplemental information to assist agencies in establishing adequate security for their information systems. Each publication provides

guidance for implementing specific steps in the Risk Management Framework. See the More Information section below for access to the NIST standards and guidelines that support the RMF.

NIST and the Joint Task Force Transformation Initiative

In a new effort to build a unified information security framework for the information systems of the federal government and its contractors, NIST has been working in partnership with the Joint Task Force Transformation Initiative. The Joint Task Force includes participants from the Department of Defense (DOD), the Intelligence Community, and civil agencies of the federal government.

A common foundation for information security will provide all sectors of the federal government and their contractors with more uniform and consistent ways to manage the risks that result from the operation and use of information systems. A common foundation for information security will also provide a strong basis for reciprocal acceptance of security assessment results and facilitate information sharing. NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Other publications developed in cooperation with the Joint Task Force include NIST SP 800-53. Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, and NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* See the Related Publications section below.

Ongoing and Future Activities

Working with the Joint Task Force, NIST plans to update a set of Assessment Cases, examples of assessor actions derived from assessment procedures (described in Appendix H of NIST SP 800-53A, Rev. 1) to provide organizations and assessors with additional details for conducting specific assessments of federal information systems.

NIST has been developing the Security Content Automation Protocol (SCAP). SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information. SCAP is designed to organize, express, and measure security-related information in standardized ways.

SCAP is expected to evolve and expand in support of the growing needs to define and measure the effectiveness of security controls, assess and monitor ongoing aspects of information security, and successfully manage systems in accordance with risk management procedures. This anticipated development should help organizations manage

the security of their systems, to conduct continuous monitoring of the security configuration of systems, and to comply with security requirements.

Related Publications

NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. In particular, the assessment procedures and the guidelines provided for developing security assessment plans for organizational information systems contained in NIST SP 800-53A, Rev. 1, directly support the security control assessment and continuous monitoring activities that are integral to the risk management process described in NIST SP 800-37, Rev. 1. This includes providing near real-time information to organization officials regarding the ongoing security state of their information systems.

NIST SP 800-53, Rev. 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.

More Information

NIST publications that provide information and guidance on planning, implementing, and assessing information system security 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, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*;

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*;

NIST SP 800-60, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide, Volume 2: Appendices*;

NIST SP 800-64, Rev. 2, *Security Considerations in the System Development Life Cycle*;

NIST SP 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0*; and

NIST SP 126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0.*

For information about these NIST standards and guidelines, as well as other security-related publications, see the NIST 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.

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 is the FISMA Implementation 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.