SECURITY ASSESSMENTS: TOOLS FOR MEASURING THE EFFECTIVENESS OF SECURITY CONTROLS

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

The selection and implementation of security controls are critical decisions for protecting the security of an organization's information and information systems. Security controls are the management, operational, and technical safeguards or countermeasures that protect the confidentiality, integrity, and availability of an information system and its information.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently supplemented its guidance to federal agencies about selecting, implementing, and assessing security controls for their information systems. The updated advice helps organizations apply measurement tools to assess the proper implementation, operation, and effectiveness of their security controls, and to correct any deficiencies in information security in a cost-effective manner. Security assessments make it possible for implementers and operators of information systems to verify that their systems are meeting their stated security goals and objectives. The assessments also provide organizations with valuable information about the quality of their risk management processes and about the strengths and weaknesses of security controls in their information systems.

Assessments also support the organization's security accreditation processes and its security planning processes in general. The ability to measure and assess is vital to the dependable operation of federal information systems, which support critical agency missions and applications in a global environment where there are constant hostile threats.

Security Assessments and the Federal Information Security Management Act of 2002 (FISMA)

The Federal Information Security Management Act of 2002 establishes a governmentwide policy for the implementation and assessment of security controls. FISMA requires that federal agencies develop, document, and implement programs to protect their information and information systems. This policy applies to the systems that support the operations and assets of the agency, and includes those systems provided or managed by another agency, contractor, or other source. FISMA calls for agencies to apply a risk-based policy to achieve cost-effective results for the security of their information and information systems.

Standards and guidelines developed by NIST help agencies carry out effective information security programs based on assessments of risk. The first important step for

agencies is to categorize their federal information systems and select security controls as specified by Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. Under FIPS 199 and 200, federal agencies must categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability, and then select an appropriate set of security controls from NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, to satisfy their minimum security requirements.

Through their risk assessment processes, agencies can validate the selection of security controls and determine if any additional controls are needed to protect the agency's operations, taking into consideration the agency's mission, functions, image, reputation, its assets, and potential impacts of security breaches on individuals, other organizations, and the country in general. The security controls that are selected establish a level of "security due diligence" for the federal agency and its contractors.

In addition to the security requirements established by FISMA, agencies may be responsible for specific security requirements that may apply to different business areas within agencies, as specified by other laws, Executive Orders, directives, policies, or regulations. Some examples are the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, and Office of Management and Budget (OMB) Circular A-127 on Financial Management Systems. These measures may have additional complementary or specific security requirements. Agencies must ensure that all appropriate security requirements are addressed in agency acquisitions of information systems and information system services, and that all required security controls are implemented in agency information systems

NIST SP 800-53A*, Guide for Assessing the Security Controls in Federal Information Systems*

Issued in July 2008, NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, was written by Ron Ross, Arnold Johnson, Stu Katzke, and Patricia Toth of NIST, by Gary Stoneburner of the Johns Hopkins University Applied Physics Laboratory, and by George Rogers of BAE Systems. NIST SP 800-53A is a companion guideline to NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. Both of these publications emphasize the use of security control assessments within an effective risk management framework.

NIST SP 800-53A introduces the fundamental concepts that support the assessment of security controls, including the integration of assessments into the system development life cycle and the need for an organizational strategy for conducting security controls assessments. Other topics addressed include building an assurance case for effectiveness of security controls.

The process for assessing the security controls is discussed in detail in the new guide. Steps in the process include the preparation for security control assessments; the development of security assessment plans; the conduct of security control assessments; the analysis, documentation, and reporting of assessment results; the post-assessment report analysis, and follow-on activities.

Both NIST SP 800-53 and NIST SP 800-53A are available at NIST's Web page: http://csrc.nist.gov/publications/PubsSPs.html.

The appendices to NIST SP 800-53A provide an extensive compilation of resources to help organizations in assessing security controls, and include the following useful materials:

- a list of general references, the definitions and terms associated with the assessment process;
- an explanation of the acronyms used in the guide;
- a description of assessment methods;
- assessment expectations for low-impact, moderate-impact, and high-impact information systems;
- a master catalog of assessment procedures that can be used to develop plans for assessing security controls;
- assessment tools and techniques to identify information system weaknesses;
- an assessment procedure work sheet for identifying and selecting the base set of procedures for assessing the information system security controls;
- a sample format for security assessment reports; and
- worked examples of assessment procedures providing the definition, format, and use of assessment cases.

These worked examples, which are presented in Appendix J of the guide, are the result of the collaborative efforts of experienced assessors from several federal organizations. They participated in the Assessment Case Development Project that was organized by NIST. These assessors provided a set of assessment cases for each assessment procedure in the catalog of procedures that are listed in the publication. The assessment cases promote ongoing community-wide review of and comment on the assessment cases and support the continuous improvement of the assessment process to achieve more consistent, cost-effective security assessments of federal information systems.

Implementing the Risk Management Framework

The Risk Management Framework, developed by NIST, delineates a multistep process for categorizing systems and for selecting, implementing, assessing, and managing controls throughout the life cycle of an information system. NIST SP 800-53 covers the steps in the Risk Management Framework for determining needed security controls, selecting an initial set of baseline controls, and supplementing the security controls as needed based on the organization's assessment of risk. The steps include:

- categorizing information and information systems in accordance with FIPS 199;

- selecting an initial set of baseline security controls based on FIPS 199 impact levels;
- tailoring the baseline security controls;
- supplementing the security controls, as necessary, based on an organizational assessment of risk.
- implementing controls; and
- assessing controls and monitoring security.

NIST SP 800-53 provides tailoring guidance to enable agencies to adjust security controls to fit their mission requirements and operational environments. Tailoring involves scoping the assessment procedures to match the characteristics of the information system under assessment. The tailoring process provides organizations with the flexibility needed to avoid assessment approaches that are unnecessarily extensive or more rigorous than necessary. Under the tailoring guidance, agencies can eliminate unnecessary controls, incorporate compensating controls when needed, and specify agency-specific conditions. This approach gives agencies flexibility to respond to known threats and to take action on agency-identified risks. NIST SP 800-53A also supports these tailoring concepts.

NIST SP 800-53A covers both the security control assessment and continuous monitoring steps in the Risk Management Framework and provides guidance on the security assessment process, including how to build effective security assessment plans and how to manage assessment results.

When using the Risk Management Framework to supplement their security controls, organizations can add assessment procedures or assessment details to meet their risk management needs. These decisions can help an organization maximize its flexibility in developing security assessment plans and apply the results of risk assessments effectively.

While flexibility continues to be an important factor in developing security assessment plans, consistency of assessments is also an important consideration. NIST SP 800-53A provides an assessment framework and initial starting point for assessment procedures that are essential for achieving the needed consistency.

The findings produced by the assessors of security controls are used primarily in determining the overall effectiveness of the security controls in an information system and in providing credible and meaningful inputs to the organization’s security accreditation process. The accreditation process covers the official management decision of a senior agency official to authorize the operation of an information system and to accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. The information and supporting evidence needed for security accreditations are often developed during the security certification process, which is a comprehensive assessment of the management, operational, and technical security controls to determine the extent to which the controls

are implemented correctly, operating as intended, and meeting the security requirements for the system.

A well-executed assessment of controls contributes to the accreditation and certification processes by helping to determine the validity of the security controls contained in the agency's security plan and in facilitating a cost-effective approach to correcting any deficiencies in systems.

A new publication in development at NIST, draft SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, will provide guidance for implementing the risk management framework, and advise agencies on developing a structured, yet flexible approach for managing the risks that result from the incorporation of information systems into the mission and business processes of organizations.

NIST Recommendations for Assessing Security Controls

NIST recommends that organizations carry out the following activities in assessing their security controls:

Prepare for security control assessments by assuring the cooperation and collaboration of all parties having a vested interest in the security status of the organization's information systems. Issues to be addressed include costs, schedules, and the time frame for the performance of the assessments. Organizational activities that should be in place include policies covering security control assessments; steps in the Risk Management Framework; assignment of responsibility for common controls; agreement on scope of assessments; establishment of time frame for assessments; identification of an assessment team; and establishment of communications with all appropriate parties.

Organizations should use NIST SP 800-53A in conjunction with an approved security plan to develop assessment procedures that will be the starting point for input to the development of a security assessment plan. The procedures should be designed to produce the information necessary for determining the effectiveness of the security controls employed in the information system.

Develop security assessment plans that will provide the objectives for the security control assessment and produce a detailed roadmap of how to conduct such an assessment. The output and end result of the security control assessment is the security assessment report, which documents the assurance case for the information system and is one of three key documents in the development of documentation for security accreditation. The security assessment plan should take into consideration the extent of the assessment, the controls to be assessed, the procedures to be used, and approvals of agency authorities.

Carry out the assessment plans in accordance with the agreed-upon milestones and schedule. Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling the information necessary to make the determination associated with each assessment objective. Assessors examine each

determination statement contained within an assessment procedure and produce findings of "satisfied," indicating that the control produces an acceptable result, or "other than satisfied," indicating that the control may be deficient or that insufficient information was available to make a determination.

The assessor's findings should be unbiased and factual in reporting what was found concerning each security control assessed. For each finding of "other than satisfied," assessors should indicate the parts of the security control that are affected by the finding, how the control differs from the planned or expected state, and the potential for compromises to confidentiality, integrity, and availability of information and systems.

Security control assessment results should be documented at the level of detail appropriate for the assessment in accordance with the reporting format prescribed by organizational policy, NIST guidelines, and OMB policy. The reporting format should also be appropriate for the type of security control assessment conducted, such as self-assessments, independent verification and validation, independent assessments by assessors or assessment teams, or independent audits of security controls by auditors or inspectors general.

Analyze assessment reports and conduct follow-on activities. The results of the security control assessment influence the organization's security plan and its plan of action and milestones. Appropriate officials such as the system's authorizing official, chief information officer, senior agency information security officer, and system owners, should be involved in decisions to mitigate risks and to correct weaknesses and deficiencies to the organization's information and information systems. It may be necessary to involve the agency's senior leadership to ensure that resources are effectively allocated in accordance with organizational priorities, providing resources first to the information systems that support the most critical and sensitive missions for the organization or correcting the deficiencies that pose the greatest degree of risk. Security plans, security assessment reports, and plans of action and milestones should be updated to reflect the results of the security control assessment.

More Information

See http://csrc.nist.gov/sec-cert/ca-compliance.html for additional information on FISMA, and NIST's activities to support federal agencies in the implementation of strong information security programs.

Assessment cases, based on the assessment procedures in NIST SP 800-53A and developed by an interagency task force, are available to all public and private sector organizations. See http://csrc.nist.gov/groups/SMA/fisma/assessment.html.

NIST's Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP) also support and complement the process for achieving consistent, cost-effective security control assessments. ISAP/SCAP improve the automated application, verification, and reporting of commercial information technology

product-specific security configuration settings, thereby helping to reduce vulnerabilities when products are not configured properly. More about ISAP/SCAP is available at http://nvd.nist.gov/scap.cfm.

Information about the NIST Risk Management Framework can be found at http://csrc.nist.gov/groups/SMA/fisma/framework.html.

Draft NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, is available at http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf.

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.