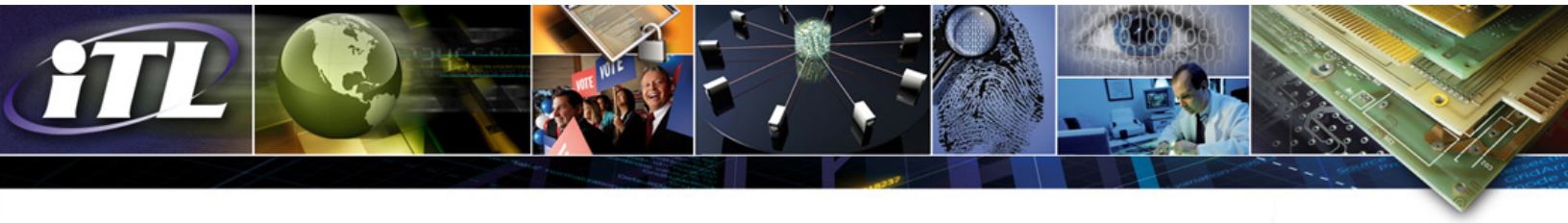


ITL BULLETIN FOR JANUARY 2015

RELEASE OF NIST SPECIAL PUBLICATION 800-53A, REVISION 4, *ASSESSING SECURITY AND PRIVACY CONTROLS IN FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS*

Kelley Dempsey, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

NIST has published an updated version of Special Publication (SP) 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. SP 800-53A provides guidelines for building effective security assessment plans and procedures for assessing the effectiveness of security controls employed in federal information systems and organizations. This updated version (Revision 4) contains significant changes to the 2010 version, in both content and format. The changes are driven by four fundamental needs of federal agencies:

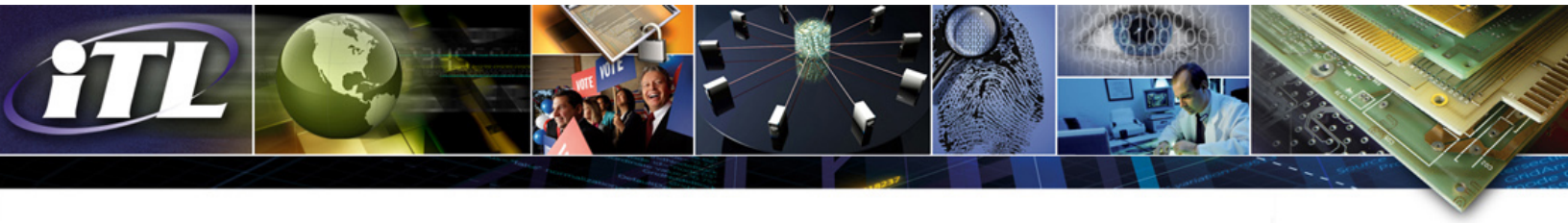
- The need for new or updated assessment procedures for security controls and privacy controls, as defined in NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
- The need for a more granular breakdown of assessment objectives to support continuous monitoring and ongoing authorization programs;
- The need for an enhanced structured format and syntax for assessment procedures that can support the use of automated tools for assessment and monitoring activities; and
- The need to support assessments of security capabilities and root cause analysis of failure modes for individual security controls or groups of controls.

By addressing these needs, the revised document helps organizations to:

- Define specific security control components that require greater scrutiny, monitoring, or assessment than others;
- Tailor the scope and level of effort required for assessments;
- Assign assessment and monitoring frequencies on a targeted basis; and
- Take advantage of new opportunities to assess security capabilities including analysis of control dependencies.

There have also been significant improvements in security assessment procedures based on feedback from federal agencies, reflecting lessons learned while conducting the Risk Management Framework (RMF) process. This feedback led NIST to clarify terminology, expand the number of potential per-control assessment methods/objects, and provide a simpler decomposition of assessment objects.

The publication reflects ongoing integration of privacy elements and information security. Privacy terminology has been integrated into SP 800-53A in a manner that complements and supports the



privacy controls defined in SP 800-53, Appendix J. The privacy assessment procedures that will eventually populate Appendix J in SP 800-53A are currently being developed by a joint interagency working group, established by the Best Practices Subcommittee of the CIO Council Privacy Committee. NIST anticipates a draft of privacy assessment procedures in early 2015.

SP 800-53A Rev. 4 satisfies the requirements of the Federal Information Security Management Act (FISMA) and meets or exceeds the information security and privacy requirements established for executive agencies by the Office of Management and Budget (OMB) in Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*, and Appendix III, *Security of Federal Automated Information Resources.*

SP 800-53A Rev. 4 was developed by the *Joint Task Force Transformation Initiative* Working Group with representatives from the Civilian, Defense, and Intelligence Communities to produce a *unified information security framework* for the federal government. It is notable that a one-time change has been made in the revision number of SP 800-53A (skipping revision numbers 2 and 3) so this document can be aligned with the current publication version of SP 800-53, Revision 4.

Assessment Procedures

An important component of the NIST Risk Management Framework (RMF) is Step 4: Assess. During this step, the user assesses the planned or implemented security controls, using appropriate 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. SP 800-53A, Rev. 4 provides detailed assessment procedures to accomplish that step. An assessment procedure consists of a set of assessment *objectives*, each with an associated set of potential assessment *methods* and assessment *objects*. An assessment objective includes a set of *determination statements* related to the particular security or privacy control under assessment. The determination statements are linked to the content of the security or privacy control to ensure traceability of assessment results back to the fundamental control requirements. The application of an assessment procedure to a security or privacy control produces assessment *findings*. These findings reflect, or are subsequently used, to help determine the overall effectiveness of the security or privacy control.

Assessment objects identify the specific items being assessed and include *specifications*, *mechanisms*, *activities*, and *individuals*. Specifications are the document-based artifacts (e.g., policies, procedures, plans, system security and privacy requirements, functional specifications, architectural designs) associated with an information system. Mechanisms are the specific hardware, software, or firmware safeguards and countermeasures employed within an information system. Activities are the specific protection-related actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic, exercising a contingency plan).

Assessment methods define the nature of the assessor actions and include *examine*, *interview*, and *test*. The *examine* method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). The purpose of the examine method is to facilitate assessor understanding, achieve clarification, or obtain evidence. The *interview* method is the process of holding discussions with individuals or groups of individuals within an organization to once again, facilitate assessor understanding, achieve clarification, or obtain evidence.

The *test* method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior. In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure. Appendix D of the publication provides a complete description of assessment methods and assessment objects.

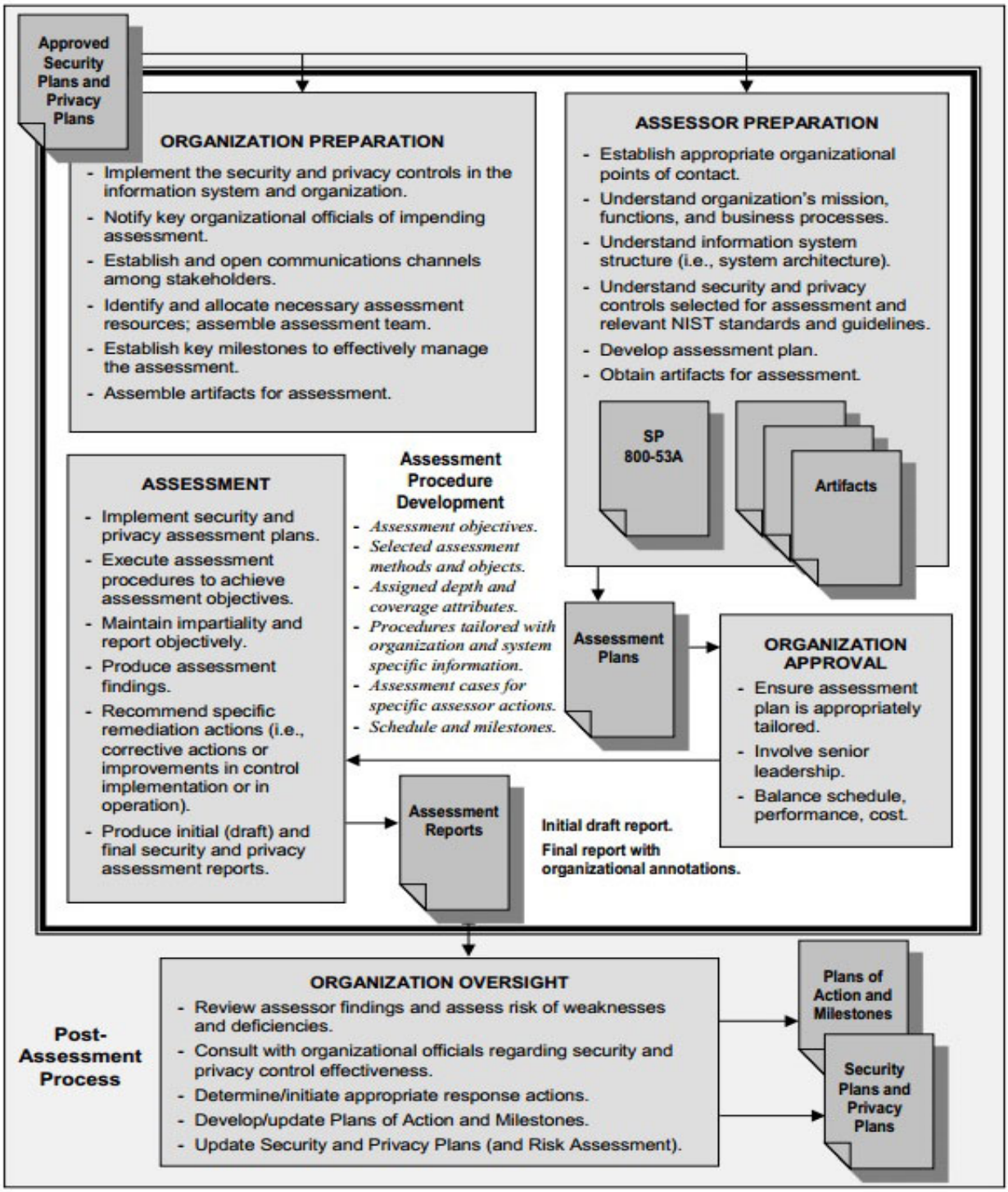
Capability-Based Assessments

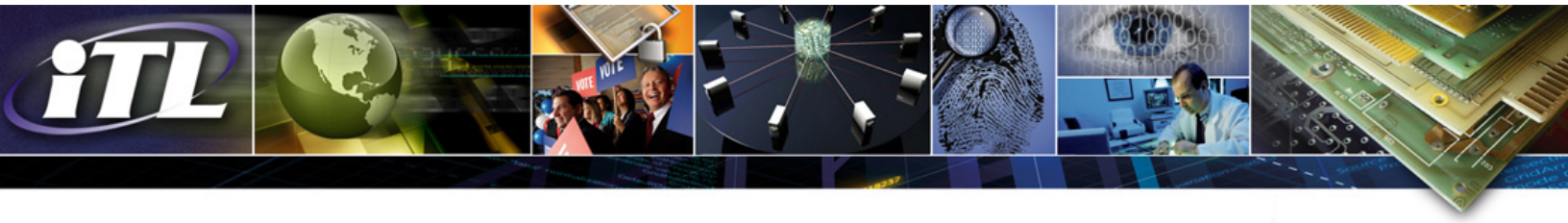
In accordance with SP 800-53, organizations may define a set of security capabilities or privacy capabilities as a precursor to the security control or privacy control selection process. The concept of *capability* recognizes that the protection of information being processed, stored, or transmitted is seldom derived from a single security safeguard or countermeasure. In most cases, such protection results from the selection and implementation of a set of mutually reinforcing security controls and privacy controls.

The use of root cause analysis is necessary to determine if the failure of a particular security or privacy capability can be traced to the failure of one or more individual security or privacy controls. The structure of the 800-53A, Rev. 4 assessment procedures, with more granular decomposition and a more structured format and syntax of assessment objectives, supports such root cause analysis. The new structure brings numerous benefits, not only for those using security capabilities but also for other IT service management capabilities. It provides flexible support for Information Security Continuous Monitoring (ISCM) and Ongoing Authorization (OA), and facilitates the use of automated tools for assessment and monitoring, to help the organization:

- Attain better risk management through identification of parts of security controls that require increased scrutiny, monitoring, or assessment rather than focusing only at the control level;
- More effectively tailor the scope and level of effort required for assessments to achieve risk management objectives in a cost-effective manner;
- Assign assessment and monitoring frequencies on a more targeted basis; and
- Gain cost benefits or risk reduction advantage from new opportunities to conduct assessments based on system and platform-specific and/or organization-specific dependencies.

Figure 1, **Security and Privacy Control Assessment Process Overview**, summarizes the security control and privacy control assessment process including activities carried out during pre-assessment, assessment, and post-assessment.





Assessment Reports

The primary purpose of the *security assessment report* and *privacy assessment report* is to convey the results of the security and privacy control assessment. The report provides a disciplined and structured approach for documenting the assessor's findings and recommendations. The report is included in the security authorization package along with the security plan (including an updated risk assessment) and the plan of action and milestones to provide authorizing officials with the information necessary to make risk-based decisions on whether to place an information system into operation or continue its operation. Organizations may choose to include similar privacy-related artifacts in the authorization package. Appendix G of the document provides information for reporting the results from security control assessments and privacy control assessments. As the assessment and authorization process becomes more dynamic, relying to a greater degree on continuous monitoring aspects, the ability to frequently update the security assessment report and privacy assessment report becomes a critical aspect.

Ongoing Assessment and Automation

Ongoing security assessment is the continuous evaluation of the effectiveness of security control implementation. It is an essential subset of *Information Security Continuous Monitoring (ISCM)* activities. Ongoing assessment encompasses ISCM Steps 3 and 4 and is initiated as part of ISCM Step 3, *Implement*, when the collection of security-related information begins in accordance with the organization-defined frequencies. Ongoing assessment continues as the security-related information generated as part of ISCM Step 3 is correlated, analyzed, and reported to senior leaders as part of ISCM Step 4. As noted in Special Publication 800-137, security-related information is generated, correlated, analyzed, and reported using automated tools to the extent that it is possible and practical to do so. When it is not possible and practical to use automated tools, security-related information is generated, correlated, analyzed, and reported using manual or procedural methods. In this way, senior leaders are provided with the security-related information necessary to make credible, risk-based decisions regarding information security risk to the mission/business.

Automating assessments is a fundamental element in supporting organizations' risk management. Evolving threats create a challenge for organizations that design, implement, and operate complex information systems. The ability to assess all implemented security controls as frequently as needed, using manual or procedural methods, has become impractical for most organizations due to the size, complexity, and scope of their information technology infrastructures. To assist with automation, NIST provides an (XML) version of the assessment objectives as well as a tab-delimited version and an associated XSL file, available at the National Vulnerability Database website. A database version of SP 800-53A will be added at the same location later in fiscal year 2015.

NIST initiated the Security Content Automation Protocol (SCAP) project to support consistent, cost-effective security control assessments. The primary purpose of SCAP is to standardize the format and nomenclature used for communicating information about configurations and security flaws. This standardization enables automated system configuration assessment, vulnerability assessment, and patch checking. It aids in report aggregation and interoperability among SCAP-enabled security products. As a result, SCAP enables organizations to identify and reduce vulnerabilities associated with products that are not patched or insecurely configured. SCAP also includes the Open Checklist

Interactive Language (OCIL) specification that provides the capability to express the determination statements in the assessment procedures in Appendix F in a framework that will establish interoperability with the SCAP-enabled tools.

Conclusion

SP 800-53A provides the changes to the current security assessment procedures that will result in significant improvements in the efficiency and cost-effectiveness of control assessments for federal agencies. Efficient and cost-effective assessments are essential in order to provide senior leaders with the necessary information to understand the security and privacy posture of their organizations and to be able to make credible, timely, and risk-based information security and privacy decisions.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov