NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. Such information security standards and guidelines shall not apply to national security systems without the express approval of the appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, OMB Director, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-53A Revision 5
Natl. Inst. Stand. Technol. Spec. Publ. 800-53A, Rev. 5, **733 pages** (January 2022)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the designated public comment periods and provide feedback to NIST. Many NIST publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Submit comments on this publication to: sec-cert@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA) [FOIA96].

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and privacy and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication provides a methodology and set of procedures for conducting assessments of security and privacy controls employed within systems and organizations within an effective risk management framework. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in NIST Special Publication 800-53, Revision 5. The procedures are customizable and can be easily tailored to provide organizations with the needed flexibility to conduct security and privacy control assessments that support organizational risk management processes and are aligned with the stated risk tolerance of the organization. Information on building effective security and privacy assessment plans is also provided with guidance on analyzing assessment results.

Keywords

Assessment; assessment plan; assurance; control assessment; FISMA; Privacy Act; privacy controls; Open Security Controls Assessment Language; OSCAL; privacy requirements; Risk Management Framework; security controls; security requirements.

Acknowledgments

This publication was developed by the *Joint Task Force* Interagency Working Group. The group includes representatives from the civil, defense, and intelligence communities. The National Institute of Standards and Technology wishes to acknowledge and thank the senior leaders from the Department of Commerce, Department of Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to this publication.

Department of Defense

HON. John Sherman
Chief Information Officer

Dr. Kelly Fletcher
Principal Deputy Chief Information Officer

David McKeown
Deputy CIO for Cybersecurity and DoD CISO

Mark Hakun
Principal Deputy CIO for Cybersecurity

Kevin Dulany
Director, Cybersecurity Policy and Partnerships

Office of the Director of National Intelligence

Michael E. Waschull
Acting Chief Information Officer

Michael E. Waschull
Deputy Chief Information Officer

C. Matthew Conner
Cybersecurity Group and IC CISO

Cheri Benedict
Director, Security Coordination Center

National Institute of Standards and Technology

James St. Pierre
Acting Director, Information Technology Laboratory (ITL)

Kevin Stine
Cybersecurity Advisor, ITL

Matthew Scholl
Chief, Computer Security Division

Kevin Stine
Chief, Applied Cybersecurity Division

Victoria Yan Pillitteri
Risk Management Framework Project Leader

Committee on National Security Systems

Mark G. Hakun
Chair

Dominic A. Cussatt
Co-Chair

Kevin Dulany
Tri-Chair—Defense Community

Chris Johnson
Tri-Chair—Intelligence Community

Vicki Michetti
Tri-Chair—Civil Agencies

Joint Task Force (JTF) Working Group

Victoria Yan Pillitteri
NIST, JTF Leader

McKay Tolboe
DoD

Andy Rovnak
Intelligence Community

Angela Smith
NIST

Katie Isaacson
The MITRE Corporation

Eduardo Takamura
NIST

Dave Myers
Veterans Affairs

Peter Duspiva
Intelligence Community

Jon Boyens
NIST

Randy Gabel
The MITRE Corporation

Kelley Dempsey
NIST

Vicki Michetti
Veterans Affairs

Chris Johnson
Intelligence Community

Ned Goren
NIST

David Black
The MITRE Corporation

Ron Ross
NIST

Naomi Lefkovitz
NIST

Jessica Dickson
NIST

Kaitlin Boeckl
NIST

Pam Miller
The MITRE Corporation

In addition to the above acknowledgments, a special note of thanks goes to Jeff Brewer, Jim Foti, Cristina Ritfeld, Isabel Van Wyk, and the NIST web team for their outstanding administrative support, Chris Enloe for his technical review and insight, and to David Waltermire and Wendell Piez for their contribution to the development of the SP 800-53A assessment tables (both electronic sources, and derivative publications) using Open Security Controls Assessment Language (OSCAL). The authors also wish to recognize the professional staff from the NIST Computer Security Division and Applied Cybersecurity Division, and the representatives from the Federal Chief Information Officer (CIO) Council, Federal Chief Information Security Officer (CISO) Council, and Federal Privacy Council for their ongoing contributions in helping to improve the content of the publication. Finally, the authors gratefully acknowledge the contributions from individuals and organizations in the public and private sectors, both nationally and internationally, whose insightful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

HISTORICAL CONTRIBUTIONS TO NIST SPECIAL PUBLICATION 800-53A

The authors wanted to acknowledge the many individuals who contributed to previous versions of Special Publication 800-53A since its inception in 2005. They include Marshall Abrams, Dennis Bailey, Matt Barrett, Nadya Bartol, Frank Belz, Paul Bicknell, Deb Bodeau, Brett Burley, Bill Burr, Dawn Cappelli, Corinne Castanza, Matt Coose, George Dinolt, Donna Dodson, Randy Easter, Kurt Eleam, Jennifer Fabius, Daniel Faigin, Denise Farrar, Harriett Goldman, Peter Gouldmann, Richard Graubart, Jennifer Guild, Sarbari Gupta, Peggy Himes, Bennett Hodge, Cynthia Irvina, Arnold Johnson, Roger Johnson, Lisa Kaiser, Stu Katzke, Sharon Keller, Cass Kelly, Steve LaFountain, Steve Lipner, Bill MacGregor, Tom Macklin, Tom Madden, Erika McCallister, Tim McChesney, Michael McEvilley, John Mildner, Sandra Miravalle, Joji Montelibano, Doug Montgomery, George Moore, Harvey Newstrom, Robert Niemeyer, LouAnna Notargiacomo, Dorian Pappas, Tim Polk, Esten Porter, Karen Quigg, Steve Quinn, Ed Roback, George Rogers, Scott Rose, Mike Rubin, Karen Scarfone, Roger Schell, Matt Scholl, Murugiah Souppaya, Kevin Stine, Gary Stoneburner, Keith Stouffer, Marianne Swanson, Pat Toth, Glenda Turner, Joe Weiss, Richard Wilsher, Mark Wilson, John Woodward, and Carol Woody.

Document Conventions

For the purposes of this document, the term "security *and* privacy" is universally used since the guidance is applicable to both security and privacy control assessments. For certain systems, however, the guidance may only be relevant for ***security or privacy***. Organizations make their own determinations on when to manage security and privacy control assessments together or separately.

SP 800-53A provides guidance on assessing controls in information security program plans, privacy program plans, system security plans, and privacy plans. Where the guidance refers to all plans listed above, the term "security and privacy plans" is used. If the guidance is specific to a single type of plan (e.g., system security plan), the specific type of plan is specified.

Supplemental Content

The assessment procedures in Chapter 4 are published in multiple data formats, including comma-separated values (CSV), plain text, and Open Security Controls Assessment (OSCAL). The available data formats are accessible from the NIST SP 800-53A Revision 5, publication details page at https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final. The OSCAL Content Git Repository is available at https://github.com/usnistgov/oscal-content.

The CSV, plain text, and OSCAL formats represent derivative formats of the (normative) assessment procedures in this publication. If there are any discrepancies between the content in derivative formats and this publication, please contact sec-cert@nist.gov.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

DEVELOPING COMMON INFORMATION SECURITY AND PRIVACY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by [FISMA], NIST consults with other federal agencies and offices as well as private sector entities to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST publications complement the standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST collaborates with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DoD), and the Committee on National Security Systems (CNSS) to establish and maintain a unified framework and common foundation for information security across the Federal Government. A common foundation and framework for information security provides the intelligence, defense, and civilian sectors of the Federal Government and their contractors more uniform and consistent ways to manage risks to organizational operations and assets, individuals, other organizations, and the Nation that result from the operation and use of systems. A common foundation and framework also provides a strong basis for the reciprocal acceptance of security authorization decisions and facilitate information sharing. NIST also works with public and private sector entities to establish and maintain specific mappings and relationships between the security standards and guidelines developed by NIST, the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC).

ASSESSMENT PROCEDURE FORMATTING

The new format for assessment procedures introduced in Special Publication (SP) 800-53A Revision 4, is further improved in this revision (SP 800-53A Revision 5). The format continues to reflect the decomposition of assessment objectives into more *granular* determination statements wherever possible, thus providing the capability to identify and assess specific parts of security and privacy controls. Updates to SP 800-53A Revision 5:

- Identify determination statements for organization-defined parameters (ODPs) first and separately from the determination statements for each control item;
- Improve the readability of the assessment procedures;
- Provide a structured schema for automated tools when assessment information is imported into such tools;
- Provide greater flexibility in conducting assessments by giving organizations the capability to target certain aspects of controls (highlighting the particular weaknesses and/or deficiencies in controls),
- Improve the efficiency of security and privacy control assessments;
- Support continuous monitoring and ongoing authorization programs by providing a greater number of component parts of security and privacy controls that can be assessed at organization-defined frequencies and degrees of rigor.

The ability to apply assessment and monitoring resources in a targeted and precise manner and simultaneously maximize the use of automation technologies can result in more timely and cost-effective assessment processes for organizations.

Note: NIST [SP 800-53] will be updated accordingly to ensure that the numbering scheme for all security and privacy controls is consistent with the new format introduced in this publication.

Executive Summary

Security and privacy control assessments are not about checklists, simple pass/fail results, or generating paperwork to pass inspections or audits. Rather, control assessments are the principal vehicle used to verify that selected security and privacy controls are implemented and meeting stated goals and objectives. Special Publication (SP) 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations*, facilitates security control assessments and privacy control assessments conducted within an effective risk management framework. A major design objective for SP 800-53A is to provide an assessment framework and initial starting point for assessment procedures that are flexible enough to meet the needs of different organizations while providing consistency in conducting control assessments. Control assessment results provide organizational officials with:

- Evidence of the effectiveness of implemented controls,
- An indication of the quality of the risk management processes, and
- Information about the security and privacy strengths and weaknesses of systems that are supporting organizational missions and business functions.

The findings identified by assessors are used to determine the overall effectiveness of security and privacy controls associated with systems and their environments of operation and to provide credible and meaningful inputs to the organization's risk management process. A well-executed assessment helps determine the validity of the controls contained in the organization's security and privacy plans and subsequently employed in organizational systems and environments of operation. Control assessments facilitate a cost-effective approach to managing risk by identifying weaknesses or deficiencies in systems, thus enabling the organization to determine appropriate risk responses in a disciplined manner that is consistent with organizational mission and business needs.

SP 800-53A is a companion guideline to [SP 800-53] *Security and Privacy Controls for Systems and Organizations*. Each publication provides guidance for implementing specific steps in the Risk Management Framework (RMF).[1] SP 800-53 and [SP 800-53B] address the Select step of the RMF and provide guidance on security and privacy control selection (i.e., determining the controls needed to manage risks to organizational operations and assets, individuals, other organizations, and the Nation). SP 800-53A addresses the Assess and Monitor steps of the RMF and provides guidance on the security and privacy control assessment processes. SP 800-53A also includes guidance on how to build effective assessment plans and how to analyze and manage assessment results.

SP 800-53A provides a process that allows organizations to tailor the assessment procedures outlined in the guidance. Tailoring involves customizing the assessment procedures to match the characteristics of the system and its environment of operation more closely. The tailoring process described in this guidance gives organizations the flexibility needed to avoid assessment approaches that are unnecessarily complex or costly while simultaneously meeting the assessment requirements and risk management principles established in the RMF. Tailoring decisions are left to the discretion of the organization to maximize flexibility in developing assessment plans – applying the results of risk assessments to determine the extent, rigor, and level of intensity of the assessments needed to provide sufficient assurance about the security and privacy posture of the system.

[1] [SP 800-37], *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* provides guidance on applying the RMF to systems and organizations.