NIST SP 800-53 and SP 80053A, Revision 5: What's New and Looking Ahead

NIST Risk Management Framework (RMF) Team

sec-cert@nist.gov

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Agenda

NIST Special Publication (SP) 800-53 Series at a Glance

SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*

- Summary of changes in Revision 5

SP 800-53B, *Control Baselines for Information Systems and Organizations*

SP 800-53A Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*

- Summary of changes in Revision 5

Future Revisions of SP 800-53

SP 800-53 at a Glance

CATALOG OF
SECURITY & PRIVACY CONTROLS

USED AS PART OF A
RISK MANAGEMENT
PROCESS

APPLICABLE TO
ALL TYPES
OF SYSTEMS & ORGANIZATIONS

6 REVISIONS SINCE
2005

INTERNATIONAL
USE AND IMPACT

AVAILABLE IN
MULTIPLE DATA FORMATS

ASSESSMENT PROCEDURES
SP 800-53A

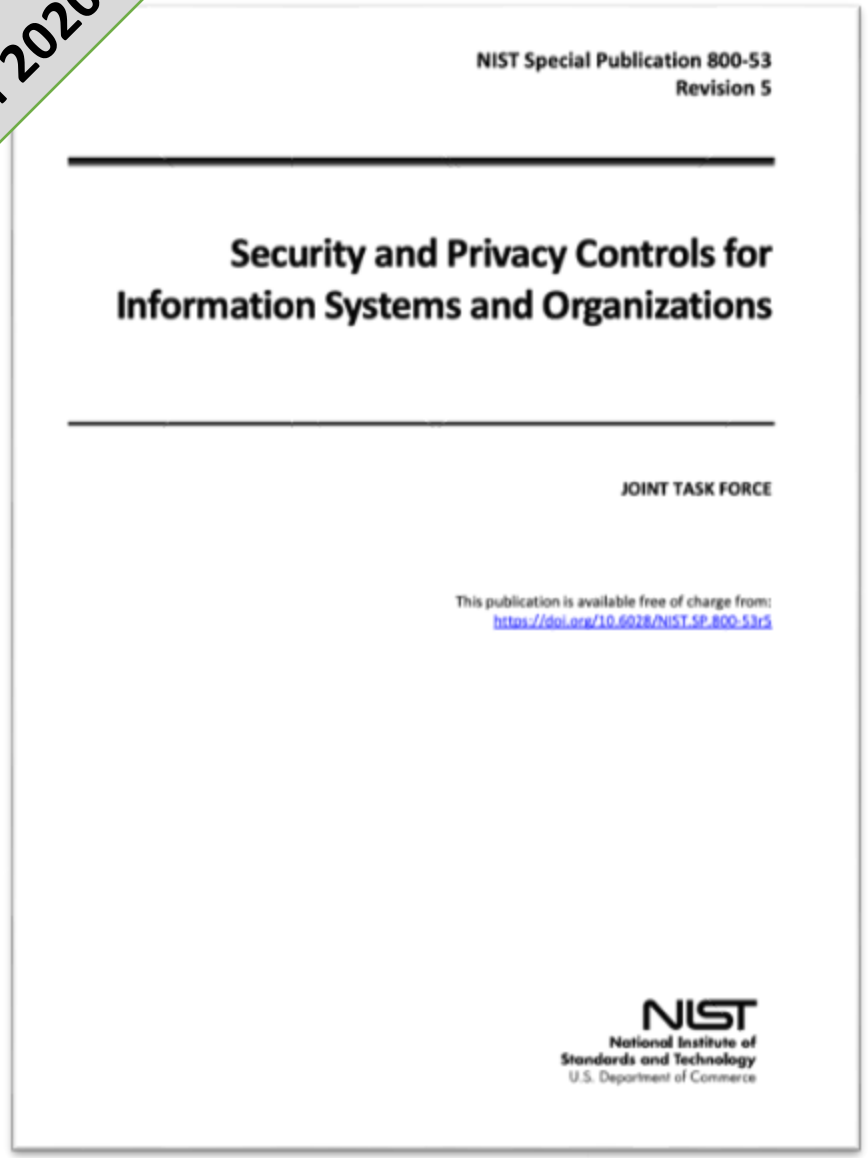
CONTROL BASELINES
SP 800-53B

SUBMIT YOUR
COMMENTS 24/7

NIST SP 800-53 Rev 5

Security and Privacy Controls for Information Systems and Organizations

Published September 2020


NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

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

- Catalog of **security and privacy controls** to protect organizational operations and assets from risk
- Controls are **outcomes** that can be selected and implemented as part of an organization-wide process to manage risk
- Controls are **applicable to any type of system**, including IoT, industrial control systems, communications & enterprise IT
- SP 800-53 is part of a **suite of guidelines** to manage cybersecurity risk

Summary of Changes: SP 800-53 Rev 5

- Separation of **controls** from the **process**
- Controls are more **outcome-focused**

- Privacy and Supply Chain Risk Management controls added to the Program Management (PM) Family & incorporated into applicable controls throughout
- New Control Families: Personally Identifiable Information Processing and Transparency (PT) and Supply Chain Risk Management (SR)

- Control baselines, overlay & tailoring guidance **moved to SP 800-53B**
- Mappings and control keywords posted as **supplemental materials**

SP 800-53 Rev 5 Supplemental Materials

- Controls in spreadsheet format
- SP 800-53 control mappings to **Cybersecurity Framework, Privacy Framework, and ISO 27001**
- Collaboration template for security & privacy programs
- Analysis of **changes** between Rev 4 and Rev 5, Rev 4 and 800-53B

GitHub

- Controls in **Open Security Control Assessment Language (OSCAL)**
  - Available in XML, JSON and YAML

Analysis of Changes Between Rev 4 & 5

Rev 5 Update	NIST SP 800-53 Rev 5 Controls	NIST SP 800-53B Control Baselines				More than editorial or administrative change? (Y/N)	Changed Elements	Change Details
AT-3	Role-Based Training	X	X	X	X	Y	Changes title Changes control text Adds parameter Changes discussion Adds to Privacy Control Baseline (SP 800-53B)	privacy incidents into training Adds parameter requiring role-based security and privacy training for personnel with specific roles and responsibilities Adds new control text with a parameter to update role-based training at a specific frequency Discussion adds examples of personnel to be trained as well as events that may precipitate an update to role-based training Incorporates role-based training elements of withdrawn App J control AR-5
AT-3(1)	Role-Based Training | Environmental Controls					N	Changes discussion	Does not change intent
AT-3(2)	Role-Based Training | Physical Security Controls					N	Changes discussion	Does not change intent
AT-3(3)	Role-Based Training | Practical Exercises					Y	Adds control text Changes discussion	Adds privacy to control text, to imply training includes privacy, as well as security Discussion expanded to include examples of practical exercises for privacy
AT-3(4)	*Role-Based Training | Suspicious Communications and Anomalous System Behavior*					Y	Withdrawn	Moved to AT-2(4)
AT-3(5)	Role-Based Training | Processing Personally Identifiable Information	X				Y	New control enhancement Adds to Privacy Control Baseline (SP 800-53B)	Provide specific personnel or roles with initial and at a specific frequency training in the employment and operation of PII processing and transparency controls Incorporates training elements of withdrawn App J control UL-2
AT-4	Training Records	X	X	X	X	Y	Changes title Changes control text Changes discussion Adds to Privacy Control Baseline (SP 800-53B)	Title changed from 'Security Training Records' Adds privacy to control text, to imply training includes privacy, as well as security Discussion includes reference to NARA
AT-5	*Contacts With Security Groups and Associations*					N	N	Previously withdrawn in Rev4; Incorporated into PM-15

Thank you to MITRE Corporation & Director of National Intelligence for sharing a spreadsheet analysis of control changes

NIST SP 800-53B

Control Baselines for Information Systems & Organizations

Published October 2020

3 security control baselines

- Low, Moderate, High Impact Levels
- ***Minor updates between SP 800-53 Revision 4 and 800-53B***

Guidance on Tailoring Control Baselines and Developing Control Overlays

- Control candidates for downgrading
- Selecting compensating controls and supplementing baselines
- Reference to Security Control Overlay Repository online resource (https://csrc.nist.gov/projects/risk-management/scor)

New in SP 800-53B

Privacy Control Baseline

- Initial privacy control baseline to address **privacy requirements** and manage privacy risks from the **processing of PII based on privacy program responsibilities under OMB Circular A-130**
- **Independent of the security control baselines**

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE-IN-DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x

SP 800-53A Rev 5

Assessing Security and Privacy Controls in Information Systems and Organizations

- Provides a methodology and set of customizable procedures for conducting assessments of security and privacy controls within an effective risk management framework.
- Includes information on building effective security and privacy assessment plans with a focus on analyzing assessment results.

SP 800-53 control assessments:

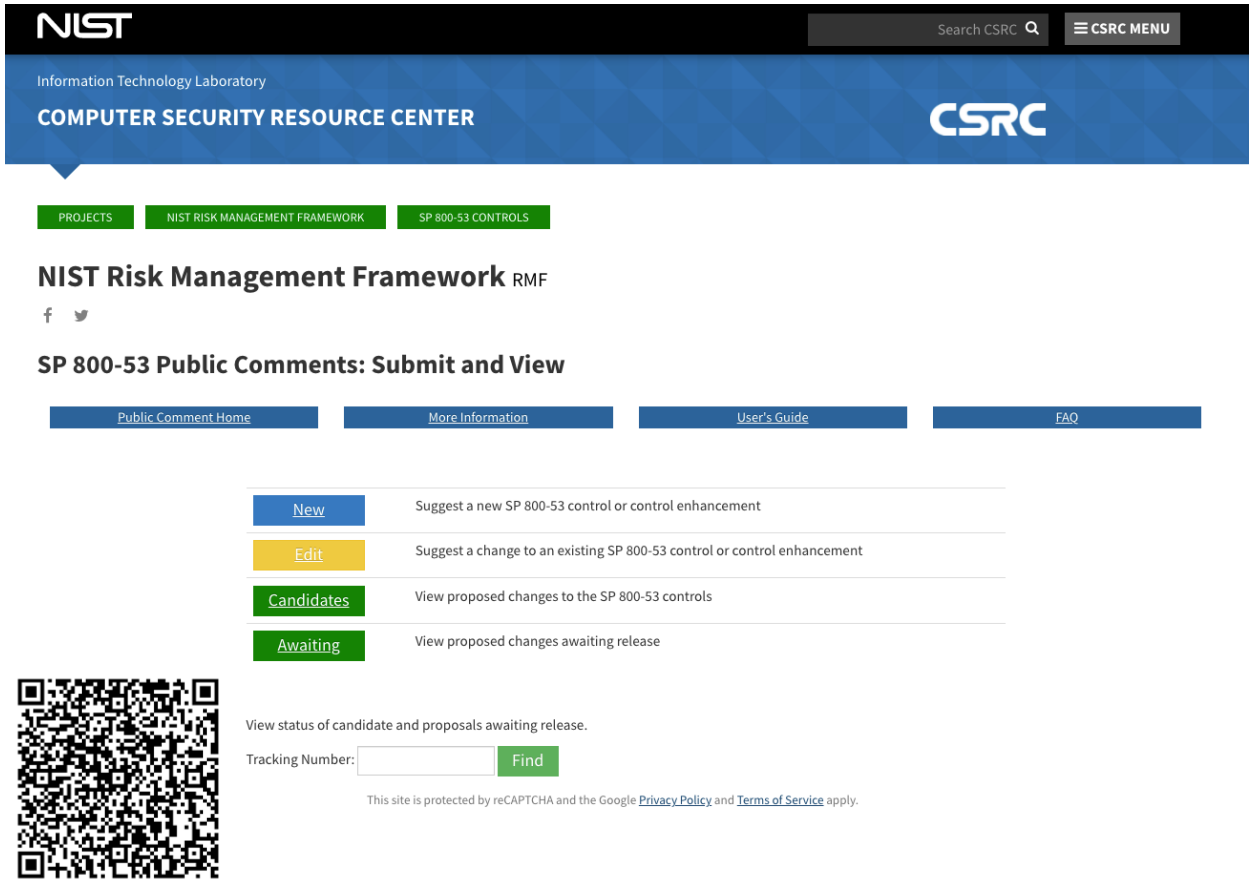
- ☑ Determine overall effectiveness of implemented controls
- ☑ Indication of quality of risk management process
- ☑ Information about security & privacy strengths/weaknesses of the system/organization

- ⊘ Checklist for compliance
- ⊘ Simple pass/fail results
- ⊘ Paperwork exercise to pass inspections/audits

Summary of Changes: SP 800-53A Rev 5

- Updated assessment procedures to correspond with SP 800-53 Rev 5 controls
- First set of procedures for privacy controls
- Updated assessment procedure structure to:
  - Improve the efficiency of conducting control assessments
  - Provide better traceability between controls and assessment procedures
  - Better support the use of automated tools, continuous monitoring, and ongoing authorization programs
- Assessment procedures in PDF, CSV, spreadsheet, plain text, and OSCAL (XML, YAML, JSON) formats

Future Revisions of NIST SP 800-53



https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/public-comments

SP 800-53 controls, baselines, and assessment procedures* as a **machine-readable & web-based data set**

Suggest new controls, improve existing controls anytime.

Comment on draft controls and see feedback from others.

Receive status updates on your comments!

Preview planned changes in next revision.

Additional Resources

Risk Management Framework

https://nist.gov/RMF

RMF resources for implementers, controls & baselines search, 800-53 control downloads in multiple data formats, and 3-hour online intro to RMF course.

OSCAL on GitHub

https://github.com/usnistgov/oscal-content

OSCAL content for SP 800-53 controls (Rev 4, Rev 5, and draft baselines).

Available in XML, JSON, and YAML

NIST Computer Security Resource Center

https://csrc.nist.gov

NIST cybersecurity and privacy publications, project pages, events and other resources

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

STAY IN TOUCH

CONTACT US

nist.gov/RMF

sec-cert@nist.gov

@NISTcyber