SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-53 Rev. 5 – Low / Moderate / High

NIST SP 800-53 Rev. 5 provides a catalog of security and privacy controls to manage risks to information systems.

What it is

NIST SP 800-53 Revision 5 is a comprehensive cybersecurity and privacy control framework that helps organizations manage security risks and protect sensitive information across information systems. This framework establishes a catalog of security and privacy controls designed to strengthen the resilience and trustworthiness of organizational operations.

Published by the National Institute of Standards and Technology (NIST), NIST SP 800-53 is widely adopted by federal agencies, contractors, and regulated entities as part of compliance requirements and risk management programs. The framework covers areas such as access control, incident response, risk assessment, system and communications protection, and privacy governance, aligning closely with broader regulatory and security standards like the NIST Risk Management Framework (RMF).

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION NIST SP 800-53 Revision 5
EFFECTIVE September 2020	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Very High

Source: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Why it matters

- **Strengthen risk-based security governance** Establishes a structured approach for assessing and managing cybersecurity and privacy risks across systems and business processes.
- **Support regulatory and compliance obligations** Aligns internal policies with federal and sector-specific requirements, simplifying compliance efforts and audit preparation.
- **Promote operational resilience** Improves the organization's ability to withstand, respond to, and recover from cybersecurity incidents and service disruptions.
- **Enhance data protection practices** Implements robust controls to secure sensitive information and mitigate risks related to unauthorized access, disclosure, or data breaches.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-53 Rev.5

Control Catalog and Tailoring

Manage 800-53 controls, parameters, and tailored baselines by system.

System-to-Control Mapping

Link controls to systems, assets, and owners for clear accountability.

Evidence Collection and Audit Trail

Centralize evidence, test results, and documentation tied to each control.

Assessments, POA&Ms, and Corrective Actions

Track assessments, POA&Ms, corrective actions, and closure verification.

Vendor Control and Attestation Management

Manage vendor controls, attestations, and monitoring aligned to 800-53 expectations.

Reporting and Readiness Dashboards

Report coverage, gaps, and risk posture across systems, families, and owners.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-171 Rev. 3 | NIST 800-37 Rev.2 | SOC 2

Official resources

NIST SP 800-53 Revision 5

Defines the security and privacy controls for federal information systems.

csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST Security and Privacy Controls Implementation Guide

Outlines methods to implement NIST SP 800-53 controls effectively.

csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

Risk Management Framework (RMF) Overview

Outlines the RMF and details integration of NIST SP 800-53 controls.

csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Frequently asked questions

What is NIST SP 800-53 used for?

NIST SP 800-53 is a framework used to implement and manage security and privacy controls for federal information systems and organizations. It helps organizations reduce risks to their operations, assets, and individuals by providing a comprehensive catalog of controls covering access, incident response, and privacy management.

Is NIST SP 800-53 a required or certifiable standard?

NIST SP 800-53 is mandatory for U.S. federal agencies and contractors managing federal data, but it is not a certifiable standard in itself. Compliance is typically demonstrated through independent assessments, audits, and integration with broader programs like the NIST Risk Management Framework (RMF).

What is the scope of NIST SP 800-53?

The scope of NIST SP 800-53 covers all federal information systems, except those related to national security, and is applicable to organizations that process, store, or transmit federal data. Private and regulated entities often adopt these controls as industry benchmarks for comprehensive security and privacy management.

What are the key components or artifacts required by NIST SP 800-53?

Key artifacts include system security plans, risk assessments, control implementation summaries, and evidence of ongoing control monitoring and remediation. Organizations must document how selected controls are applied, tailored, and evaluated in the context of their specific operations.

 © 2026 SmartSuite Inc. All rights reserved.

How do organizations implement NIST SP 800-53 controls?

Organizations implement NIST SP 800-53 by categorizing their information systems, selecting appropriate baseline controls based on impact levels, tailoring controls as needed, and documenting the implementation in security plans. Regular risk assessments and control effectiveness evaluations are integral to the process.

How does NIST SP 800-53 relate to other security frameworks?

NIST SP 800-53 aligns closely with the NIST RMF and supports compliance with regulations such as FISMA. Its control catalog can be mapped to other frameworks like ISO 27001, aiding organizations that must meet multiple regulatory and risk management requirements.

What are the ongoing compliance requirements for NIST SP 800-53?

Ongoing compliance requires continuous monitoring of controls, regular risk and vulnerability assessments, and prompt remediation of identified issues. Documentation, testing, and audit readiness must be maintained to ensure both operational effectiveness and regulatory alignment.

How would SmartSuite support NIST SP 800-53?

SmartSuite supports NIST SP 800-53 by providing centralized control libraries, risk registers, and policy management tools. It enables automated evidence collection, compliance tracking, and structured remediation workflows, all supporting audit readiness. Dashboards and reporting features offer ongoing oversight of risk management, control effectiveness, and security posture for organizations implementing the framework.

License included / downloadable: Yes NIST SP 800-53 Rev. 5 is publicly available from NIST. No separate commercial license is required to access the framework.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-53-rev-5

 © 2026 SmartSuite Inc. All rights reserved.