SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-53 Rev.4 – Low / Moderate / High

NIST SP 800-53 Rev. 4 provides security and privacy controls to help organizations protect federal information systems and manage risk.

What it is

NIST SP 800-53 Revision 4 is a cybersecurity and privacy control framework that helps organizations safeguard federal information systems and manage risk. It provides a comprehensive catalog of security and privacy controls to protect the confidentiality, integrity, and availability of sensitive information.

Developed and published by the National Institute of Standards and Technology (NIST), this framework is primarily used by U.S. federal agencies and contractors but is also adopted by private-sector organizations aiming to align with rigorous security requirements. The controls cover areas such as access control, incident response, risk assessment, system and communications protection, and privacy governance.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Control Framework	VERSION Rev. 4
EFFECTIVE April 2013	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Very High		

Source: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

Why it matters

- **Strengthen security governance** Enable organizations to establish consistent security oversight and accountability across all information systems and operational processes.
- **Enhance regulatory compliance** Support adherence to federal regulations such as FISMA, helping organizations demonstrate compliance during audits and reduce regulatory risk.
- **Increase audit readiness** Provide a structured set of controls and documentation practices, making it easier to prepare for internal and external security audits.
- **Improve incident detection and response** Implement robust controls that facilitate early threat identification and prompt response to cybersecurity incidents, reducing potential impact.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-53 Rev.4

NIST Control Catalog Management

Organize the full NIST 800-53 control families with ownership, scope, implementation notes, and system applicability.

Control Implementation and Monitoring

Track implementation status, operational cadence, and control effectiveness across systems and security domains.

Risk and Control Linkage

Link controls to system risks, mitigation strategies, and system security plans for structured risk management.

Evidence Collection and Assessment Readiness

Capture assessment evidence, artifacts, and documentation tied to each control for audit and authorization reviews.

Control Deficiency and Monitoring Tracking

Track control deficiencies, remediation tasks, and monitoring activities required for ongoing compliance.

Security Authorization and Assessment Readiness Reporting

Provide dashboards showing control coverage, open findings, and readiness for security authorization and assessment processes.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | FedRAMP Rev. 5 | HIPAA (NIST SP 800-66 Rev. 2) | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | PCI DSS 4.0.1 | SOC 2

Official resources

NIST SP 800-53 Revision 4 Publication

Provides comprehensive security and privacy controls for federal information systems.

csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

NIST Risk Management Framework Overview

Outlines the integration of security and privacy into the system development life cycle.

csrc.nist.gov/projects/risk-management

NIST SP 800-53 Control Families

Outlines the control families included in the SP 800-53 standard.

csrc.nist.gov/publications/detail/sp/800-53/rev-4/final#appendix-D

NIST SP 800-53A Revision 4 Guide

Provides assessment procedures for evaluating security and privacy controls.

csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final

Frequently asked questions

What is NIST SP 800-53 Rev. 4 used for?

NIST SP 800-53 Rev. 4 is used to establish and implement security and privacy controls for federal information systems. It helps organizations manage risk and protect the confidentiality, integrity, and availability of sensitive federal data. The framework is widely adopted to demonstrate compliance with federal mandates such as FISMA.

Is NIST SP 800-53 Rev. 4 mandatory or certifiable?

NIST SP 800-53 Rev. 4 is mandatory for U.S. federal agencies and their contractors, as required by FISMA. However, it is not a certifiable standard, meaning organizations do not receive certification; rather, compliance is assessed as part of federal information system authorization processes.

Who is required to comply with NIST SP 800-53 Rev. 4?

Compliance with NIST SP 800-53 Rev. 4 is required for all U.S. federal agencies and organizations processing federal information, including many federal contractors. Private-sector organizations may voluntarily adopt the controls to align with rigorous security baselines or support federal partnership requirements.

 © 2026 SmartSuite Inc. All rights reserved.

What are control families and baselines in NIST SP 800-53 Rev. 4?

Control families in NIST SP 800-53 group related controls into categories such as Access Control, Incident Response, and Risk Assessment. Baselines define minimum sets of controls for low, moderate, and high-impact systems, guiding organizations on the controls appropriate to their risk environment.

How should organizations implement NIST SP 800-53 Rev. 4 controls?

Organizations implement the controls by selecting a baseline, performing risk assessments, and tailoring controls to system-specific requirements. Implementation involves integrating technical, operational, and managerial safeguards, followed by ongoing monitoring and documented assessment.

How does NIST SP 800-53 Rev. 4 relate to the Risk Management Framework (RMF)?

NIST SP 800-53 Rev. 4 is integral to the NIST Risk Management Framework (RMF), providing the control catalog used in system categorization, security control selection, implementation, and continuous monitoring steps. This relationship enables consistent alignment of controls to risk management processes.

What ongoing compliance activities are required for NIST SP 800-53 Rev. 4?

Ongoing compliance requires continuous monitoring, regular control assessments, maintenance of risk and vulnerability registers, and prompt update of Plans of Action and Milestones (POA&Ms). Documentation of evidence and preparation for periodic system reauthorization are also key to sustaining compliance.

How would SmartSuite support NIST SP 800-53 Rev. 4?

SmartSuite streamlines NIST SP 800-53 Rev. 4 compliance by centralizing risk tracking, managing control libraries, and facilitating evidence collection. The platform supports audit readiness by tracking compliance status, managing remediation plans, and providing real-time reporting dashboards to demonstrate governance and support regulatory requirements.

License included / downloadable: Yes NIST Special Publication 800-53 Rev. 4 is published by NIST and is publicly available free from NIST's website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-53-rev-4

 © 2026 SmartSuite Inc. All rights reserved.