SmartSuite

Framework / Supply Chain Security / NIST Special Publications

NIST SP 800-161 Rev. 1 (Flow Down)

NIST SP 800-161 Rev. 1 (Flow Down) guides flow of cybersecurity supply chain risk management requirements to suppliers.

What it is

NIST SP 800-161 Revision 1 (Flow Down) is a cybersecurity risk management framework that helps organizations manage supply chain risks for information systems and critical assets. The framework focuses on identifying, assessing, and mitigating cybersecurity threats originating from third-party suppliers and contractors throughout an organization's supply chain.

Developed and published by the National Institute of Standards and Technology (NIST), this framework is used by federal agencies, defense contractors, and private sector organizations managing critical infrastructure. It covers areas including cybersecurity controls, supply chain risk management processes, threat identification, supplier risk assessment, and compliance with federal regulations.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION Rev. 1
EFFECTIVE May 2022	DOMAIN Supply Chain Security	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY High

Source: https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final

Why it matters

- **Strengthen supply chain security governance** Establishes clear policies and responsibilities for managing cybersecurity risks throughout the supply chain lifecycle.
- **Improve vendor oversight and control** Provides structured assessments and monitoring to reduce risk exposure from third-party products, services, and relationships.
- **Enhance regulatory and compliance alignment** Supports compliance with federal and industry requirements for supply chain risk management and documentation.
- **Promote operational resilience** Improves preparedness for disruptions by identifying critical dependencies and ensuring continuity through risk-informed practices.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-161 Rev. 1

Supplier Inventory and Classification

Maintain an inventory of suppliers, contractors, and service providers supporting systems and operations.

Contractual Security Requirements Tracking

Track baseline cybersecurity requirements applied to vendors and contractual obligations.

Supplier Cybersecurity Posture Assessment

Assess supplier cybersecurity posture and identify potential supply chain risks.

Third-Party Security Monitoring

Track vendor security incidents, vulnerabilities, and remediation actions affecting the organization.

Supplier Contract and Attestation Management

Manage supplier contracts, compliance documentation, and security attestations.

Vendor Risk Exposure and Compliance Reporting

Provide dashboards summarizing vendor risk exposure, supplier compliance status, and mitigation progress.

Common framework mappings

CIS Controls v8.1 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | NIST 800-171 Rev. 3 | PCI DSS 4.0.1 | SOC 2

Official resources

NIST SP 800-161 Rev. 1

Defines supply chain risk management practices for federal information systems and organizations.

csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

NIST Cybersecurity Framework Overview

Outlines the structure and components of the NIST Cybersecurity Framework for organizations.

nist.gov/cyberframework

NIST Risk Management Framework (RMF)

Outlines the process for risk management in federal information systems.

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

NIST 800 Series Publications

Provides a collection of guides and standards for cybersecurity risk management.

csrc.nist.gov/publications/sp800

Frequently asked questions

What is NIST SP 800-161 Rev. 1 used for?

NIST SP 800-161 Rev. 1 provides organizations with guidelines for identifying, assessing, and mitigating cybersecurity risks in their supply chains. It aims to reduce vulnerabilities associated with the acquisition and management of information and communication technology (ICT) products and services throughout their lifecycle.

Is NIST SP 800-161 Rev. 1 mandatory or certifiable?

NIST SP 800-161 Rev. 1 is not a certifiable standard, nor is it mandatory for all organizations. However, organizations supporting U.S. federal systems or those wishing to align with federal supply chain risk management (SCRM) best practices may be required or strongly encouraged to adopt its controls.

Who does NIST SP 800-161 Rev. 1 apply to?

NIST SP 800-161 Rev. 1 applies to organizations that procure, integrate, or operate products and services from external suppliers, especially those in federal, defense, or critical infrastructure sectors. It is relevant to any entity seeking to manage cyber supply chain risk in their operations.

 © 2026 SmartSuite Inc. All rights reserved.

What are the key components or artifacts of NIST SP 800-161 Rev. 1?

Key components include supply chain risk assessments, control baselines, supplier due diligence documentation, and SCRM plans. Organizations are expected to maintain records of supplier verification, risk mitigation strategies, and continuous monitoring of supply chain-related threats.

How do organizations implement NIST SP 800-161 Rev. 1 controls?

Implementation involves integrating supply chain risk management processes into existing risk and cybersecurity programs. This includes establishing governance structures, performing supplier risk assessments, documenting requirements in acquisition contracts, and continuously monitoring supplier performance and cyber threats.

How does NIST SP 800-161 Rev. 1 relate to other security frameworks?

NIST SP 800-161 Rev. 1 complements other frameworks like NIST SP 800-53 and the Cybersecurity Framework by providing additional focus on supply chain risks. It extends core security controls to address third-party and supplier contexts, supporting broader compliance and risk management efforts.

What are the ongoing compliance requirements for NIST SP 800-161 Rev. 1?

Ongoing compliance requires maintaining current supplier inventories, updating risk assessments, monitoring for new threats, and ensuring continued effectiveness of controls. Regular audits, reporting, and adaptation to regulatory changes are also necessary components of compliance.

How would SmartSuite support NIST SP 800-161 Rev. 1?

SmartSuite enables organizations to manage NIST SP 800-161 Rev. 1 compliance by tracking supplier risks, maintaining control libraries, collecting evidence for supply chain controls, and facilitating audit readiness. Its dashboards and reporting capabilities support continuous monitoring and streamline compliance assessments for executive oversight.

License included / downloadable: Yes NIST SP 800-161 Rev. 1 is publicly available for free from the NIST website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/nist-800-161-rev-1-flow-down