SmartSuite

Framework / Supply Chain Security / NIST Special Publications

NIST SP 800-161 Rev. 1 – Level 1

Provides guidance for identifying, assessing, and mitigating cybersecurity risks across organizational supply chains and system components.

What it is

NIST SP 800-161 Rev. 1 is a cybersecurity and risk management framework that guides organizations in managing cyber supply chain risks throughout the lifecycle of systems and services. Its primary aim is to help organizations identify, assess, and mitigate risks associated with the use of third-party products and suppliers.

Developed and published by the National Institute of Standards and Technology (NIST), the framework is applicable to federal agencies, contractors, and critical infrastructure operators but is also relevant for private sector organizations with complex supply chains. NIST SP 800-161 Rev. 1 outlines requirements for supply chain risk management (SCRM), including the integration of security controls, risk assessment processes, and due diligence across procurement, development, and operations.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Rev. 1
EFFECTIVE May 5, 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 cybersecurity governance** Establish clear accountability and structured oversight for supply chain risks throughout the technology lifecycle.
- **Enhance risk-informed decision-making** Enable organizations to make procurement and partnership choices based on thorough assessments of vendor and supplier risks.
- **Support regulatory and compliance efforts** Facilitate alignment with federal requirements and standards, promoting consistency in risk management practices across agencies.
- **Improve detection of supply chain threats** Bolster capabilities to identify, monitor, and respond to emerging threats and vulnerabilities within diverse supply chain environments.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-161 Rev.1 Level 1

Supplier Security Control Library

Organize supplier cybersecurity requirements aligned with NIST SP 800-161 risk management practices.

Advanced Vendor Risk Assessments

Evaluate supplier cybersecurity posture using structured assessments and security questionnaires.

Vendor Compliance and Attestation Tracking

Track vendor control effectiveness, security attestations, and compliance documentation.

Incident and Vulnerability Coordination

Manage supplier-related vulnerabilities and coordinate remediation activities with affected vendors.

Supply Chain Risk Governance

Integrate supplier risks into enterprise risk management processes and security oversight programs.

Supplier Risk Exposure and Compliance Reporting

Provide dashboards showing supplier risk exposure, compliance status, and remediation progress.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | FedRAMP Rev. 5 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-37 Rev.2 | NIST 800-53 Rev.5 | PCI DSS 4.0.1

Official resources

NIST SP 800-161 Rev. 1 Document

Provides detailed guidance on Cybersecurity Supply Chain Risk Management (C-SCRM).

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

NIST Cyber Supply Chain Risk Management

Describes cybersecurity practices and controls for managing risks in the supply chain.

csrc.nist.gov/projects/cyber-supply-chain-risk-management

Supply Chain Risk Management Practices Guide

Outlines best practices for protecting supply chain integrity and security.

csrc.nist.gov/projects/cyber-supply-chain-risk-management

NIST C-SCRM Program Overview

Provides an overview of NIST's Cyber Supply Chain Risk Management initiatives and resources.

csrc.nist.gov/Projects/cyber-supply-chain-risk-management

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 required or certifiable?

NIST SP 800-161 Rev. 1 is mandatory for U.S. federal agencies per executive and regulatory directives. However, it is not a certifiable framework—there is no official certification for organizations. Agencies and contractors must demonstrate compliance through policy, process implementation, and ongoing risk management activities.

What is the scope of NIST SP 800-161 Rev. 1?

The scope of NIST SP 800-161 Rev. 1 covers information systems, components, and services obtained through supply chains in federal and critical infrastructure organizations. It applies to both information security and privacy programs and spans from initial acquisition to disposal of systems and related products.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are key concepts or artifacts required by NIST SP 800-161 Rev. 1?

Key artifacts include supply chain risk assessments, supplier evaluation criteria, contract language addressing cybersecurity, documented risk management strategies, and continuous monitoring processes. Organizations must also develop SCRM plans and maintain evidence of due diligence in supplier selection and risk mitigation.

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

Implementation involves integrating supply chain risk management into existing cybersecurity and procurement processes. Organizations must conduct risk assessments, establish supplier requirements, embed SCRM controls in contracts, and monitor supplier performance and compliance throughout the system lifecycle.

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

NIST SP 800-161 Rev. 1 complements NIST SP 800-53 by focusing specifically on supply chain controls and requirements. It aligns with other frameworks like ISO 27036 for supply chain security, ensuring practices are harmonized and comprehensive as part of a broader risk management strategy.

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 NIST. License included with platform

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

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.