SmartSuite

Framework / Supply Chain Security / NIST Special Publications

NIST SP 800-161 Rev. 1 – Level 3

NIST SP 800-161 Rev. 1 provides practices to manage cybersecurity risks across systems and organizational supply chains.

What it is

NIST SP 800-161 Revision 1 is a cybersecurity supply chain risk management (C-SCRM) framework that assists organizations in identifying, assessing, and mitigating risks to their information systems and critical operations arising from their supply chain relationships. The framework provides structured guidance to help organizations strengthen the security, integrity, and resilience of products and services acquired from external suppliers and partners.

Published by the National Institute of Standards and Technology (NIST), this standard is used by federal agencies, contractors, and private sector organizations to manage cybersecurity, compliance, and operational risks associated with supply chain activities. NIST SP 800-161 Rev. 1 covers areas such as supply chain risk assessment, supplier controls, procurement requirements, and integration with broader risk management and cybersecurity programs.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	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 oversight** Promote effective evaluation and monitoring of suppliers and service providers to minimize security vulnerabilities introduced through third parties.
- **Enhance regulatory alignment** Enable organizations to align cybersecurity supply chain risk management practices with federal and industry compliance requirements.
- **Increase risk visibility** Provide structured approaches to identify, assess, and prioritize supply chain risks across the entire system lifecycle.
- **Promote operational resilience** Support continuity of critical operations by reducing potential disruptions stemming from supply chain incidents or compromises.

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

How SmartSuite supports NIST 800-161 Rev.1 Level 3

Enterprise Supply Chain Security Governance

Structure policies, roles, and oversight for managing cybersecurity risks across the supplier ecosystem.

Advanced Vendor Risk Intelligence

Integrate threat intelligence and supplier risk indicators to identify emerging supply chain threats.

Critical Supplier and Dependency Tracking

Track critical suppliers, system dependencies, and high-risk components affecting mission operations.

Supplier Incident Investigation and Remediation

Coordinate investigation and remediation of cybersecurity incidents involving suppliers and partners.

Supplier Assurance and Compliance Monitoring

Monitor supplier compliance with contractual security requirements and regulatory obligations.

Strategic Supply Chain Risk Reporting

Provide leadership dashboards summarizing supplier risk posture, dependency risks, and mitigation progress.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-37 Rev.2 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

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 Cybersecurity Supply Chain Risk Management Practices

Outlines implementation strategies for managing cybersecurity risks in supply chains.

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

NIST Risk Management Framework

Describes the framework for integrating supply chain risk management into system lifecycle.

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

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 compliance with NIST SP 800-161 Rev. 1 mandatory?

For U.S. federal agencies, using NIST SP 800-161 Rev. 1 is mandated by federal regulations and executive orders. For private sector and non-federal organizations, adoption is voluntary but recommended for those managing complex or critical supply chains.

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 the key concepts or required artifacts in NIST SP 800-161 Rev. 1?

Key concepts include risk identification, risk assessment, and mitigation strategies focused on supply chain threats and vulnerabilities. Required artifacts often include supply chain risk assessments, documented C-SCRM policies, supplier risk profiles, and ongoing monitoring mechanisms.

How should organizations approach implementing NIST SP 800-161 Rev. 1?

Organizations should take a risk-based approach by establishing robust C-SCRM policies, integrating risk management activities into procurement and contracting processes, and continuously monitoring supplier risk. Collaboration between cybersecurity, acquisition, and risk management functions is crucial for successful implementation.

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

NIST SP 800-161 Rev. 1 aligns with NIST SP 800-53 controls and complements frameworks such as NIST Cybersecurity Framework (CSF) and ISO 27036. It offers more specialized guidance specific to supply chain risks, often referenced by other frameworks for comprehensive supply chain management.

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 published by NIST and is publicly available for free from NIST's website.
License included with platform

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-161-rev-1-level-3

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