

NIST SP 800-161 Rev. 1

NIST SP 800-161 Rev. 1 guides organizations to identify, assess, and mitigate cybersecurity risks across their supply chains.



What it is

NIST SP 800-161 Revision 1, Cybersecurity Supply Chain Risk Management (C-SCRM), is a specialized cybersecurity risk management framework that supports organizations in identifying, assessing, and mitigating risks within their supply chains. Its primary purpose is to address threats that can arise throughout the acquisition, integration, and operational lifecycles of products and services.

Issued by the National Institute of Standards and Technology (NIST), this framework is used by federal agencies, critical infrastructure sectors, and organizations that depend on complex supply chains. NIST SP 800-161 Rev. 1 covers controls for supply chain security, procurement risk, supplier evaluation, continuity, and regulatory compliance, and it aligns with broader risk management standards such as NIST SP 800-53 and NIST’s Risk Management Framework (RMF).

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION NIST SP 800-161 Revision 1
EFFECTIVE May 2024	DOMAIN Cybersecurity	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 governance** Establish structured oversight for identifying and controlling risks across acquisition, procurement, and supplier relationships.
- **Enable informed supplier risk management** Support consistent evaluation and monitoring of suppliers to reduce vulnerabilities stemming from third-party products and services.
- **Improve regulatory compliance posture** Align security practices with federal and industry standards, streamlining documentation and reporting for audits and regulatory reviews.
- **Enhance threat response capabilities** Facilitate timely detection and remediation of supply chain incidents, reducing the impact of compromised or counterfeit components.

How SmartSuite supports NIST SP 800-161 Rev.1

Supplier Inventory and Tiering

Centralize vendor inventory, criticality tiers, and dependency mapping.

Due Diligence and Assessments

Standardize supplier security assessments, evidence requests, and approvals.

Contract Security Clauses and Renewals

Track security clauses, obligations, and renewal review cadences per supplier.

Ongoing Monitoring and Reviews

Manage recurring monitoring for incidents, posture changes, and compliance drift.

Findings, Corrective Actions, and Risk Acceptance

Track findings, corrective actions, compensating controls, and risk acceptance.

Supply Chain Risk Reporting

Report supplier risk posture, open issues, and concentration risk to leadership.

Common framework mappings

EU DORA

ISO 28000

ISO 27001:2022

ISO 27002:2022

MITRE ATT&CK

NIST CSF 2.0

NIST 800-53 Rev.5

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 Risk Management Framework (RMF) Overview

Describes the integration of NIST SP 800-53 controls within the Risk Management Framework.

csrc.nist.gov/projects/risk-management

NIST SP 800-53 Control Catalog

Defines security controls for federal information systems, applicable to low-impact OT environments.

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

NIST Cyber Supply Chain Risk Management (C-SCRM) Program

Outlines program strategies for implementing supply chain cybersecurity risk measures.

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 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.

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.

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

Key concepts include supply chain risk assessment, supplier evaluation, risk mitigation planning, and continuous monitoring. Required artifacts often include supplier risk registers, documented contract requirements, compliance matrices, and evidence of ongoing risk management activities.

How is NIST SP 800-161 Rev. 1 implemented in practice?

Organizations implement NIST SP 800-161 Rev. 1 by integrating C-SCRM controls into their procurement processes, establishing supplier assessment criteria, defining contractual security requirements, and conducting ongoing risk monitoring and reporting. Formal governance and executive oversight are essential for effective implementation.

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

NIST SP 800-161 Rev. 1 extends the NIST Risk Management Framework (RMF) and references the control families in NIST SP 800-53. It enables organizations to harmonize supply chain risk management with broader enterprise risk management and cybersecurity programs.

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 is publicly available through official NIST publications.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-161-rev-1-cybersecurity-supply-chain-risk-management-c-scrm