SmartSuite

Framework / Supply Chain Security / NIST Special Publications

NIST SP 800-161 Rev.1 – Level 2

NIST SP 800-161 Rev. 1 provides practices for systems and organizations to identify and mitigate cybersecurity supply chain risks.

What it is

NIST SP 800-161 Revision 1 is a cybersecurity supply chain risk management (C-SCRM) framework that helps organizations identify, assess, and mitigate risks associated with acquiring and integrating information and communications technology products and services. Its primary purpose is to strengthen organizational resilience by addressing vulnerabilities within supply chains that may impact the security and integrity of information systems.

Published by the National Institute of Standards and Technology (NIST), this framework is widely adopted across federal agencies, defense contractors, and private sector entities seeking to comply with U.S. government cybersecurity mandates. NIST SP 800-161 Rev. 1 addresses critical areas such as supply chain risk assessment, cybersecurity controls, contract requirements, and continuous risk monitoring, and is closely aligned with other NIST publications and the Risk Management Framework (RMF).

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 Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

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

Why it matters

- **Strengthen supply chain governance** Enhance oversight of suppliers and partners to identify, assess, and address risks affecting organizational information systems.
- **Support regulatory compliance** Align acquisition and risk management activities with federal requirements to enable consistent, auditable compliance with government mandates.
- **Improve risk assessment capabilities** Systematically identify vulnerabilities in ICT products and suppliers, enabling proactive risk mitigation and better-informed procurement decisions.
- **Enhance operational resilience** Reduce the likelihood and impact of supply chain disruptions by continuously monitoring and managing risks to mission-critical systems.

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

How SmartSuite supports NIST SP 800-161 Rev.1 Level 2

Security Requirements and Engineering Traceability

Capture security requirements and trace them across system architecture, components, and lifecycle phases.

Risk-Informed System Design

Link threats, vulnerabilities, and risks to engineering decisions and system design controls.

Secure Development Lifecycle Governance

Manage security activities across design, development, integration, and deployment stages.

Verification, Validation, and Assurance Evidence

Track testing, validation results, and assurance artifacts tied to security requirements.

Supply Chain and System Integration Oversight

Monitor supplier components, system integrations, and external dependencies impacting security.

Engineering Risk and Compliance Reporting

Provide visibility into system risk posture, control coverage, and engineering assurance status.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | FedRAMP Rev. 5 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | NIST 800-171 Rev. 3 | SOC 2 | Cyber Essentials

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

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.

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.

What key concepts and artifacts does NIST SP 800-161 Rev. 1 require?

Key concepts include risk assessment, supply chain mapping, threat identification, and mitigation strategy development. Critical artifacts required may include C-SCRM plans, supplier risk assessments, due diligence documentation, and ongoing monitoring records. Documentation must demonstrate the implementation and maintenance of robust supply chain controls.

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

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

Implementation involves integrating C-SCRM into existing risk management processes and aligning with the organization's cybersecurity policies. Organizations should assess supply chain risk, develop tailored policies, define supplier requirements, and continuously monitor suppliers. Ongoing training and periodic reviews 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.

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. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-161-rev-1-level-2

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