SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-161 Rev. 1

NIST SP 800-161 Rev. 1 is NIST's C-SCRM guidance: three-level risk management, 20 control families with supply chain guidance, risk scenarios and templates.



What it is

NIST SP 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, is NIST's foundational guidance for identifying, assessing and mitigating cybersecurity risks in the ICT and operational technology supply chain at every level of an enterprise. Jon Boyens and Angela Smith of NIST and four Boston Consulting Group co-authors published it on May 5, 2022, superseding the original SP 800-161 of April 8, 2015. Update 1 of November 1, 2024 is the current text, and NIST's C-SCRM project page still names Revision 1 as its foundational publication. It is voluntary guidance for non-federal organizations and written to support federal agencies.

NIST developed it under the Federal Information Security Modernization Act of 2014, and its Authority statement says nongovernmental organizations may use it on a voluntary basis. Section 1.1 defines cybersecurity supply chain risk management (C-SCRM) as a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing response strategies, policies, processes and procedures.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Revision 1 (May 2022), Update 1 of November 1, 2024; supersedes SP 800-161 (April 2015)
EFFECTIVE May 5, 2022 (Update 1: November 1, 2024)	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY High

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

Why it matters

- **Know the exposed assets** Section 2.1 says an established C-SCRM program lets an enterprise understand which critical assets are most susceptible to supply chain weaknesses and vulnerabilities.
- **One approach at three levels** Section 2.3 gives each level its own deliverables: enterprise strategy, policy and implementation plan; mission and business process strategies; and system-level C-SCRM plans.
- **A control set built on SP 800-53** Appendix A adds Supplemental C-SCRM Guidance, with the levels where each control applies, to 20 control families including Supply Chain Risk Management (SR).
- **Templates to adapt** Appendix D provides a C-SCRM strategy and implementation plan template, a policy template, a plan template and a supply chain risk assessment (C-SCRA) template whose Table 26 is the information gathering and scoping questionnaire.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-161 Rev.1

Supplier Inventory and Criticality

Record each supplier with its products and services, the systems they support and an assigned criticality level, and review the inventory on a set frequency (control SR-13).

Three-Level Strategy and Plan Records

Hold the C-SCRM strategy and implementation plan, the Level 1 and 2 policies and the Level 3 system plans, with owners and revision dates, using the Appendix D templates.

Supplier Risk Assessments

Run supplier and product assessments with the Appendix D C-SCRA template and keep scoping answers, threat, vulnerability and impact findings and the response for each.

Control Library with Levels

Load the Appendix A controls as requirements with their Level 1, 2 or 3 assignment, owner, implementation status and evidence in Compliance Management.

Scenario and Risk Register

Log Appendix C threat scenarios with likelihood, impact and the chosen response in Cyber & IT Risk, linked to the suppliers and systems they involve.

Practice Maturity and Measures

Track foundational, sustaining and enhancing practices and the section 3.5 measures in Enterprise Reporting dashboards for leadership.

Common framework mappings

EU DORA | ISO 28000 | ISO 27001:2022 | ISO 27002:2022 | ISO/IEC 27036 | 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 the security and privacy controls for federal information systems that SP 800-161 draws its C-SCRM controls from.

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 and which edition is current?

It is NIST's guidance on cybersecurity supply chain risk management (C-SCRM), published May 5, 2022 and superseding SP 800-161 of April 8, 2015. Update 1, dated November 1, 2024, is the current text, and NIST's project page still calls Revision 1 its foundational C-SCRM publication. It is voluntary for organizations outside the federal government.

What changed in Update 1 of November 2024?

Appendix K lists the changes. NIST deleted Table 3-1 (C-SCRM in the procurement process) as confusing, added a semiconductor manufacturer example to section 2.2, updated references from CSF 1.1 to CSF 2.0 and to SP 800-160 Rev. 1 volumes, and revised guidance for controls such as AC-17, RA-3 and RA-5. It also updated the online Appendix F for OMB M-22-18 software attestations and software bills of materials.

 © 2026 SmartSuite Inc. All rights reserved.

How does SP 800-161 integrate C-SCRM into enterprise risk management?

Section 2.3 uses the three levels of SP 800-39: enterprise, mission and business process, and operational. Level 1 sets the C-SCRM strategy, policy and implementation plan, Level 2 tailors them to mission and business processes, and Level 3 writes system-level C-SCRM plans. A cross-disciplinary C-SCRM Program Management Office (2.3.5) can support all three levels.

What are foundational, sustaining and enhancing C-SCRM practices?

Section 3.4 groups key practices by maturity. Foundational practices include a dedicated multidisciplinary C-SCRM team or PMO and senior leadership support. Sustaining practices build on them, for example continuous monitoring and reassessment of suppliers and C-SCRM metrics. Enhancing practices, such as automation and quantitative risk analysis, come once sustaining practices are standardized across the enterprise.

Is NIST SP 800-161 Rev. 1 mandatory, and how does it relate to FedRAMP and FASCSA?

The Authority statement says nongovernmental organizations may use it voluntarily. Section 1.3 tells federal agencies assessing cloud service providers to apply FedRAMP guidelines first and then this document for what FedRAMP does not address. Appendix E adds guidance for federal executive agencies on supply chain risk assessments under the Federal Acquisition Supply Chain Security Act of 2018.

License included / downloadable: Yes SP 800-161 Rev. 1 is a U.S. government publication, free of charge from NIST and not subject to copyright in the United States (attribution is appreciated); the platform links to the official text.

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