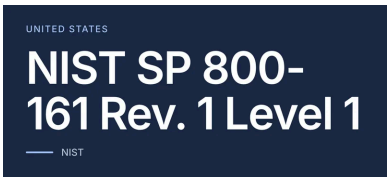
SmartSuite

Framework / Supply Chain Security / NIST Special Publications

# NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (Level 1, Enterprise)

Level 1 of NIST SP 800-161 Rev. 1: the enterprise level where executives set the C-SCRM strategy, policy, high-level implementation plan, governance model and risk appetite (Sec. 2.3.2).




## What it is

This page covers Level 1, the enterprise level, of NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations; the publication as a whole is described on the NIST SP 800-161 Rev. 1 page . Level 1 is where senior leaders set the tone and direction for cybersecurity supply chain risk management (C-SCRM) across the enterprise by providing an overarching C-SCRM strategy, a C-SCRM policy and a high-level implementation plan (Sec. 2.3.2). NIST published Revision 1 on May 5, 2022, replacing the April 8, 2015 edition, and issued Update 1 on November 1, 2024. Federal agencies must use NIST's C-SCRM guidelines by statute; every other organization adopts them voluntarily.

## At a glance

| | | |
|---|---|---|
| PUBLISHER<br>National Institute of Standards and Technology (NIST) | TYPE<br>Guidance | VERSION<br>Revision 1 (May 2022; Update 1 of November 1, 2024) |
| EFFECTIVE<br>May 5, 2022 | DOMAIN<br>Supply Chain Security | FAMILY<br>NIST Special Publications |
| REGION<br>United States | ADOPTION MODEL<br>Voluntary | IMPLEMENTATION COMPLEXITY<br>High |

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

## Why it matters

- **Named executive ownership** The head of the organization owns supply chain cybersecurity risk, and an executive-level individual, office or group is designated to lead agency-wide SCRM activities whatever the organizational structure (Sec. 2.3.2).
- **Three documents that bind the lower levels** The C-SCRM Strategy, the C-SCRM Policy and the High-Level Implementation Plan shape and constrain how C-SCRM is carried out at Level 2 and Level 3 (Sec. 2.3 and Fig. 6).
- **Explicit risk framing** Level 1 states the enterprise's assumptions about threats, vulnerabilities, impact and likelihood, its constraints, its risk appetite and tolerance, and its priorities and trade-offs, which become the inputs to the strategy (Sec. 2.3.2 and Appendix G.2.1).
- **A governance model that fits the enterprise** Sec. 2.3.2 allows centralized authority with a C-SCRM PMO consolidating resource-intensive tasks such as vendor risk assessments, or decentralized authority where business processes are autonomous.


Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

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

### Strategy and Implementation Plan Record

Keep the Appendix D.1 sections as fields: purpose, authority and compliance, strategic objectives, implementation milestones with owners and dates (Tables 14 to 16), roles, definitions and the version table.

### C-SCRM Policy Register

Hold the Appendix D.2 policy with its authority, policy statements, delegated roles, compliance and enforcement expectations and revision history, and record each lower-level policy that implements it.

### Risk Framing Statements

Use Enterprise Risk Management to record the assumptions, constraints, risk appetite and tolerance statements, priorities and trade-offs of the Level 1 Frame step so Levels 2 and 3 tailor from one source (Sec. 2.3.2).

### Governance and Role Map

Record the ERM council, the C-SCRM council, the designated executive lead and the C-SCRM PMO, with the Level 1 roles for acquisition, information security, IT, legal, program management and supply chain and logistics.

### Level 1 Measures Dashboard

Report the Table 4 Level 1 topics: policy adoption at lower levels and its timeliness, adherence to appetite and tolerance statements, risk exposure across Level 2 and compliance with regulatory mandates.

### Level 1 Control Set

Load the Appendix A controls tagged Level 1, such as PM-9, PM-30, SR-1, SR-3, SR-5, SR-11, RA-3 and SA-4, into Compliance Management with owners, status and evidence, using the Table 6 summary as the index.

## Common framework mappings

CIS Controls v8.1 | COBIT 2019 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO/IEC 27036 | 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 does Level 1 of NIST SP 800-161 Rev. 1 cover?

Level 1 is the enterprise level of the three-level structure NIST SP 800-161 Rev. 1 takes from SP 800-39. Sec. 2.3.2 says it sets the tone and direction for enterprise-wide C-SCRM by providing an overarching C-SCRM strategy, a C-SCRM policy and a high-level implementation plan, forms the governance structures through which executives make C-SCRM decisions, and frames risk for the enterprise. Its outputs shape and constrain how C-SCRM is carried out at Level 2 and Level 3.

### Who are the Level 1 stakeholders?

Table 1 lists executive leadership: the CEO, CIO, COO, CFO, CISO, chief technology officer, chief acquisition officer, chief privacy officer and chief risk officer. Sec. 2.3.2 adds that ownership and accountability lie with the head of the organization, that an executive-level individual, office or group should be designated to lead agency-wide SCRM, and that an ERM council, often with a supporting C-SCRM council formed by the CIO or CISO, is where enterprise risk decisions are made.



Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

### Which documents does Level 1 produce?

Three: the C-SCRM Strategy, the C-SCRM Policy and the High-Level Implementation Plan (Sec. 2.3 and Fig. 6). Appendix D.1 gives a template for the strategy and implementation plan, which may be a single document or several, and Appendix D.2 gives a template for the policy. Sec. 2.3.2 also expects Level 1 to define the governance structure and operating model and to establish a C-SCRM PMO or another dedicated function.

### Is Level 1 of NIST SP 800-161 Rev. 1 mandatory?

For federal agencies, yes in substance: NIST's C-SCRM program states that by statute agencies must use NIST's C-SCRM and other cybersecurity guidelines, and Appendix E explains the Federal Acquisition Supply Chain Security Act duty to assess and respond to supply chain risk. For every other organization the publication is voluntary guidance. It is not a certification scheme, and acquirers are told in Appendix A not to write requirements such as "ensure compliance with NIST SP 800-161, Rev. 1 controls" but to select the controls relevant to the acquisition.

### How does Level 1 relate to Levels 2 and 3?

Level 1 outputs are tailored and refined within Level 2 to fit each mission and business process, and Level 2 outputs in turn shape the C-SCRM plans written for individual systems at Level 3 (Sec. 2.3.2 and 2.3.3). The flow is bidirectional: Level 1 outputs are updated from results at the lower levels. Appendix G.2 adds that the Frame, Assess, Respond and Monitor cycle is used primarily at Levels 1 and 2, while the Risk Management Framework of SP 800-37 operates predominantly at Level 3.

License included / downloadable: Yes NIST SP 800-161 Rev. 1 is free of charge from NIST; the Level 1 guidance is Sec. 2.3.2 and Appendices D.1 and D.2 of the same publication.

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


Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.