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 3, Operational)

Level 3 of NIST SP 800-161 Rev. 1: the operational level where system owners and contracting officers write C-SCRM plans, assess suppliers and apply controls under the RMF (Sec. 2.3.4).



What it is

This page covers Level 3, the operational level, of NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations; the complete publication is described on the NIST SP 800-161 Rev. 1 page . Sec. 2.3.4 defines Level 3 as the personnel responsible and accountable for operational activities, including conducting procurements and executing system-related C-SCRM activities across the system development life cycle, and its central product is the C-SCRM plan for an individual system. NIST published Revision 1 on May 5, 2022, superseding the April 8, 2015 edition, and issued Update 1 on November 1, 2024; federal agencies must use NIST's C-SCRM guidelines by statute, and other organizations use them by choice.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Revision 1 (May 2022; Update 1 of November 1, 2024)
EFFECTIVE May 5, 2022	DOMAIN Supply Chain Security	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

- **A plan per system** C-SCRM plans dictate how C-SCRM is integrated into every SDLC phase of a system: acquisition, requirements, architectural design, development, delivery, installation, integration, maintenance and disposal or retirement (Sec. 2.3.4).
- **Risk responses chosen, not assumed** After determining risk, Level 3 evaluates alternative courses of action, accept, avoid, mitigate, share or transfer, and responds by selecting, tailoring, implementing and monitoring C-SCRM controls through the SDLC under the RMF (Sec. 2.3.4).
- **Inherited and system-specific controls** Selected C-SCRM controls are usually a combination of common controls inherited from Levels 1 and 2 and information system-specific controls at Level 3 (Sec. 2.3.4).
- **Tactical reporting for system owners** Level 3 reporting covers implementation, efficiency, effectiveness and the system's exposure, giving system owners insight to make rapid adjustments, with metrics against the appetite and tolerance statements of all three levels (Sec. 2.3.4).

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

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

System C-SCRM Plan Record

Keep the Appendix D.3.1 sections as fields for each system: identifier, description, information type and categorization (Table 19), operational status, diagrams and inventory, connections, control details, roles, contingencies, related laws, revision history and approval.

Component and Supplier Inventory

Track the system's components, their suppliers and life cycle activities in IT Asset Management (ITAM) to satisfy D.3.1.5 and the CM-8 and SR-13 controls tagged for Levels 2 and 3.

Cybersecurity Supply Chain Risk Assessment

Run the Appendix D.4 assessment per product, service or supplier in Third Party Risk Management: Table 26 scoping questions, then threat, vulnerability, impact and risk response analysis with the chosen course of action.

Control Selection and Tailoring Log

Record which C-SCRM controls are inherited common controls from Levels 1 and 2 and which are system-specific, with the tailoring rationale and approvals Appendix A requires, in Cyber & IT Risk.

Living Plan and Continuous Monitoring

Schedule the periodic review and refresh Sec. 2.3.4 expects, link monitoring results to the plan as the reference for monitored controls, and keep PM-31 continuous monitoring evidence in Compliance Management.

Level 3 Measures and Reporting

Report the Table 4 Level 3 topics, design effectiveness, operating effectiveness and cost efficiency of controls, with the system's exposure, to Level 2 so it can act on the results (Sec. 2.3.4).

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 (SP 800-37 Rev. 2)

Describes the seven-step process for categorizing systems and selecting, implementing, assessing, authorizing, and monitoring security and privacy controls (NIST SP 800-37 Rev. 2).

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

Frequently asked questions

What does Level 3 of NIST SP 800-161 Rev. 1 cover?

Level 3 is the operational level. Sec. 2.3.4 says it comprises the personnel responsible and accountable for operational activities, including procurements and system-related C-SCRM across the SDLC, and that C-SCRM is applied to information systems through the development and implementation of C-SCRM plans. Level 3 manages the operational risk exposure from ICT/OT products and services in use or within a system's authorization boundary and executes C-SCRM in accordance with the RMF of SP 800-37.

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

Who is responsible at Level 3?

Sec. 2.3.4 names system owners, contracting officers, contracting officer representatives, architects, system engineers, information security personnel, system integrators and developers. Table 1 lists systems management roles including architects, developers, system owners, QA/QC and testing staff, contracting personnel, C-SCRM PMO staff and control engineers or control system operators, with the activities of developing C-SCRM plans, implementing policies and requirements, adhering to Level 1 and 2 constraints, tailoring to the system across the SDLC and reporting to Level 2.

What goes into a C-SCRM plan?

Along with security control information, Sec. 2.3.4 says the plan holds information on the system, its categorization, operational status, related agreements, architecture, critical system personnel, related laws, regulations and policies, and the contingency plan. Appendix D.3 gives a template whose sections run from system name and identifier and information type and categorization through diagrams, inventory and life cycle activities, information exchange and connections, security control details, role identification, contingencies and emergencies, related laws, revision and maintenance, approval and attachments. The plan may stand alone or form part of the system security and privacy plan.

How does Level 3 use the Risk Management Framework?

Appendix G.2 describes two complementary approaches: Frame, Assess, Respond and Monitor at Levels 1 and 2, and the RMF, which operates predominantly at Level 3 through Prepare, Categorize, Select, Implement, Assess, Authorize and Monitor. Level 1 and 2 inputs are synthesized in the Prepare step and tailored through each successive step to the system or procurement. Sec. 2.3.4 adds that risk response is achieved by selecting, tailoring, implementing and monitoring C-SCRM controls throughout the SDLC in accordance with the RMF.

What is the cybersecurity supply chain risk assessment template?

Appendix D.4 provides a cybersecurity supply chain risk assessment template that guides the review of any third-party product, service or supplier that could present a cybersecurity risk to the procurer. It is a toolbox of questions, typically executed by C-SCRM PMOs at Level 3, covering authority and compliance, description, information gathering and scoping analysis (the Table 26 scoping questionnaire, released as a fillable form on December 2, 2025), threat analysis, vulnerability analysis, impact analysis and risk response analysis. Enterprises tailor it to their Level 1 and Level 2 risk postures.

License included / downloadable: Yes NIST SP 800-161 Rev. 1 is free of charge from NIST; the Level 3 guidance is Sec. 2.3.4 of the same publication, with the C-SCRM plan and risk assessment templates in Appendices D.3 and D.4 and the Table 26 questionnaire as a separate download.

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

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