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 2, Mission and Business Process)

Level 2 of NIST SP 800-161 Rev. 1: the mission and business process level where program owners tailor the C-SCRM strategy, set risk tolerances and run supplier assessments (Sec. 2.3.3).



What it is

This page covers Level 2, the mission and business process level, of NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations; the whole publication is described on the NIST SP 800-161 Rev. 1 page . Sec. 2.3.3 defines Level 2 as the level that addresses how the enterprise's mission and business processes assess, respond to and monitor cybersecurity risks throughout the supply chain, working within the strategy and policies that Level 1 provides. 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 voluntarily.

Level 2 is run by business management: program managers, project managers, integrated project team members, research and development, engineering with SDLC oversight, acquisition and supplier relationship management, cost accounting, and the managers responsible for reliability, safety, security and quality (Table 1). At this level the enterprise defines and manages its C-SCRM program requirements, which Sec. 2.3.3 lists as cost, schedule, performance and security together with non-functional requirements such as reliability, dependability, safety and quality.

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

- **Process-specific strategy, policy and plan** Mission areas and business lines generate their own tailored strategy and implementation plan within the constraints of the enterprise strategy and in conformance with enterprise policy (Sec. 2.3.3).
- **Program requirements with C-SCRM built in** Cost, schedule, performance and security requirements, plus reliability, dependability, safety and quality, are defined and managed at Level 2 (Sec. 2.3.3).
- **Earlier vulnerability reduction** Table 1 assigns Level 2 the task of reducing vulnerabilities at the onset of new IT projects and related acquisitions, and of reviewing the system, human and organizational flaws that expose business, technical and acquisition environments.
- **Risk tolerances set once, used twice** Level 2 tailors the enterprise risk framework by setting risk tolerances and may define common control baselines that Level 3 then applies to individual systems (Table 1 and Sec. 2.3.3).

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

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

Process Strategy and Implementation Plan

Keep each mission or business process's tailored strategy and its implementation plan with roles, milestones, dates and reporting processes as records that reference the enterprise documents they tailor (Sec. 2.3.3).

Supplier Inventory and Segmentation

Maintain the inventory of supplier relationships, contracts and the products and services supplied, grouped as strategic or innovative, mission-critical, sustaining or standard (Sec. 3.1.1; SR-13) in Third Party Risk Management.

Supplier Assessments and Reviews

Run due diligence questionnaires, requests for information and procurement-specific supplier risk assessments against the SR-6 control, and keep the supplier risk profile that Sec. 3.1.2 asks market analysis to produce.

Risk Tolerances and Common Control Baselines

Record the process-level tolerances and the common control baseline decisions that Level 3 will tailor to systems, in Enterprise Risk Management, beside the enterprise appetite statements (Sec. 2.3.3).

Acquisition Requirements and Clauses

Hold the checklist of acquisition security requirements, the C-SCRM criteria used in source selection, the SBOM expectation and the SR-8 notification agreements that go into contracts (Sec. 3.1.1 and 3.1.2).

Level 2 Measures and Reporting

Report the Table 4 Level 2 topics, mitigation effectiveness, time allocation, process risk exposure, requirement adoption and PMO use, to Level 1, and log the Level 3 reports the process acts on (Table 1).

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · FedRAMP Rev. 5 · ISO 27001:2022 · ISO/IEC 27036 · 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 does Level 2 of NIST SP 800-161 Rev. 1 cover?

Level 2 is the mission and business process level. Sec. 2.3.3 says it addresses how the enterprise's mission and business processes assess, respond to and monitor cybersecurity risks throughout the supply chain, acting in accordance with the C-SCRM strategy and policies provided by Level 1. Process-specific strategies, policies and implementation plans dictate how the enterprise's C-SCRM goals are met within each process, and program requirements for cost, schedule, performance, security, reliability, dependability, safety and quality are defined here.

Who works at Level 2?

Table 1 lists business management: program managers, project managers, integrated project team members, research and development, engineering with SDLC oversight, acquisition and supplier relationship management, cost accounting, the managers responsible for reliability, safety, security and quality, and the C-SCRM PMO. Sec. 2.3.3 adds that each mission and business process should be represented and suggests a committee drawn from all of them to coordinate Level 2 strategy and implementation plans.

What is a Level 2 C-SCRM implementation plan?

Sec. 2.3.3 describes it as a detailed roadmap for operationalizing the C-SCRM strategy within a mission and business process. It specifies C-SCRM roles, responsibilities, implementation milestones, dates and the processes for monitoring and reporting. Appendix D provides example templates for the strategy, the implementation plan and the policy, and D-1 notes that the strategy and plan may be developed as one document or split into several.

© 2026, SmartSuite Inc. All rights reserved.

How does Level 2 handle acquisition and suppliers?

Sec. 3.1.1 starts with a current inventory of supplier relationships, contracts and the products and services supplied, mapped into groupings such as mission-critical or standard so that contract language and evaluation criteria can be tailored. Sec. 3.1.2 then integrates C-SCRM into each step of the procurement life cycle, from planning and requirements through market analysis, proposal evaluation against C-SCRM criteria and post-award monitoring, and advises against lowest price, technically acceptable selection for ICT/OT products and services.

What does a C-SCRM PMO do for Level 2?

Sec. 2.3.5 says a PMO may develop C-SCRM starter kits containing a base strategy and a set of policies, procedures and guidelines that each mission and business process customizes, provide subject matter consulting while process-specific strategies and implementation plans are written, advise on or develop common control baselines, and perform risk assessments of suppliers, developers, system integrators and service providers. Table 1 lists forming or collaborating with a PMO among the Level 2 activities.

License included / downloadable: Yes NIST SP 800-161 Rev. 1 is free of charge from NIST; the Level 2 guidance is Sec. 2.3.3 and Sec. 3.1 of the same publication, with templates in Appendix D.

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

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