SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-128 – Guide for Security-Focused Configuration Management of Information Systems

NIST SP 800-128 is NIST's guide to security-focused configuration management (SecCM): four phases, baselines, change control and monitoring for federal systems.



What it is

NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems, is the NIST guide to building, controlling and monitoring secure system configurations. Published in August 2011 and updated with errata on October 10, 2019, it is written for the people who manage the security of U.S. federal information systems and may be used voluntarily by any other organization. It is guidance, not a law or a certifiable standard. Its central term, security-focused configuration management (SecCM), means the management and control of configurations for systems to enable security and facilitate the management of information security risk.

NIST developed the guide under the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551 et seq.). Section 1.1 explains the basis: federal agency security programs must include policies and procedures that ensure compliance with minimally acceptable system configuration requirements, managing system configurations is a minimum security requirement in FIPS 200, and the guide provides implementation guidelines for the Configuration Management family of controls in SP 800-53, CM-1 through CM-9. It applies to all federal information systems other than national security systems, which may use it with the approval of the responsible federal officials.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Original edition (August 2011) with errata update of October 10, 2019
EFFECTIVE August 2011	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: csrc.nist.gov/pubs/sp/800/128/upd1/final

Why it matters

- **An approved baseline** A baseline configuration is a set of specifications that has been formally reviewed and agreed on at a point in time and can be changed only through change control (section 2.3.7, control CM-2).
- **Change reviewed before it happens** Each change is requested, recorded, analyzed for security impact, tested, approved, implemented, verified and closed out (section 3.3.2, controls CM-3 and CM-4).
- **Visibility of components** A component inventory (2.3.4, CM-8) and monitoring show unapproved items, such as a test router left on the network or a wireless access point set up without management consent (3.4).
- **Named accountability** Section 2.4 assigns SecCM duties to the CIO, senior agency information security officer, authorizing official, system owner, SecCM Program Manager, system security officer, system administrator, developer and system user.

How SmartSuite supports NIST SP 800-128

Component Inventory and Configuration Items

Record components and group them into configuration items in IT Asset Management (ITAM), each with one system owner and a lifecycle (sections 2.3.4 and 2.3.5).

Baseline Register

Keep each approved baseline with its version, the common secure configuration it came from and its approver, and retain older baselines for review or rollback (2.3.7).

Change Request Workflow

Run the section 3.3.2 steps in IT Service Management (ITSM): request, record, security impact analysis, test, CCB approval, implementation, verification and close-out.

Configuration Control Board Records

Hold CCB membership, the charter, meeting decisions and the approvals linked to each change, following the Appendix H charter sample.

Monitoring Findings

Log the results of baseline and inventory assessments in Cyber & IT Risk, including unapproved components and deviations, and track each to closure (3.4).

CM Control Evidence

Hold CM-1 through CM-9 as requirements in Compliance Management with the SecCM plan, test results and evidence, and report status to system owners and auditors.

Common framework mappings

NIST 800-53 Rev.5 | NIST 800-53B Rev. 5 | NIST 800-37 Rev.2 | NIST CSF 2.0 | NIST 800-171 Rev. 3 | CIS Controls v8.1 | ISO 27002:2022 | ITIL 4 | COBIT 2019 | CIS Benchmarks

Official resources

NIST SP 800-128 publication page

The NIST Computer Security Resource Center record for the guide and its October 2019 update, with status, abstract, keywords, and authors.

csrc.nist.gov/pubs/sp/800/128/upd1/final

NIST SP 800-128 (PDF, includes updates as of October 10, 2019)

The full text of the guide, including the errata table, the four SecCM phases, and the plan, change request, CCB charter, and impact analysis templates in the appendices.

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

NIST SP 800-53 Rev. 5 publication page

The control catalog whose Configuration Management (CM) family NIST SP 800-128 supports.

csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST National Checklist Program

The NIST program that publishes common secure configuration checklists referenced by the guide as the basis for baseline configurations.

nist.gov/programs-projects/national-checklist-program

Frequently asked questions

What is NIST SP 800-128 and who is it for?

SP 800-128 is the NIST guide to security-focused configuration management (SecCM), published in August 2011 and updated with errata on October 10, 2019. Section 1.1 aims it at organizations that manage the security of federal information systems, and section 1.2 lists CIOs, security officers, system owners, administrators and assessors as its audience. State, local and tribal governments and private organizations are encouraged to use it voluntarily.

What does security-focused configuration management mean?

SecCM is the management and control of configurations for systems to enable security and facilitate the management of information security risk (Chapter 1). The guide assumes information security is part of an organization's overall configuration management and concentrates on its security aspects. Its goal, stated in Chapter 3, is to manage and monitor configurations to achieve adequate security and minimize organizational risk.

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

What are the four phases of SecCM?

Section 2.2 names them: Planning; Identifying and Implementing Configurations; Controlling Configuration Changes; and Monitoring. Chapter 3 covers each in sections 3.1 to 3.4, and monitoring results can send the program back to any earlier phase. Section 3.5 adds the use of SCAP to automate checking.

Which SP 800-53 controls does SP 800-128 support?

Section 1.1 says the guide provides implementation guidelines for the Configuration Management family, CM-1 through CM-9. Section 2.3 ties each concept to controls: CM-1 and CM-9 for policy and the SecCM plan, CM-2 for baselines, CM-3 to CM-5 for change control, security impact analysis and access restrictions, CM-6 and CM-7 for settings and least functionality, and CM-8 for the component inventory.

Is SP 800-128 mandatory?

It is guidance. The authority statement says it may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States, and that it does not alter standards NIST made mandatory for federal agencies. Federal agencies remain responsible for the policies and procedures on minimally acceptable system configuration requirements in their security programs (section 1.1), which this guide helps them implement.

License included / downloadable: Yes SP 800-128 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-800-128-security-focused-configuration-management-information