

NIST SP 800-218 (SSDF) — 2020

NIST SSDF provides practices to integrate security across the software development lifecycle and reduce software vulnerabilities.



What it is

NIST SP 800-218 — Secure Software Development Framework (SSDF) is a cybersecurity framework that provides organizations with a set of practices to integrate security throughout the software development lifecycle and reduce vulnerabilities in software products. The SSDF establishes a foundation for improving the security posture of software by embedding risk management and secure coding techniques during design, development, and maintenance.

Published by the National Institute of Standards and Technology (NIST), the framework is intended for use by software producers, acquirers, and integrators across public and private sectors. It covers essential areas such as secure design, implementation, verification, and software release processes, and aligns with broader risk management and cybersecurity best practices found in frameworks like NIST SP 800-53 and the NIST Cybersecurity Framework.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION NIST SP 800-218 Version 1.1
EFFECTIVE May 2020	DOMAIN Software Security	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY High

Source: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf>

Why it matters

- **Strengthen security oversight** Establishes consistent, organization-wide practices that improve visibility and accountability throughout the software development process.
- **Enhance regulatory alignment** Aligns software development activities with widely recognized standards, supporting compliance initiatives and audit requirements across industries.
- **Promote operational resilience** Reduces the likelihood and impact of software-related incidents by proactively addressing risks at every stage of development.
- **Improve risk management** Enables continuous identification, assessment, and mitigation of cybersecurity risks within both internally developed and third-party software.

How SmartSuite supports NIST 800-218 SSDF

Secure SDLC Requirements Library

Track SSDF practices across design, development, testing, release, and maintenance.

Engineering Evidence Hub

Centralize scan outputs, code review proof, training, and release evidence tied to practices.

Vulnerability Management Workflow

Track findings, remediation SLAs, retesting, and closure with clear ownership.

Supply Chain and Dependency Controls

Manage SBOM/dependency practices, approvals, and exceptions with traceability.

Change and Release Governance

Document release approvals, change risk decisions, and rollback readiness.

Customer-Ready Assurance Reporting

Provide clean reporting on secure development posture and improvement over time.

Common framework mappings

CIS Controls v8.1

ISO 27001:2022

ISO 27002:2022

MITRE ATT&CK

NIST CSF 2.0

NIST SP 800-160 Vol. 1

NIST 800-53 Rev.5

OWASP ASVS 4.0

Official resources

NIST SP 800-218, Secure Software Development Framework (SSDF)

Provides practices for integrating security into the software development lifecycle.
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

NIST Cybersecurity Framework

Describes common policies to improve cybersecurity risk management.
nist.gov/cyberframework

NIST SP 800-53, Security and Privacy Controls for Information Systems

Outlines security controls that align with secure software development processes.
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Frequently asked questions

What is NIST SP 800-218 (SSDF) used for?

The NIST SP 800-218 Secure Software Development Framework (SSDF) is used to guide organizations in integrating secure development practices throughout the software lifecycle. It helps reduce vulnerabilities and manage software security risks by embedding controls during software design, development, and maintenance. The framework is beneficial for software producers, acquirers, and integrators in both public and private sectors.

Is SSDF compliance mandatory or certifiable?

SSDF is not currently mandatory or certifiable as a standalone framework, but its adoption may be required by certain federal contracts or industry regulations. Organizations may align with SSDF to fulfill broader regulatory or compliance obligations, particularly where secure software development is specified.

Who should use NIST SP 800-218, and what is its scope?

NIST SP 800-218 applies to any organization involved in developing, acquiring, or integrating software, regardless of industry or organization size. Its scope covers the entire software development lifecycle, including secure design, coding, verification, supply chain integrity, and vulnerability management.

What are the core practice groups or artifacts required by SSDF?

SSDF defines four primary practice groups: Prepare the Organization, Protect the Software, Produce Well-Secured Software, and Respond to Vulnerabilities. Key artifacts may include security policies, coding standards, risk assessments, secure release procedures, and vulnerability management documentation.

How should organizations implement the Secure Software Development Framework?

Organizations implement SSDF by integrating its recommended practices into existing development workflows, establishing secure coding requirements, performing regular code reviews, and systematically managing risks. Tailoring the implementation to fit organizational environments and supply chain considerations is crucial for effective adoption.

How does SSDF relate to other NIST frameworks such as SP 800-53 or the Cybersecurity Framework?

SSDF is designed to complement other NIST frameworks, such as SP 800-53 and the NIST Cybersecurity Framework, by addressing the specific needs of secure software development. It can be mapped to broader controls and risk management practices, enhancing an organization's overall security and compliance posture.

What ongoing compliance activities are required under SSDF?

Maintaining SSDF alignment requires ongoing risk assessments, periodic software security reviews, timely vulnerability management, and continuous improvement of development policies and procedures. Organizations should monitor the effectiveness of controls and update practices to address emerging security threats and compliance requirements.

How would SmartSuite support NIST SP 800-218 (SSDF)?

SmartSuite helps organizations manage SSDF compliance by centralizing control documentation, tracking software-related risks, and automating evidence collection. The platform supports policy governance, facilitates remediation workflows, and streamlines audit preparation. Real-time dashboards and reporting enable teams to monitor SSDF control implementation, maintain audit readiness, and demonstrate effective secure software development practices.

License included / downloadable: Yes NIST SP 800-218 is publicly available through official NIST publications.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-218-secure-software-development-framework-ssdf