SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-160 Vol. 1 (2016)

NIST SP 800-160 guides integrating security and risk management into system engineering across the lifecycle to build resilient, trustworthy systems.

What it is

NIST SP 800-160 is a systems security engineering framework that helps organizations integrate security and trustworthiness into the engineering of complex systems throughout the system life cycle. The framework provides a structured approach to embedding cybersecurity and risk management principles within system design, development, and operations.

Published by the National Institute of Standards and Technology (NIST), SP 800-160 is used by federal agencies, defense contractors, critical infrastructure operators, and enterprises managing high-value or mission-critical systems. Its guidance covers multidisciplinary areas such as security controls, risk assessment, system resilience, and the intersection of engineering and cybersecurity practices.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION 2016
EFFECTIVE November 2016	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY Very High

Source: https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

Why it matters

- **Strengthen systems engineering discipline** Integrate security and risk considerations into engineering methodologies to ensure robust, resilient systems from initial design through operation.
- **Improve stakeholder confidence** Demonstrate a measurable commitment to system trustworthiness, increasing assurance for customers, regulators, and business partners.
- **Enhance regulatory and compliance alignment** Facilitate adoption of best practices that streamline adherence to regulatory requirements and simplify compliance management.
- **Support operational resilience** Address risks throughout the lifecycle to minimize business disruption and improve system reliability during adverse conditions.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-160 Vol. 1

Security Requirements and Engineering Traceability

Capture security requirements and trace them across system architecture, components, and lifecycle phases.

Threat, Vulnerability, and Risk Linkage

Link threats, vulnerabilities, and risks to engineering decisions and system design controls.

Secure Development Lifecycle Governance

Manage security activities across design, development, integration, and deployment stages.

Contractual Security Requirement Tracking

Manage flow-down security clauses and obligations embedded in supplier contracts and agreements.

Supply Chain and System Integration Oversight

Monitor supplier components, system integrations, and external dependencies impacting security.

System Risk Posture and Engineering Assurance Reporting

Provide visibility into system risk posture, control coverage, and engineering assurance status.

Common framework mappings

CIS Controls v8.1 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

NIST SP 800-160 Volume 1

Defines systems security engineering practices for trustworthy secure systems.

csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

NIST SP 800-160 Volume 2

Provides assessment procedures for systems security engineering practices.

csrc.nist.gov/publications/detail/sp/800-160/vol-2/final

Frequently asked questions

What is NIST SP 800-160 used for?

NIST SP 800-160 provides detailed guidance for integrating systems security engineering practices into the lifecycle of complex systems. It is used to help organizations develop and implement trustworthy, secure systems by embedding security considerations into each phase of engineering. The framework aims to address security risks from the earliest design stages through operations and sustainment.

Is compliance with NIST SP 800-160 mandatory or certifiable?

NIST SP 800-160 is not a certifiable standard, nor is its use mandatory for all organizations. However, federal agencies and contractors may be required or strongly encouraged to align with its principles to meet regulatory and contractual security obligations.

Who should use NIST SP 800-160, and what systems does it apply to?

NIST SP 800-160 is intended for system engineers, architects, risk managers, and security professionals working with critical systems in both public and private sectors. Its guidance applies to any system where trustworthy, secure, and resilient operation is a priority, including IT, industrial, and cyber-physical systems.

What are the key artifacts or activities required by NIST SP 800-160?

Key artifacts include engineered security requirements, architecture documentation, risk assessments, control selection and integration, assurance cases, and verification and validation evidence. These are developed and maintained to demonstrate that security and resilience objectives are systematically addressed throughout the system lifecycle.

 © 2026 SmartSuite Inc. All rights reserved.

How is NIST SP 800-160 implemented within engineering processes?

Organizations implement NIST SP 800-160 by integrating its security engineering practices into each phase of their system development and acquisition workflows. This involves deriving security requirements from risk assessments, selecting appropriate controls, evaluating threats and vulnerabilities, validating designs, and documenting risk decisions.

How does NIST SP 800-160 relate to other NIST frameworks like SP 800-53 and RMF?

NIST SP 800-160 complements frameworks such as SP 800-53 and the Risk Management Framework (RMF) by providing engineering processes and activities for integrating and managing security controls throughout the system life cycle. It focuses on secure-by-design principles that support ongoing compliance with broader security and risk management requirements.

What are the ongoing compliance requirements for NIST SP 800-160?

Ongoing compliance with NIST SP 800-160 requires continual integration of security considerations into systems engineering processes, including monitoring risk, updating security architecture, and documenting changes throughout the system lifecycle. Regular reviews and updates to artifacts, risk assessments, and security requirements are critical to maintaining compliance.

How would SmartSuite support NIST SP 800-160?

SmartSuite can help organizations manage NIST SP 800-160 by enabling comprehensive risk tracking, organizing and mapping security controls to engineering processes, and collecting evidence of security activities and decisions. The platform supports audit readiness through documentation management and progress tracking, while facilitating reporting and oversight across multidisciplinary engineering and compliance teams.

Is NIST SP 800-160 a mandatory compliance requirement?

NIST SP 800-160 is not a mandatory requirement by itself, but it is often referenced in federal, defense, and critical infrastructure contexts. While certification to NIST SP 800-160 is not available, demonstrating alignment supports compliance with other mandatory frameworks, such as NIST RMF (Risk Management Framework).

Who should use NIST SP 800-160 and what is its scope?

NIST SP 800-160 applies to organizations engineering high-value, mission-critical, or complex systems—such as federal agencies, defense contractors, and critical infrastructure operators. Its multidisciplinary scope encompasses system requirements, architecture, design, implementation, and sustainment.

What are the key concepts and artifacts required by NIST SP 800-160?

Key concepts include requirements engineering, system security architecture, risk assessment, security controls, verification and validation, and ongoing governance. Artifacts may include risk registers, traceability matrices, security requirements specifications, security test results, and compliance evidence.

How does systems security engineering work in NIST SP 800-160?

NIST SP 800-160 recommends integrating security requirements and risk analysis into every phase of the system life cycle. Security controls are embedded during design and development, with continuous validation, verification, and change management to maintain security posture through operations and maintenance.

How does NIST SP 800-160 relate to other frameworks like NIST RMF or ISO 27001?

NIST SP 800-160 complements the NIST Risk Management Framework (RMF) by providing detailed engineering practices for building secure systems. It can be used alongside ISO 27001 by embedding its principles into larger enterprise security management programs and by demonstrating engineering rigor during audits.

License included / downloadable: Yes NIST SP 800-160 is published by the National Institute of Standards and Technology and is publicly available for free from NIST's publications website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-160-vol-1