SmartSuite

Framework / Risk Management / NIST Special Publications

NIST SP 800-39 (2011)

NIST SP 800-39 guides organizations to identify, assess, and manage information security risk at all enterprise levels.

What it is

NIST SP 800-39 is a risk management framework that helps organizations identify, assess, and manage information security risk across all levels of the enterprise. It establishes a structured approach for integrating risk management into organizational processes to support cybersecurity and compliance objectives.

Published by the National Institute of Standards and Technology (NIST), this framework is widely adopted by federal agencies, contractors, and organizations seeking robust approaches to information security risk management. NIST SP 800-39 provides guidance for addressing risk at the organizational, mission, and information system levels, covering areas such as risk assessment, security controls, incident response, and governance.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Regulation	VERSION Rev. 1
EFFECTIVE March 2011	DOMAIN Risk Management	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY High

Source: https://csrc.nist.gov/publications/detail/sp/800-39/final

Why it matters

- **Strengthen risk management governance** Establish a consistent enterprise-wide approach to prioritizing, assessing, and responding to security risks in alignment with business objectives.
- **Enhance incident response capabilities** Improve the ability to identify, assess, and effectively respond to security events, reducing the potential impact of cyber incidents.
- **Support regulatory compliance** Facilitate alignment with federal and industry standards for risk management, helping organizations meet statutory and contractual requirements.
- **Improve decision-making** Enable leadership to make informed resource allocation and risk treatment decisions based on comprehensive, organization-wide risk insights.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-39

Content Security Control Library

Organize MPA security requirements for production, post-production, storage, and distribution environments with assigned ownership.

Production and Asset Access Governance

Control and document user access to sensitive content, systems, and facilities involved in media production workflows.

Vendor and Production Partner Oversight

Track security requirements, assessments, and contractual obligations for vendors handling pre-release content.

Security Assessments and Compliance Tracking

Manage internal reviews and studio assessments validating adherence to MPA content protection practices.

Incident and Content Leakage Response

Coordinate investigation, escalation, and remediation of security incidents involving protected media assets.

Program Reporting and Studio Assurance

Provide dashboards showing compliance status, open issues, vendor risks, and overall content security readiness.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | FedRAMP Rev. 5 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

NIST SP 800-39: Managing Information Security Risk

Defines the management of information security risk in organizational processes.

csrc.nist.gov/publications/detail/sp/800-39/final

NIST Risk Management Framework (RMF)

Outlines the process for risk management in federal information systems.

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

NIST SP 800-53: Security and Privacy Controls

Provides controls to protect organizational operations and assets from cybersecurity risks.

csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST Cybersecurity Framework

Describes common policies to improve cybersecurity risk management.

nist.gov/cyberframework

Frequently asked questions

What is NIST SP 800-39 used for?

NIST SP 800-39 provides a structured approach to managing information security risk across an entire organization. It helps organizations identify, assess, and respond to security risks at the organizational, business process, and information system levels, supporting overall cybersecurity resilience.

Is NIST SP 800-39 mandatory or certifiable?

NIST SP 800-39 is not a certifiable standard, but it is mandatory for U.S. federal agencies as part of their information security programs. Organizations in regulated sectors or working with government agencies often adopt it voluntarily to align with federal risk management best practices and demonstrate due diligence.

Who should use NIST SP 800-39, and what is its scope?

NIST SP 800-39 applies to organizations seeking a comprehensive, enterprise-wide risk management strategy for information security. Its scope includes all organizational levels, from governance and mission/business processes to individual information systems, making it suitable for entities of various sizes and industries.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the key concepts in NIST SP 800-39?

Key concepts in NIST SP 800-39 include its three-tiered risk management model (organization, mission/business process, and information system), the risk management lifecycle (framing, assessing, responding, and monitoring risk), and governance processes for integrating risk management throughout the organization.

How do organizations implement NIST SP 800-39?

Organizations implement NIST SP 800-39 by establishing risk management policies, defining risk tolerance, performing risk assessments at each tier, and mapping identified risks to specific controls. Continuous monitoring, documented reporting, and coordinated governance ensure effective risk response and mitigation over time.

How does NIST SP 800-39 relate to other NIST frameworks?

NIST SP 800-39 serves as an overarching risk management framework that aligns with other NIST publications, such as NIST SP 800-53 for security controls and the NIST Risk Management Framework (RMF). It provides the structure for integrating these controls and standards into a unified risk management program.

What are the ongoing compliance requirements for NIST SP 800-39?

Ongoing compliance with NIST SP 800-39 requires regular risk assessments, updates to control implementation, incident response readiness, and continuous monitoring of risks and controls. Governance and documentation are essential to demonstrate compliance and adapt to evolving threats and organizational changes.

How would SmartSuite support NIST SP 800-39?

SmartSuite enables organizations to manage NIST SP 800-39 by centralizing risk assessment data, maintaining control libraries, and tracking risk mitigation actions. It supports collection of compliance evidence, facilitates audit readiness with dashboard reporting, automates monitoring workflows, and streamlines governance for executive oversight.

License included / downloadable: Yes NIST SP 800-39 is publicly available from NIST. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-39-managing-information-security-risk