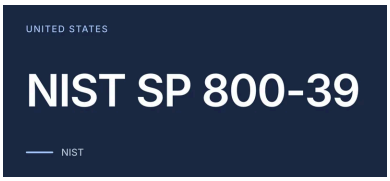
SmartSuite

Framework / Risk Management / NIST Special Publications

NIST SP 800-39 – Managing Information Security Risk: Organization, Mission, and Information System View

NIST SP 800-39 is the NIST guideline for an organization-wide information security risk program: frame, assess, respond and monitor across the organization, mission and system tiers.



What it is

NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, is the NIST guideline for an integrated, organization-wide program for managing information security risk, which Section 1.1 calls the flagship document in the series NIST developed in response to FISMA. It defines four components of risk management, framing, assessing, responding and monitoring (Section 2.1), applied across three tiers: the organization (Tier 1), mission/business processes (Tier 2) and information systems (Tier 3) (Section 2.2).

NIST published it on March 1, 2011 through the Joint Task Force Transformation Initiative, and it has not been revised since. Section 1.1 says it satisfies FISMA and meets or exceeds the OMB Circular A-130, Appendix III requirements for executive agencies, applies to all federal information systems other than national security systems, and is complementary to a broader enterprise risk management (ERM) program; state, local and tribal governments and private sector organizations are encouraged to consider using it. Its purpose is deliberately broad, with the detail of assessing, responding and monitoring left to supporting NIST publications.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Initial release (March 2011)
EFFECTIVE March 1, 2011	DOMAIN Risk Management	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY High

Source: csrc.nist.gov/pubs/sp/800/39/final

Why it matters

- **Risk framed before it is assessed** Section 2.1 and Task 1-1 to Task 1-4 make the organization state its risk assumptions, constraints, tolerance and priorities and trade-offs before any assessment is run.
- **A named owner for organization-wide risk** Section 2.3.2 establishes the risk executive (function) as the common risk management resource for senior leaders, mission owners, CIOs, CISOs, system owners and common control providers.
- **Three tiers that inform each other** Section 2.2 ties Tier 1 priorities to the Tier 2 enterprise architecture and the Tier 3 allocation of controls, with inter-tier and intra-tier communication and a feedback loop.
- **Five defined risk responses** Section 3.3 and Appendix H cover accepting, avoiding, mitigating, sharing and transferring risk, with the requirement that a decision to accept risk is consistent with the stated tolerance.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-39

Risk Frame Record (Tasks 1-1 to 1-4)

Record the organization's risk assumptions, constraints, risk tolerance and priorities and trade-offs as governed records that every assessment references.

Risk Management Strategy (Section 2.3.3)

Hold the Tier 1 strategy that states how the organization assesses, responds to and monitors risk, with the risk executive (function) as its owner.

Three-Tier Risk Register (Section 2.2)

Register organization, mission/business process and information system risks with links between tiers, so Tier 1 priorities trace to Tier 3 control decisions.

Risk Response Decisions (Tasks 3-1 to 3-4)

Capture alternative courses of action, the evaluation, the decision to accept, avoid, mitigate, share or transfer, and the implementation tasks with owners and dates.

Risk Monitoring Strategy (Tasks 4-1 and 4-2)

Define the purpose, type and frequency of monitoring and schedule the ongoing monitoring of systems and environments of operation.

Governance and Trust Records (Appendices F and G)

Document the governance model in use and the basis for trust relationships with other organizations and providers of common controls.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27005:2022 | 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 are the four components of risk management in NIST SP 800-39?

Section 2.1 defines them: frame risk (establish the context for risk-based decisions, producing the risk management strategy), assess risk, respond to risk once determined, and monitor risk on an ongoing basis. Chapter Three turns them into 14 tasks, Task 1-1 to Task 4-2, summarized in Appendix E.

What are the three tiers in NIST SP 800-39?

Section 2.2 describes Tier 1, the organization level, which implements risk framing and sets the context; Tier 2, the mission/business process level, where enterprise architecture and information security architecture are designed; and Tier 3, the information system level, where the Risk Management Framework of SP 800-37 is applied (Section 2.5). Activities at Tier 1 directly affect Tiers 2 and 3.

What is the risk executive (function)?

Section 2.3.2 defines it as a functional role established within the organization to provide an organization-wide approach to risk management. It is the common risk management resource for senior leaders, mission/business owners, chief information officers, chief information security officers, system owners, common control providers and architects, and it coordinates with senior leaders to establish risk management roles and responsibilities.

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

Which risk responses does NIST SP 800-39 recognize?

Five: accepting, avoiding, mitigating, sharing and transferring risk (Sections 2.1 and 3.3). Appendix H gives strategies for each and says an overall risk response strategy specifies who is responsible, the effectiveness criteria, dependencies, the implementation timeline, monitoring plans and triggers; a decision to accept risk must be consistent with the organization's stated risk tolerance.

Is NIST SP 800-39 mandatory, and has it been revised?

Section 1.1 says the publication satisfies FISMA and the OMB Circular A-130, Appendix III requirements for executive agencies and applies to all federal information systems other than national security systems; other organizations are encouraged to use it. NIST published it in March 2011 and the CSRC record lists no later revision, so the 2011 text is current.

License included / downloadable: Yes NIST SP 800-39 is a U.S. government publication available free of charge from NIST, and its tiers, components and tasks are included with the platform.

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