SmartSuite

Framework / Risk Management / NIST Special Publications

NIST SP 800-37 Rev. 2 – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

NIST SP 800-37 Rev. 2 is the NIST Risk Management Framework: seven steps from Prepare to Monitor, with the tasks, roles and authorization decisions federal agencies apply under OMB A-130.



What it is

NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, is the NIST guideline that describes the Risk Management Framework (RMF): seven steps (Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor) and the tasks within them for managing security and privacy risk across the life of a system (Section 2.2 and Chapter Three). OMB Circular A-130 requires federal agencies to implement the RMF described in this guideline and to integrate privacy into the RMF process (Section 1.1).

NIST published Revision 2 on December 20, 2018 through the Joint Task Force, superseding SP 800-37 Rev. 1 (updated June 5, 2014) and CSWP 3. Its scope is federal information systems, including systems operated by contractors or other organizations on behalf of an agency, and it is written to satisfy FISMA, the Privacy Act of 1974, OMB policies and the designated FIPS; state, local and tribal governments and private sector organizations are encouraged to use it (Section 1.2). Seven major objectives drove the update, including the new Prepare step, closer linkage between the C-suite and system-level activities, privacy integration and supply chain risk management.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION Revision 2 (December 2018)
EFFECTIVE December 20, 2018	DOMAIN Risk Management	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: csrc.nist.gov/pubs/sp/800/37/r2/final

Why it matters

- **One process for security and privacy** Section 2.3 and the A-130 text quoted in Section 1.1 require the two programs to collaborate; the plans, assessment reports and authorization package cover both.
- **Preparation before categorization** Tasks P-1 to P-18 set roles, the risk management strategy, organization-wide risk assessment, tailored baselines, common controls and the continuous monitoring strategy before any system is categorized.
- **A defined authorization package** Task R-1 names the package: security and privacy plans, assessment reports, the plan of action and milestones and an executive summary.
- **Ongoing rather than periodic authorization** Appendix F defines ongoing authorization as follow-on risk determinations made with continuous monitoring results, and Task M-6 makes it a Monitor-step task.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-37 Rev.2

System Register (Tasks P-8 to P-18)

Hold each system with its missions, stakeholders, assets, authorization boundary, information types and place in the enterprise architecture, and register it as Task P-18 requires.

Categorization and Control Selection (Tasks C-1 to S-3)

Record the FIPS 199 categorization and approval, the baseline chosen, tailoring decisions and the allocation of common, system-specific and hybrid controls.

Security and Privacy Plans (Tasks S-4 and I-2)

Document the planned and as-implemented state of every control in the plans the authorizing official approves at Task S-6.

Assessment and POA&M (Tasks A-1 to A-6)

Track the assessment plan, results, remediation and the plan of action and milestones with owners, milestones and closure evidence.

Authorization Package (Tasks R-1 to R-5)

Assemble the plans, assessment reports, POA&M and executive summary, record the authorization decision and its type per Appendix F, and report it.

Continuous Monitoring (Tasks M-1 to M-7)

Schedule ongoing assessments, update the package, report posture to the authorizing official, support ongoing authorization and record the disposal strategy.

Common framework mappings

CIS Controls v8.1 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | NIST CSF 2.0 | NIST SP 800-30 Rev. 1 | NIST 800-53 Rev.5

Official resources

NIST Special Publication 800-37 Revision 2

Defines the Risk Management Framework for selecting and implementing cybersecurity controls.

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

NIST Risk Management Framework Overview

Outlines the integration of security and privacy into the system development life cycle.

csrc.nist.gov/projects/risk-management

NIST RMF Quick Start Guide

Provides guidance on starting with the Risk Management Framework implementation.

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

NIST SP 800-53 Security Controls

Describes the security and privacy controls for federal information systems and organizations.

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

Frequently asked questions

What are the seven steps of the NIST SP 800-37 Rev. 2 Risk Management Framework?

Section 2.2 names a preparatory step and six main steps: Prepare, Categorize, Select, Implement, Assess, Authorize and Monitor. Chapter Three breaks them into tasks: P-1 to P-18, C-1 to C-3, S-1 to S-6, I-1 and I-2, A-1 to A-6, R-1 to R-5 and M-1 to M-7, each with inputs, outputs, responsibilities and an SDLC phase.

Who must implement the RMF, and under what authority?

Section 1.1 states that OMB Circular A-130 requires federal agencies to implement the RMF described in this guideline and to integrate privacy into the RMF process. Section 1.2 scopes it to federal information systems, including those operated by contractors on behalf of an agency, and encourages state, local and tribal governments and private sector organizations to use it.

What is in an RMF authorization package?

Task R-1 assembles the authorization package from the security and privacy plans, the security and privacy assessment reports, the plan of action and milestones and an executive summary. The authorizing official analyzes the risk (R-2), chooses a response (R-3), makes the decision (R-4) and reports it (R-5); Appendix F describes the decision types: authorization to operate, common control authorization, authorization to use and denial of authorization.

 © 2026 SmartSuite Inc. All rights reserved.

What did the Prepare step add in Revision 2?

The Executive Summary calls the Prepare step one of the key changes. Organization-level tasks P-1 to P-7 assign roles, set the risk management strategy, assess organization-wide risk, publish tailored baselines, identify common controls, prioritize systems and set a continuous monitoring strategy; system-level tasks P-8 to P-18 define the system, its boundary, information types and requirements before categorization.

What is ongoing authorization under the RMF?

Appendix F defines ongoing authorization as the subsequent risk determinations and risk acceptance decisions taken at agreed-upon and documented frequencies, or on events, using the results of continuous monitoring. Task M-6 makes it a Monitor-step task in which authorizing officials communicate changes in their risk determinations and acceptance decisions.

License included / downloadable: Yes NIST SP 800-37 Rev. 2 is a U.S. government publication available free of charge from NIST, and its seven steps and tasks are included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-37-rev-2-risk-management-framework-rmf

 © 2026 SmartSuite Inc. All rights reserved.