

NIST SP 800-37 Rev.2 – RMF

NIST RMF provides a structured process to select, implement, assess, authorize, and continuously monitor cybersecurity and privacy controls.



What it is

NIST SP 800-37 Revision 2, known as the Risk Management Framework (RMF), is a structured risk management approach that guides organizations in selecting, implementing, and continuously monitoring cybersecurity and privacy controls to manage system and organizational risks. The framework establishes a process for integrating security and privacy into the system development life cycle, supporting compliance and risk decision-making.

Published by the National Institute of Standards and Technology (NIST), the RMF is widely used by U.S. federal agencies, contractors, and organizations seeking to align with government cybersecurity requirements. It covers risk assessment, security control selection, implementation, assessment, authorization, and continuous monitoring to enhance the protection of information systems and data.

At a glance

<div>PUBLISHER</div> <div>National Institute of Standards and Technology (NIST)</div>	<div>TYPE</div> <div>Standard</div>	<div>VERSION</div> <div>NIST SP 800-37 Revision 2</div>
<div>EFFECTIVE</div> <div>December 2018</div>	<div>DOMAIN</div> <div>Risk Management</div>	<div>FAMILY</div> <div>NIST Special Publications</div>
<div>REGION</div> <div>United States</div>	<div>ADOPTION MODEL</div> <div>Risk Management</div>	<div>IMPLEMENTATION COMPLEXITY</div> <div>High</div>

Source: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>

Why it matters

- **Strengthen risk-based decision-making** Enable more consistent, informed risk management choices aligned with organizational priorities and operational requirements.
- **Enhance compliance support** Support adherence to government and industry regulations by establishing a defensible, repeatable approach to cybersecurity and privacy controls.
- **Promote continuous monitoring** Facilitate ongoing assessment and mitigation of evolving threats by embedding monitoring practices in daily operations.
- **Increase audit readiness** Document security activities and controls in a structured way that simplifies audits and demonstrates due diligence to stakeholders.

How SmartSuite supports NIST 800-37 Rev.2

RMF Step Library Run Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor as connected work.	System Boundary and Scope Management Define system scope, assets, and dependencies with clear traceability.	SSP and Control Implementation Statements Maintain SSP content and evidence tied directly to control requirements.
Assessments and POA&Ms Track findings, remediation actions, owners, retesting, and closure evidence.	Continuous Monitoring Cadence Schedule recurring monitoring tasks and maintain repeatable evidence over time.	Authorization and Governance Reporting Produce leadership-ready status reporting for ATO decisions and ongoing oversight.

Common framework mappings

CIS Controls v8.1

FedRAMP Rev. 5

ISO 27001:2022

ISO 27002:2022

ISO 27701

NIST CSF 2.0

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 is the NIST SP 800-37 Risk Management Framework (RMF) used for?

The NIST SP 800-37 RMF provides a structured methodology for organizations to manage risks to their information systems by selecting, implementing, and monitoring cybersecurity and privacy controls. It supports organizations in making informed risk decisions and helps align security practices with organizational objectives and regulatory requirements.

What is the scope of NIST SP 800-37 RMF in practice?

The RMF applies to all federal information systems, including those operated by contractors on behalf of agencies, and can be adapted by non-federal organizations. Its scope covers categorizing systems, selecting and implementing controls, assessing their effectiveness, authorizing systems for operation, and maintaining continuous oversight.

What are the key concepts and required artifacts of the RMF process?

Key concepts of the RMF include system categorization, control selection, implementation, assessment, authorization, and continuous monitoring. Required artifacts typically include system security plans, risk assessments, security assessment reports, plans of action and milestones (POA&Ms), and authorization packages.

How is the NIST SP 800-37 RMF implemented in organizations?

Organizations integrate the RMF into their system development lifecycle by classifying systems, conducting risk assessments, mapping applicable controls (often from NIST SP 800-53), and documenting implementation. Regular assessments are conducted to evaluate control effectiveness, with ongoing monitoring to ensure sustained compliance and risk mitigation.

How does NIST SP 800-37 RMF relate to other cybersecurity frameworks or regulations?

NIST SP 800-37 RMF aligns closely with frameworks such as NIST SP 800-53 (control catalog), FISMA (regulatory requirement), and FedRAMP (cloud authorization). It can also be mapped to broader governance programs and privacy regulations, supporting harmonization of security practices across multiple compliance obligations.

What are the ongoing compliance requirements under the RMF?

Ongoing RMF compliance requires continuous monitoring of controls, regular risk assessments, timely remediation of identified weaknesses, and maintenance of up-to-date security documentation. Organizations must provide evidence of ongoing oversight and take corrective actions to address new risks or changes in their threat landscape.

How would SmartSuite support NIST SP 800-37 RMF?

SmartSuite supports RMF management by centralizing risk tracking, facilitating control selection and implementation, and enabling streamlined evidence collection for compliance assessments. The platform provides automated compliance tracking, audit readiness workflows, and reporting dashboards to monitor risk posture and demonstrate ongoing adherence to RMF requirements.

License included / downloadable: Yes NIST SP 800-37 is published by the National Institute of Standards and Technology and is publicly available through official NIST publications.

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