

Federal Agency Guidance for Security Programs

NIST Risk Management Framework (RMF) Overview

Federal Information Security Modernization Act

The Federal Information Security *Management* Act (FISMA 2002) ***requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems*** that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), ***explicitly emphasizes a risk-based policy for cost-effective security.***

The Federal Information Security *Modernization* Act (FISMA 2014) amends FISMA 2002 to (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

What is FISMA?

NIST Special Publication (SP) 800-37

Risk Management Framework (RMF) for Information Systems & Organizations



HOLLISTIC & FLEXIBLE
7 STEP PROCESS
TO MANAGE RISK



ADDRESSES
**CYBERSECURITY
& PRIVACY**
RISK



APPLICABLE TO
ALL TYPES
OF SYSTEMS &
ORGANIZATIONS



SYSTEM & COMMON
CONTROL
AUTHORIZATIONS



DEVELOPED BY THE
**JOINT TASK
FORCE**



MANDATED BY
OMB A-130
FOR FEDERAL AGENCIES



PROVIDES LINKS TO
OTHER KEY
NIST PUBS

The RMF provides a ***structured, yet flexible process*** for managing ***cybersecurity and privacy risk*** that includes system categorization, control selection, implementation, assessment, authorization, and continuous monitoring.

Risk Management Framework Steps



Essential activities to **prepare** the organization to manage security and privacy risks

Categorize the system and information processed, stored, and transmitted based on an impact analysis

Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)

Implement the controls and document how controls are deployed

Assess to determine if the controls are in place, operating as intended, and producing the desired results

Senior official makes a risk-based decision to **authorize** the system (to operate)

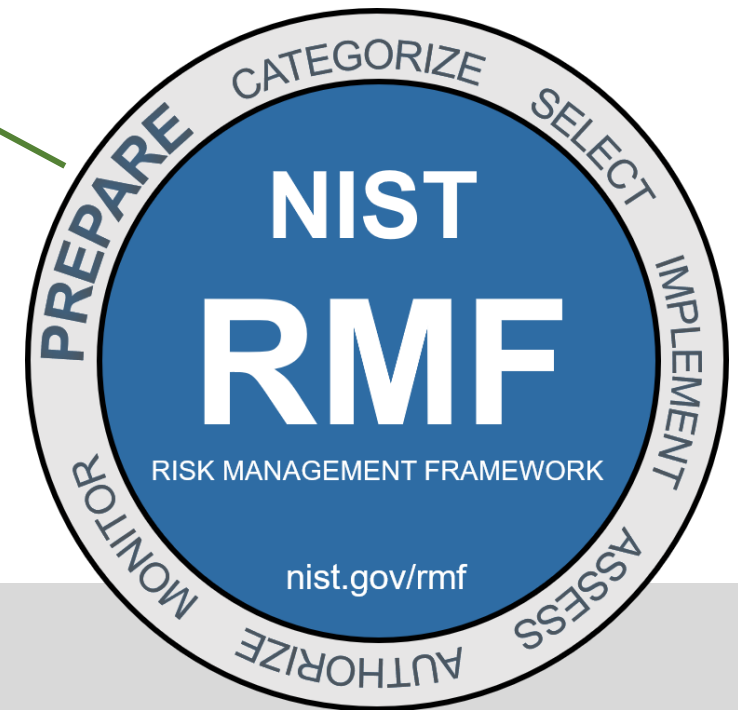
Continuously **monitor** control implementation and risks to the system

RMF Prepare Step

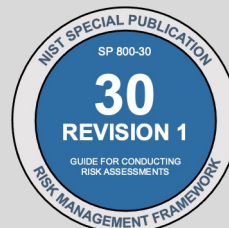
Purpose: carry out essential activities at all three risk management levels to help prepare the organization to manage its security and privacy risks using the RMF.

Organization-& Mission/Business Process Level Tasks

- P-1:** Risk Management Roles
- P-2:** Risk Management Strategy
- P-3:** Risk Assessment – Organization
- P-4:** Organizationally-tailored Control Baselines and Cybersecurity Framework Profiles (*optional*)
- P-5:** Common Control Identification
- P-6:** Impact Level Prioritization (*optional*)
- P-7:** Continuous Monitoring Strategy – Organization
- P-8:** Mission or Business Focus



Related:



RMF Prepare Step

System Level Tasks

P-9: System Stakeholders

P-10: Asset Identification

P-11: Authorization Boundary

P-12: Information Types

P-13: Information Life Cycle

P-14: Risk Assessment - System

P-15: Requirements Definition

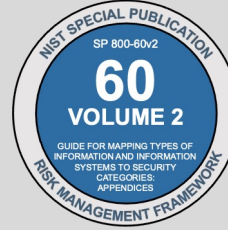
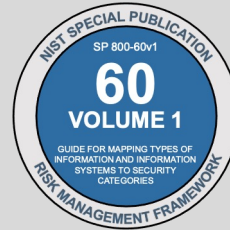
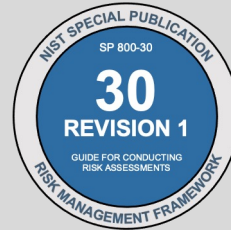
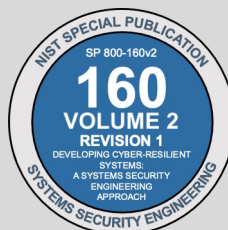
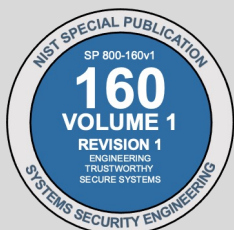
P-16: Enterprise Architecture

P-17: Requirements Allocation

P-18: System Registration



Related:



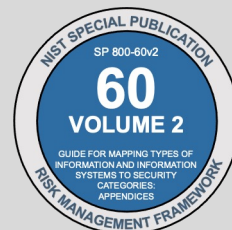
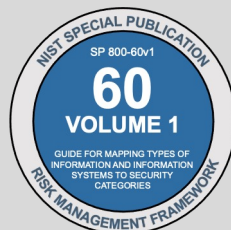
RMF Categorize Step

Purpose: inform organizational risk management processes and tasks by determining the adverse impact of the loss of confidentiality, integrity, and availability of organizational systems and information to the organization.

- C-1:** System Description
- C-2:** Security Categorization
- C-3:** Security Categorization Review and Approval

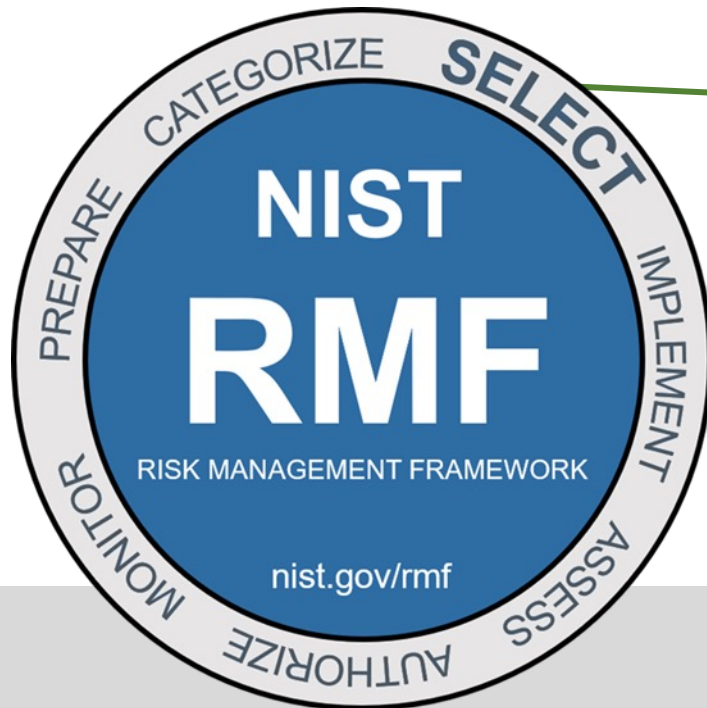


Related:



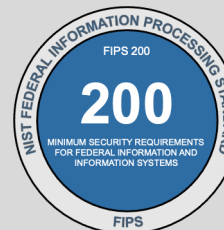
RMF Select Step

Purpose: select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, and the Nation.



- S-1:** Control Selection
- S-2:** Control Tailoring
- S-3:** Control Allocation
- S-4:** Documentation of Planned Control Implementations
- S-5:** Continuous Monitoring Strategy – System
- S-6:** Plan Review and Approval

Related:



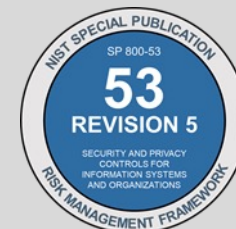
RMF Implement Step

Purpose: implement the controls as specified in security and privacy plans for the system and for the organization, and update the plans with the as-implemented details.



- I-1: Control Implementation
- I-2: Update Control Implementation Information

Related:



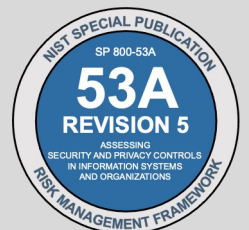
RMF Assess Step

Purpose: determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and organization.



- A-1:** Assessor Selection
- A-2:** Assessment Plan
- A-3:** Control Assessments
- A-4:** Assessment Report
- A-5:** Remediation Actions
- A-6:** Plan of Action and Milestones

Related:



RMF Authorize Step

Purpose: provide accountability by requiring a senior management official to determine if the security and privacy risk to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.



- R-1:** Authorization Package
- R-2:** Risk Analysis and Determination
- R-3:** Risk Response
- R-4:** Authorization Decision
- R-5:** Authorization Reporting

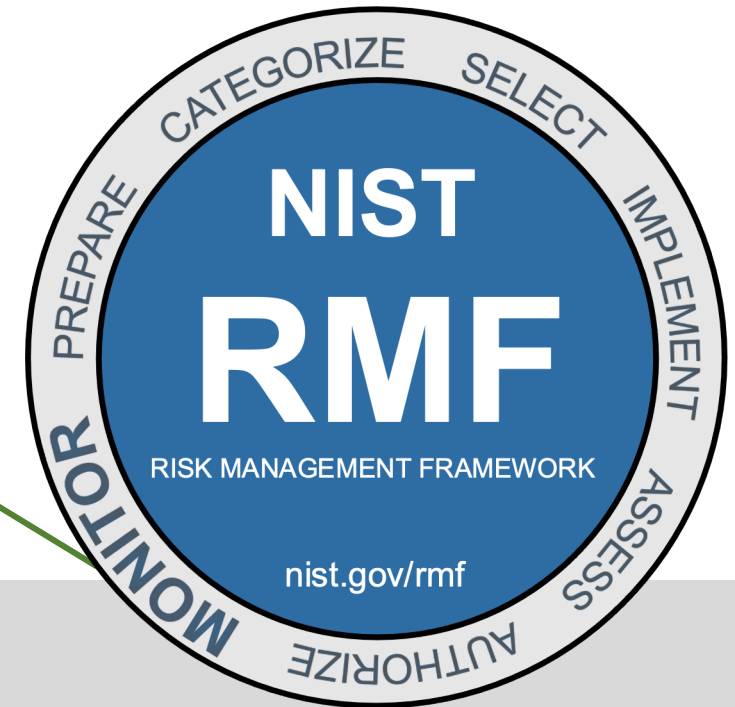
Related:



RMF Monitor Step

Purpose: maintain an ongoing situational awareness about the security and privacy posture of the system and the organization in support of risk management decisions.

- M-1:** System and Environment Changes
- M-2:** Ongoing Assessments
- M-3:** Ongoing Risk Response
- M-4:** Authorization Package Updates
- M-5:** Security and Privacy Reporting
- M-6:** Ongoing Authorization
- M-7:** System Disposal



Related:



Request ISPAB Feedback on:

- ideas and suggestions on NIST can stay updated and synced on other policy activities
- opportunities to improve the RMF and supporting suite of publications
- how can NIST better communicate and explain the RMF to both technical and non-technical audiences

Future Revisions of NIST SP 800-53

The screenshot shows the NIST CSRC website interface. At the top, there is a navigation bar with the NIST logo, 'Information Technology Laboratory', 'COMPUTER SECURITY RESOURCE CENTER', and 'CSRC'. Below this, there are tabs for 'PROJECTS', 'NIST RISK MANAGEMENT FRAMEWORK', and 'SP 800-53 CONTROLS'. The main content area is titled 'NIST Risk Management Framework RMF' and 'SP 800-53 Public Comments: Submit and View'. There are four navigation buttons: 'Public Comment Home', 'More Information', 'User's Guide', and 'FAQ'. A table lists four options: 'New' (Suggest a new SP 800-53 control or control enhancement), 'Edit' (Suggest a change to an existing SP 800-53 control or control enhancement), 'Candidates' (View proposed changes to the SP 800-53 controls), and 'Awaiting' (View proposed changes awaiting release). Below the table, there is a search bar for 'Tracking Number' with a 'Find' button. A QR code is located in the bottom left corner of the screenshot.



SP 800-53 controls, baselines, and assessment procedures* as a **machine-readable & web-based data set**



Suggest new controls, improve existing controls **anytime**.

Comment on draft controls and see feedback from others.



Receive real-time status updates on your comments!



Preview planned changes in next revision.

STAY IN TOUCH

CONTACT US



nist.gov/RMF



sec-cert@nist.gov



[@NISTcyber](https://twitter.com/NISTcyber)