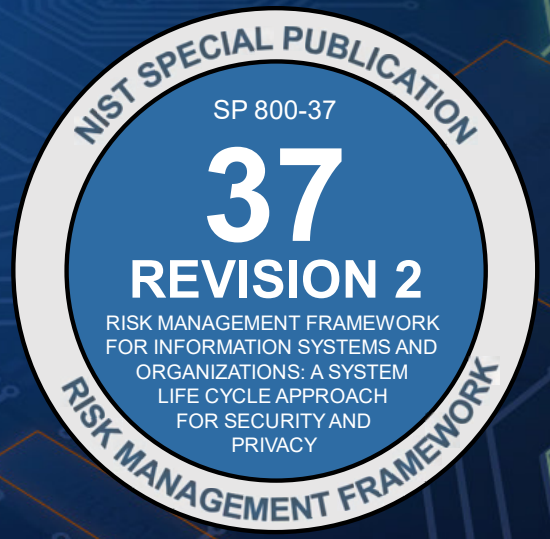
NIST Risk Management Framework

a brief primer based on NIST Special Publication 800-37



Briefing for:
Cybersecurity & Information Systems Information Analysis Center (CSIAC)
July 12, 2023 (Virtual)

Presented by:
Jeremy Licata (NIST)
NIST Risk Management Framework (RMF) Team
Computer Security Division (CSD)

NIST INFORMATION TECHNOLOGY LABORATORY

Agenda

What is the Risk Management Framework?

Who is using the RMF and why?

What happens in each step of the RMF?

What's the RMF?

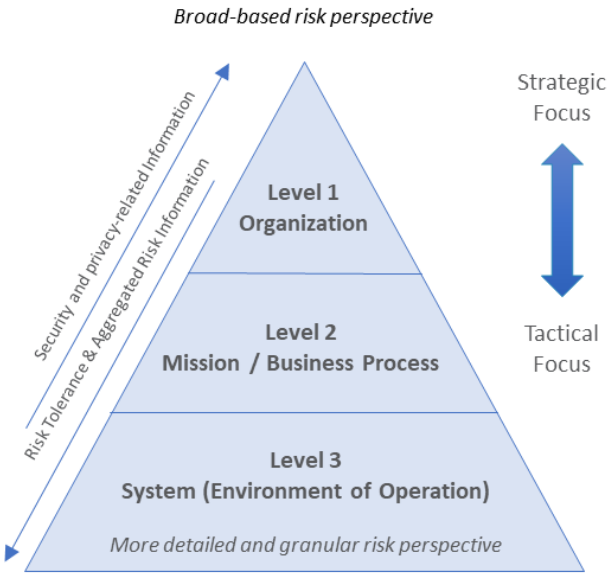
The RMF provides a ***structured, yet flexible process,*** for managing ***cybersecurity and privacy risk:***

- Multi-step, outcome-focused methodology;
- Created to help federal agencies meet **Federal Information Security Modernization Act (FISMA)** requirements for managing security and privacy risks;
- Required for federal agencies (can be adopted by non-federal entities including domestic and international organizations on a voluntary basis) → Not a compliance checklist;
- Integrates information security and risk management activities into the **system development life cycle**.

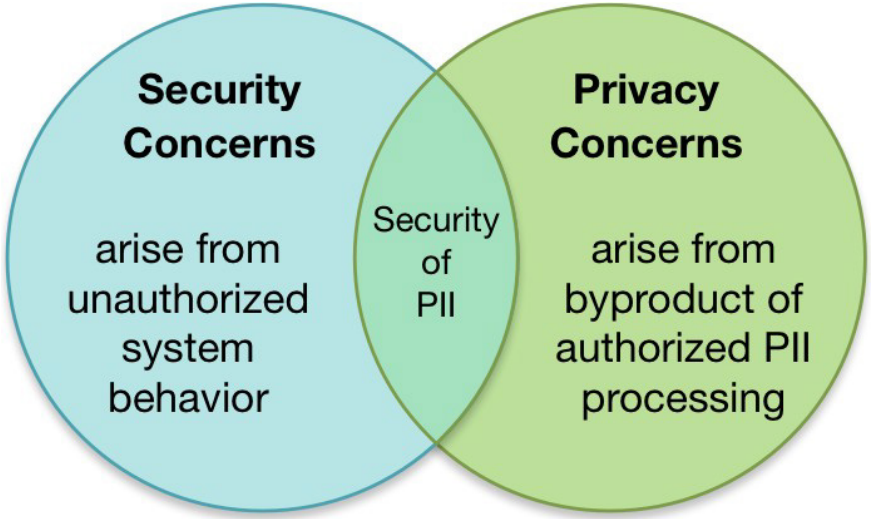
Using the RMF

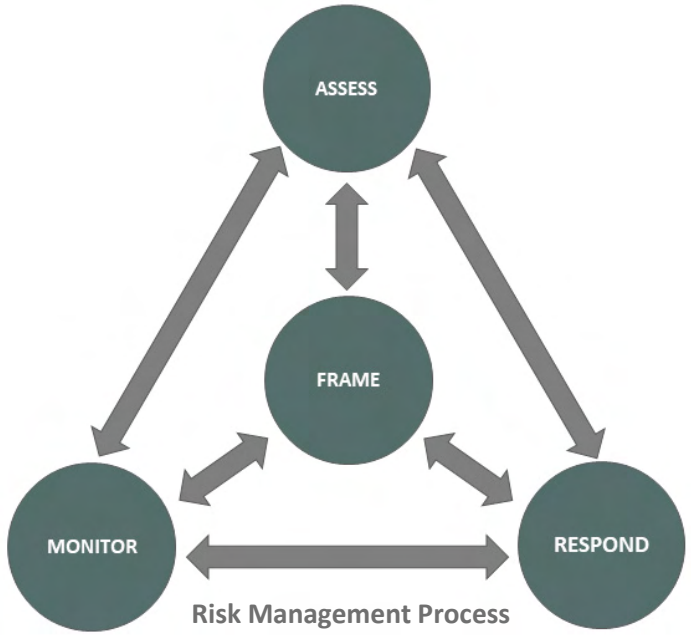
Framework enables risk management processes for any organization

Supports efforts to frame cybersecurity and privacy risks within the organization, at the mission/business level, and at the operational system level to provide consistent outcomes



Three Levels of Organization-Wide Risk Management





Risk Management Process

RMF Steps

ORGANIZATIONAL AND SYSTEM PREPARATION (TO EXECUTE THE RMF)
Essential activities to **prepare** the organization to manage security and privacy risks

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

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

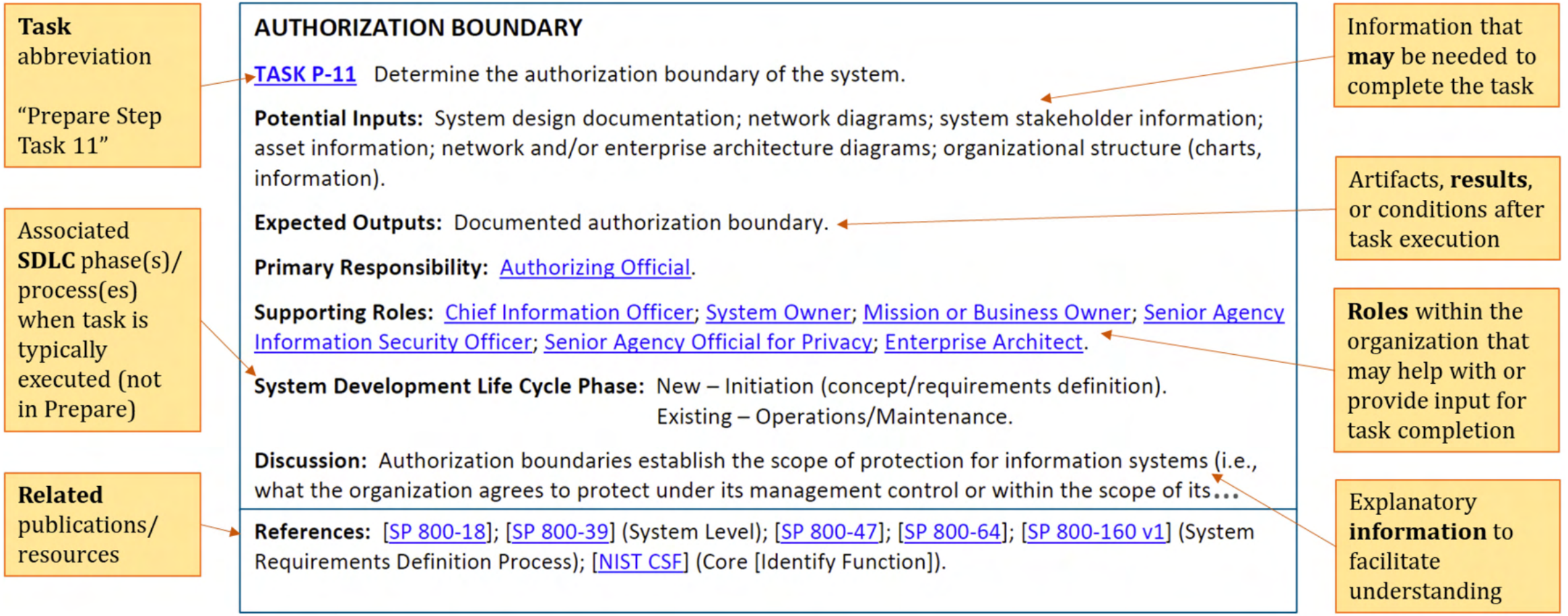
CONTROL IMPLEMENTATION
Implement the controls and document how controls are deployed

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

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

SYSTEM/CONTROL MONITORING
Continuously **monitor** control implementation and risks to the system

Task Structure



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

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

RMF Categorize Step

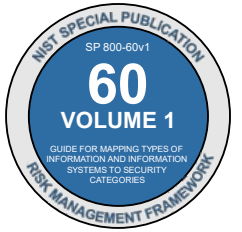
Purpose

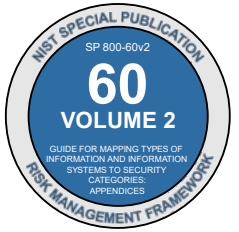
inform organizational risk management processes and tasks by determining the adverse impact of the loss of confidentiality, integrity, and availability of organizational systems and information to the organization.

C-1: System Description

C-2: Security Categorization

C-3: Security Categorization Review and Approval





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

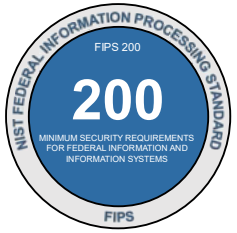
S-2: Control Tailoring

S-3: Control Allocation

S-4: Documentation of Planned Control Implementations

S-5: Continuous Monitoring Strategy – System

S-6: Plan Review and Approval



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

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

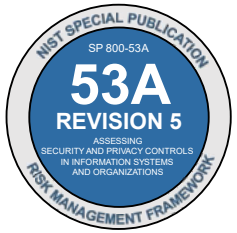
A-2: Assessment Plan

A-3: Control Assessments

A-4: Assessment Report

A-5: Remediation Actions

A-6: Plan of Action and Milestones



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

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

Resources

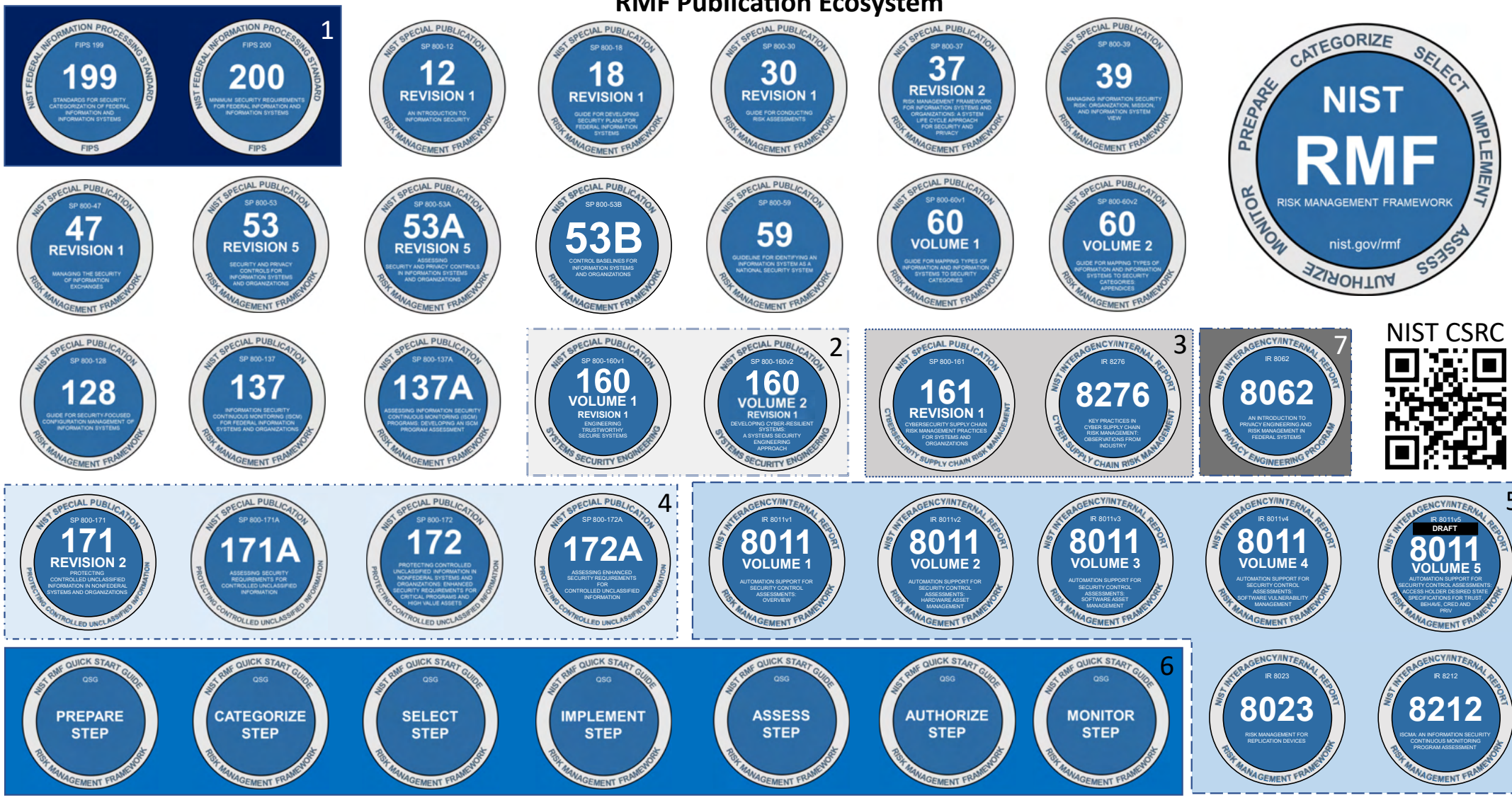
- Refer to **SP 800-37** and related publications for complete guidance.
- **RMF for Systems and Organizations Introductory Course** https://csrc.nist.gov/Projects/risk-management/rmf-course
- **NIST RMF Quick Start Guides** https://csrc.nist.gov/Projects/risk-management/about-rmf

- For DoD RMF implementation information/resources, refer to the: **DoD CIO RMF Knowledge Service Portal** at: https://rmfks.osd.mil/rmf (questions: osd.rmftag-secretariat@mail.mil)

References

1-(All federal agencies) 2-Systems Security Engineering 3-Cyber Supply Chain Risk Management 4-Protecting Controlled Unclassified Information 5-RMF NISTIRs 6-RMF Quick Start Guides 7-Privacy Engineering Program

RMF Publication Ecosystem



Q&A and Open Discussion

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

nist.gov/rmf sec-cert@nist.gov nist.gov/cyber