

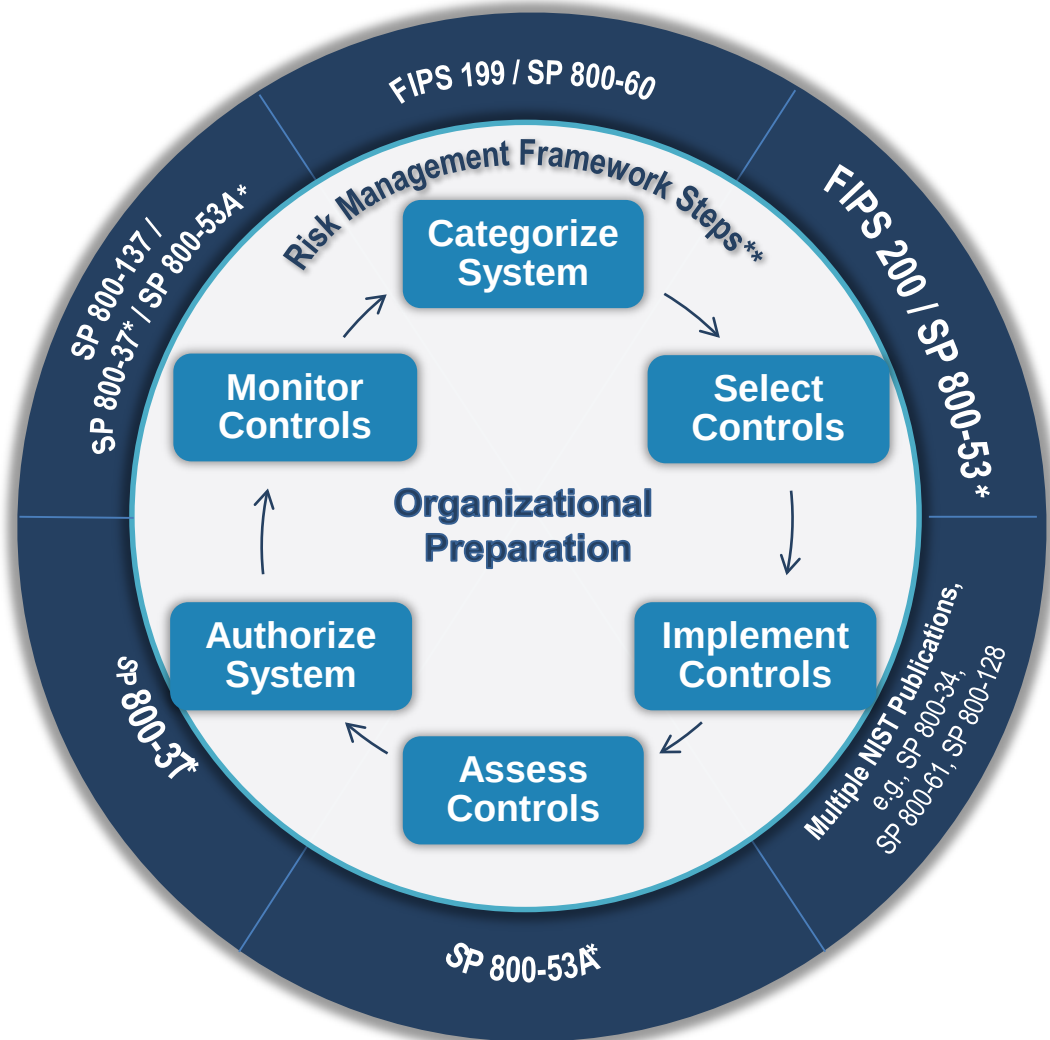
NIST Risk Management Framework Overview

NIST Risk Management Framework Overview

- About the NIST Risk Management Framework (RMF)
- Supporting Publications
- The RMF Steps
 - Step 1: Categorize
 - Step 2: Select
 - Step 3: Implement
 - Step 4: Assess
 - Step 5: Authorize
 - Step 6: Monitor
- Additional Resources and Contact Information

NIST Special Publication 800-37, Guide for Applying the Risk Management Framework

- A holistic and comprehensive risk management process
- Integrates the Risk Management Framework (RMF) into the system development lifecycle (SDLC)
- Provides processes (tasks) for each of the six steps in the RMF at the system level



Supporting Publications

Federal Information Processing Standards (FIPS)

- FIPS 199 – Standards for Security Categorization
- FIPS 200 – Minimum Security Requirements

Special Publications (SPs)

- SP 800-18 – Guide for System Security Plan Development
- SP 800-30 – Guide for Conducting Risk Assessments
- SP 800-34 – Guide for Contingency Plan development
- SP 800-37 – Guide for Applying the Risk Management Framework
- SP 800-39 – Managing Information Security Risk
- SP 800-53/53A – Security Controls Catalog and Assessment Procedures
- SP 800-60 – Mapping Information Types to Security Categories
- SP 800-128 – Security-focused Configuration Management
- SP 800-137 – Information Security Continuous Monitoring
- Many others for operational and technical implementations

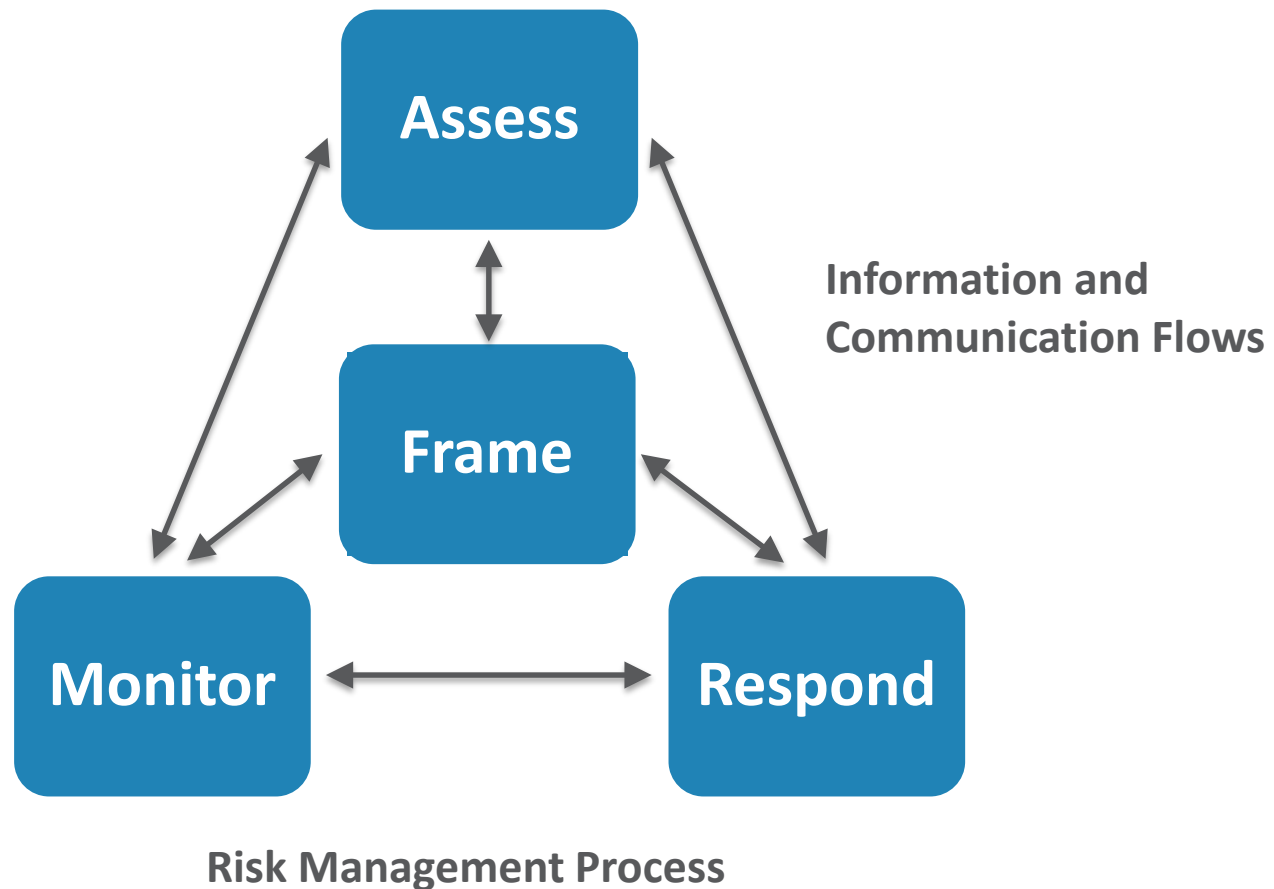


NIST SP 800-39: Managing Information Security Risk – Organization, Mission, and Information System View

- Multi-level risk management approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Supports all steps in the RMF



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

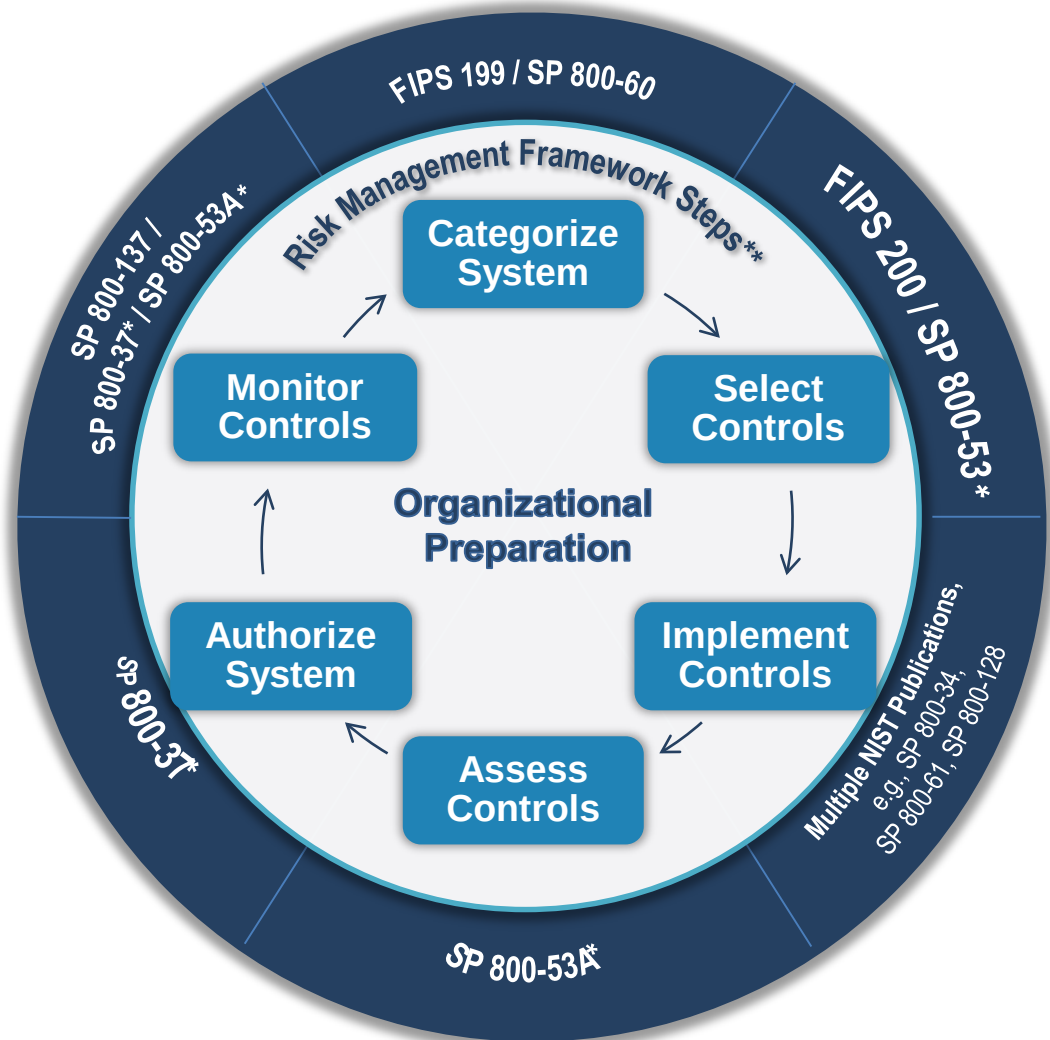


NIST Special Publication 800-30, Guide to Conducting Risk Assessments

- Addresses the Assessing Risk component of Risk Management (from SP 800-39)
- Provides guidance on applying risk assessment concepts to:
 - All three tiers in the risk management hierarchy
 - Each step in the Risk Management Framework
- Supports all steps of the RMF
- A 3-step Process
 - Step 1: Prepare for assessment
 - Step 2: Conduct the assessment
 - Step 3: Maintain the assessment

NIST Special Publication 800-37, Guide for Applying the Risk Management Framework

- A holistic and comprehensive risk management process
- Integrates the Risk Management Framework (RMF) into the system development lifecycle (SDLC)
- Provides processes (tasks) for each of the six steps in the RMF at the system level



NIST RMF Step 1: Categorize

Purpose: Determine the **criticality** of the **information and system** according to potential worst-case, adverse **impact** to the organization, mission/business functions, and the system.



Federal Information Processing Standard (FIPS) 199

Standards for Security Categorization of Federal Information and Information Systems



Security Objectives

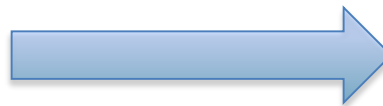
Confidentiality



Integrity



Availability



Impact Level

Low: loss has limited adverse impact

Moderate: loss has serious adverse impact

High: loss has catastrophic adverse impact

NIST RMF Step 2: Select

Purpose:

- **Select** security controls starting with the appropriate baseline **using categorization output** from Step 1
- Apply **tailoring guidance** as needed based on **risk assessment**



Federal Information Processing Standard (FIPS) 200

Minimum Security Requirements for Federal Information and Information Systems



- Defines **17 security-related areas** (families) that:
 - Represent a broad-based, balanced security program
 - Include management, operational, and technical security controls (all are needed for defense in depth)
- Specifies that a **minimum baseline of security controls**, as defined in NIST SP 800-53, will be implemented
- Specifies that the **baselines are to be appropriately tailored**

NIST Special Publication 800-53

Security and Privacy Controls for Information Systems and Organizations

- A **catalog** of security controls
- Defines **three security baselines** (L, M, H)
- Initial version published in 2005
- Currently using Rev. 4 (2013)
- ***Undergoing update*** to Rev. 5, draft released in Aug 2017 for public comment



Security and Privacy Controls

- A countermeasure prescribed for system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined requirements.
- Security and privacy controls are intentionally not focused on any specific technologies
- Control implementations and assessment methods **may vary** based on the technology to which the control is being applied, e.g.:
 - Cloud-based systems
 - Mobile systems
 - Applications



SP 800-53 Control Families

AC – Access Control

AT – Awareness and Training

AU – Audit and Accountability

CA – Security Assessment and Authorization

CM – Configuration Management

CP – Contingency Planning

IA – Identification and Authentication

IP* – Individual Participation

IR – Incident Response

MA - Maintenance

MP – Media Protection

PA* – Privacy Authorization

PE – Physical and Environmental Protection

PL – Planning

PM – Program Management

PS – Personnel Security

RA – Risk Assessment

SA – System and Service Acquisition

SC – System and Communication Protection

SI – System and Information Integrity



SP 800-53 Control Baselines

- Baselines are defined in Appendix D
- Determined by:
 - Information and system categorization (L, M, H)
 - Organizational risk assessment and risk tolerance
 - System level risk assessment



- Baselines **can and should be tailored, based on RISK, to fit the mission and system environment**
- Some controls are not included in baselines

NIST RMF Step 3: Implement



Purpose: **Implement** security controls within enterprise architecture and systems using sound system security engineering practices (see SP 800-160); **apply security configuration settings.**

Implementation Tips

- Plan for control implementation during the development phase of the SDLC – **BAKE IT IN**
- Many NIST publications are available to provide implementation guidance on a wide range of controls and control types (<https://csrc.nist.gov>)

- Implementation may include:
 - Writing and following policies, plans, and operational procedures
 - Configuring settings in operating systems and applications
 - Installing tools/software to automate control implementation
- Training



NIST RMF Step 4: Assess



Purpose: Determine **security control effectiveness** – are controls **implemented correctly, operating as intended, and meeting the security requirements** for the system and environment of operation?

NIST Special Publication 800-53A

Assessing Security and Privacy Controls in Systems and Organizations: Building Effective Security Assessment Plans



- Supports RMF Step 4 (Assess)
- Is a companion document to 800-53
- Is updated shortly after 800-53 is updated
- Describes high level procedures for assessing security controls for effectiveness
- Defines assessment procedures using
 - Assessment Objectives
 - Assessment Methods
 - Assessment Objects

SP 800-53A Assessment Steps

1. Develop the Security Assessment Plan
 - a. Determine which controls are to be assessed
 - b. Select appropriate procedures to assess those controls
 - c. Determine depth and coverage needed for assurance
 - d. Tailor the assessment procedures
 - e. Finalize the plan and obtain approval
2. Conduct the assessment
3. Analyze the results
4. Create the Security Assessment Report



SP 800-53A Assessment Procedures

“Parts”

- Assessment **objectives** – determination statements
- Three assessment **methods** and associated assessment **objects**
 - **Interview** – objects are individuals/groups of individuals
 - **Examine** – objects include:
 - Specifications (e.g., documents - policies, procedures, designs)
 - Mechanisms (e.g., functionality in HW, SW, firmware)
 - Activities (e.g., system ops, administration, mgmt., exercises)
 - **Test** – objects include:
 - Mechanisms (e.g., HW, SW, firmware)
 - Activities (e.g., system ops, administration, mgmt., exercises)



NIST RMF Step 5: Authorize

Purpose:

- The Authorizing Official (AO) **examines the output** of the security controls assessment to **determine whether or not the risk is acceptable**
- The AO may consult with the Risk Executive (Function), the Chief Information Officer, the Chief Information Security Officer, as needed since aggregate risk should be considered for the authorization decision
- After the initial authorization, ongoing authorization is put in place using output from continuous monitoring (see Supplemental Guidance on Ongoing Authorization at: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/nist_oa_guidance.pdf)



NIST RMF Step 6: Monitor

Purpose:

- **Continuously monitor** controls implemented for the system and its environment of operation for changes, signs of attack, etc. that may affect controls, and reassess control effectiveness
- **Incorporate all monitoring** (800-39 risk monitoring, 800-128 configuration management monitoring, 800-137 control effectiveness monitoring, etc.) into **an integrated organization-wide monitoring program**



Examples of Applications



Committee on
National Security Systems

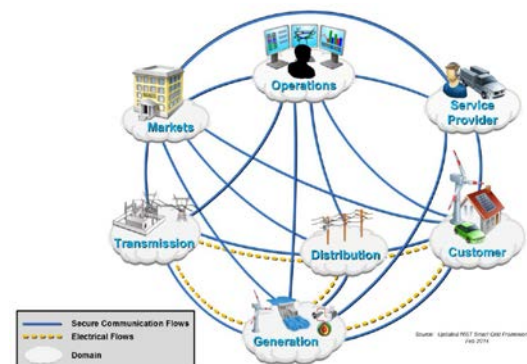
Overlays for specific **national security systems/operational environments**, such as: space platform, privacy, classified information, etc.



FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to **security assessment, authorization, and continuous monitoring** for **cloud** products and services.

NIST Interagency Report 7628, Rev. 1,
Guidelines for Smart Grid Cybersecurity



Additional Resources and Contact Information



FISMA Publications: sec-cert@nist.gov



<https://csrc.nist.gov/Projects/Risk-Management>



@usaNISTgov
@NISTcyber

THANK YOU!