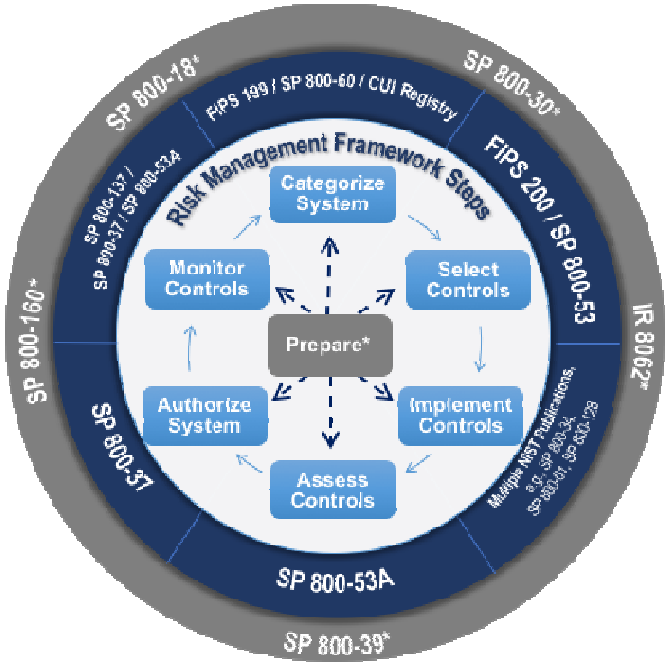
Security and Privacy: A Life Cycle Approach

6.7.2019

National Institute of Standards and Technology
U.S. Department of Commerce

The NIST Risk Management Framework

NIST Special Publication 800-37, Rev. 2, *Risk Management Framework for Information Systems & Organizations: A System Life Cycle Approach for Security & Privacy*



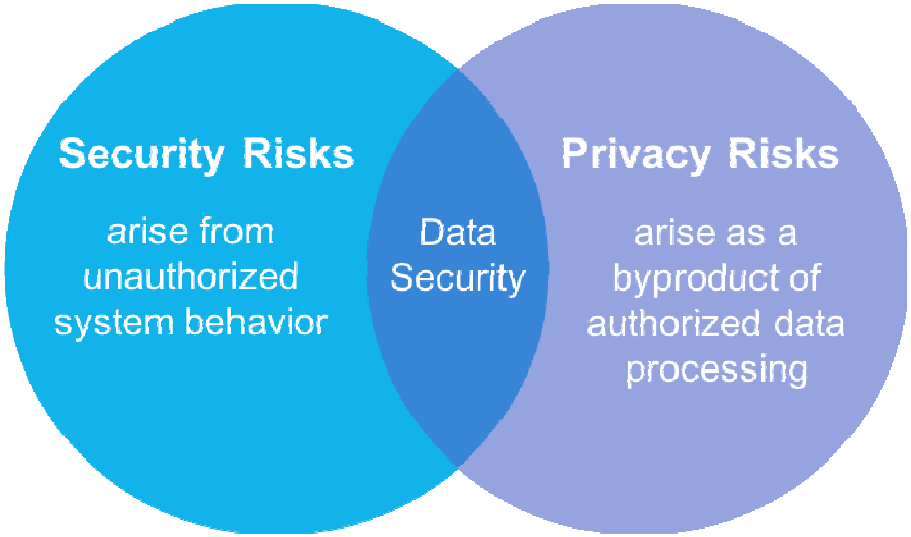
Update Purpose: **Expand** on the holistic risk management process for systems & organizations

- Provide closer links and **improve communication** between C-Suite/Governance-level to system/operational-level
- Integrates **privacy**, **supply chain**, and **security engineering** into the Risk Management Framework (RMF)
- Aligns the **Cybersecurity Framework (CSF)** to the RMF
- Demonstrates how RMF is implemented in the **system development life cycle (SDLC)**

Privacy Integration into RMF

- In accordance with OMB Circular A-130
- Privacy and RMF addressed in section 2.3
- Privacy called out in task text as appropriate (e.g., Task P-3 is to assess security *and privacy* risk)
- Privacy-specific inputs, outputs, roles, and references specified as appropriate in tasks
- Privacy-specific detail in task discussions

Security & Privacy Risk* Relationship



- There is a clear recognition that security of data plays an important role in the protection of privacy
- Individual privacy cannot be achieved solely by securing data
- Authorized processing: system operations that handle data (collection – disposal) to enable the system to achieve mission/business objectives

*For more information about the privacy risk model, see NIST Interagency Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*

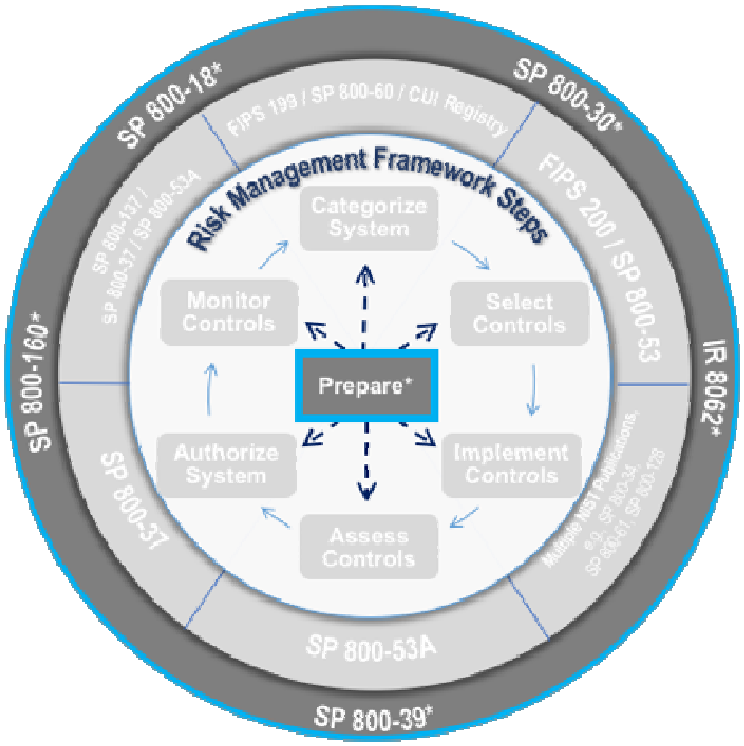
Use Case: Smart TVs

Brady Company, a *fictional* management consulting company, wants to renovate it's conference rooms and offices to include "smart technology" such as smart TVs.

Step 1: Prepare

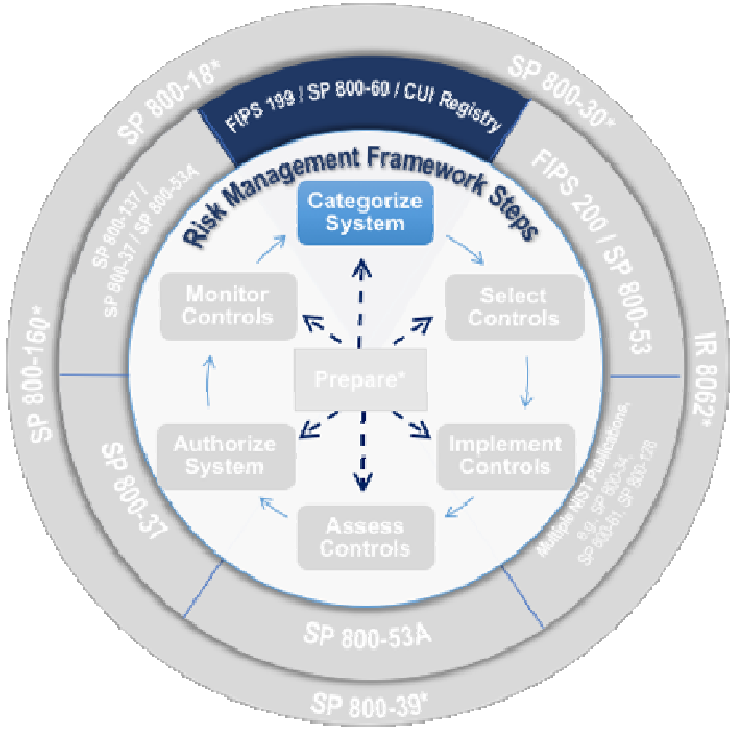
Organization & Mission/Business Process Level: The organization develops a risk management strategy

System-Level: Determine the authorization boundary, conduct a system-level risk assessment, and define security and privacy requirements of the system



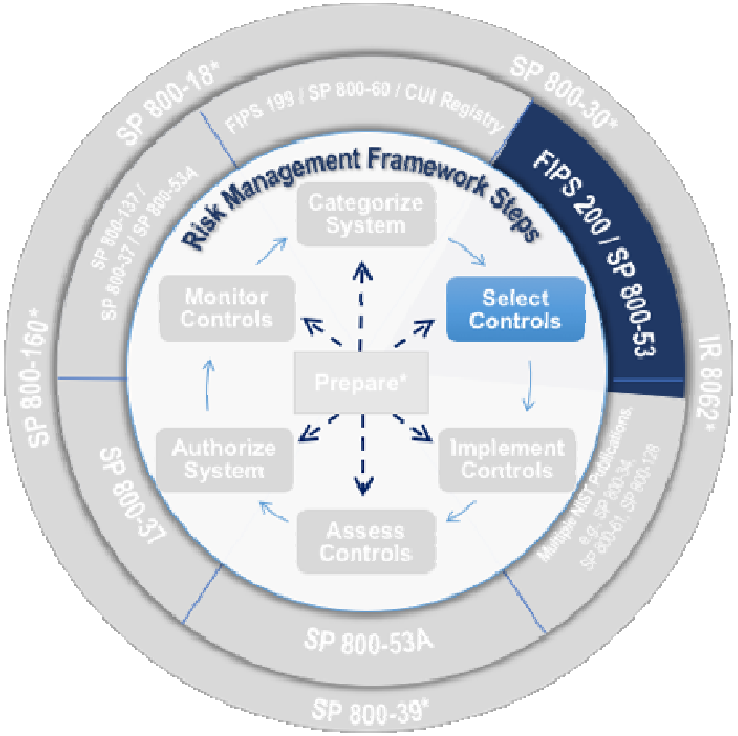
Step 2: Categorize

Categorize the system based on security impact



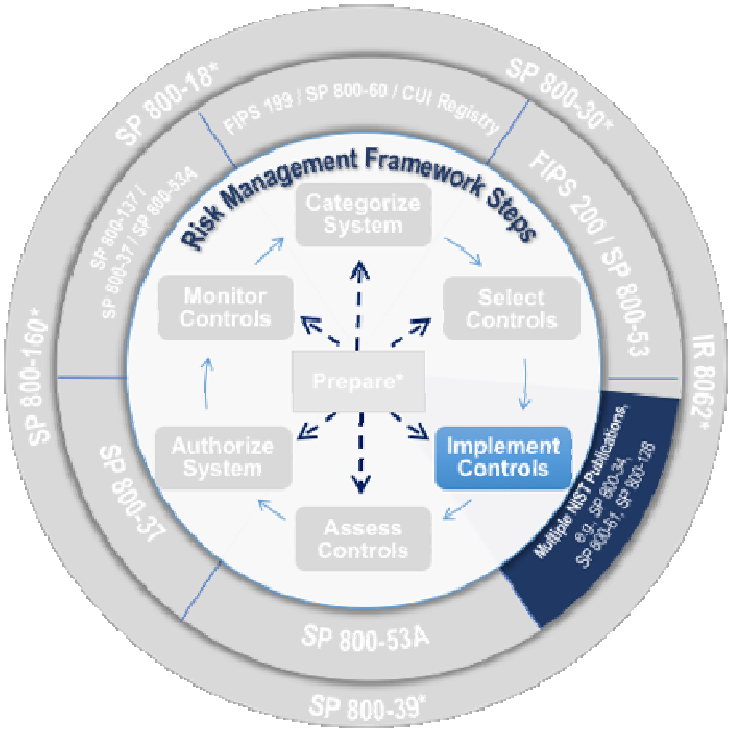
Step 3: Select

Select, tailor and allocate controls



Step 4: Implement

Implement what you planned in **Select**

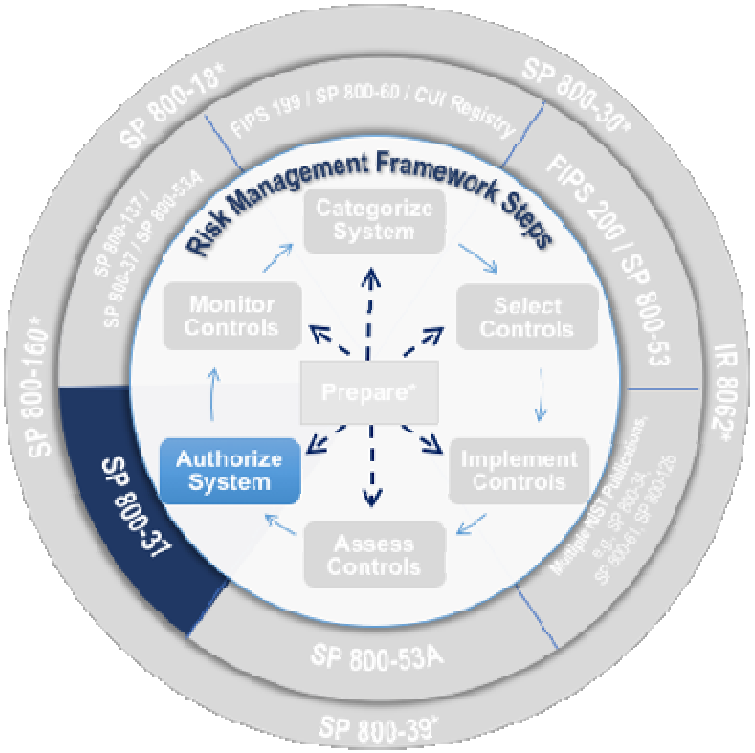


Step 5: Assess

Select assessor, develop assessment plan, conduct assessment, develop report and conduct initial remediation actions, and develop POA&M

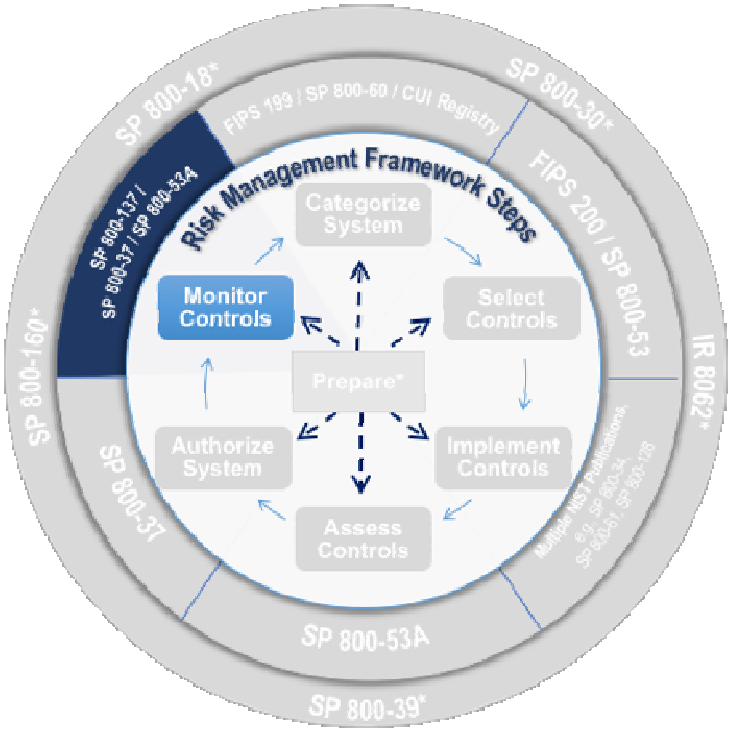
Step 6: Authorize

Senior management official determines if security and privacy risk is acceptable



Step 7: Monitor

Maintain ongoing situational awareness about the security and privacy posture of the system and organization



Learn More & Contact

NIST Privacy Engineering Program:
https://nist.gov/Privacy-Engineering

NIST Risk Management Program:
https://csrc.nist.gov/Projects/Risk-Management

Privacy Team: privacyeng@nist.gov

RMF Team: sec-cert@nist.gov

Resource List

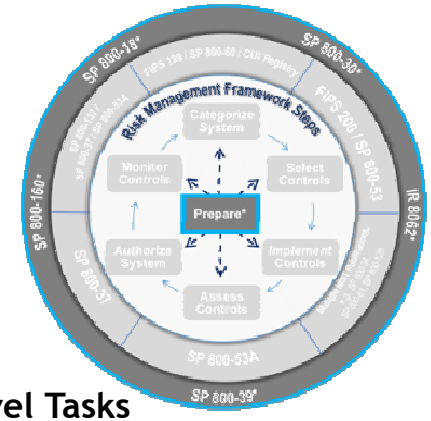
I. NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

II. NIST Risk Management Framework Webcast: A Flexible Methodology to Manage Information Security and Privacy Risk
go.usa.gov/xENcs

SUPPLEMENTAL MATERIALS

National Institute of Standards and Technology
U.S. Department of Commerce

RMF Step: Prepare



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 CSF 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

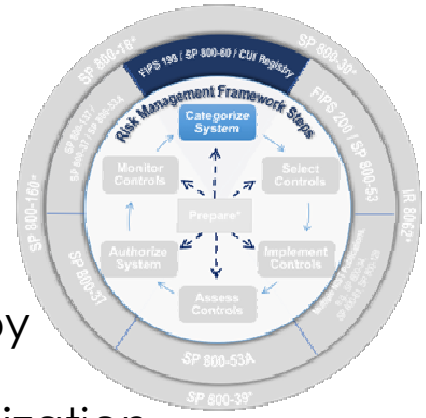
P-15: Requirements Definition

P-16: Enterprise Architecture

P-17: Requirements Allocation

P-18: System Registration

RMF Step: Categorize



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 Step: Select

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

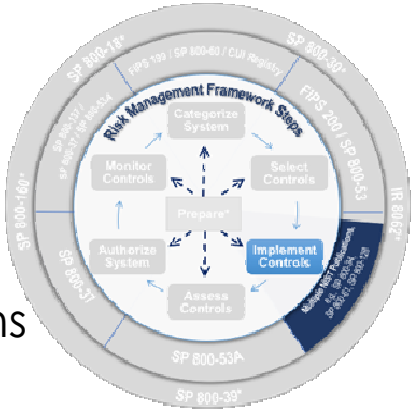
S-3: Control Allocation

S-4: Documentation of Planned Control Implementations

S-5: Continuous Monitoring Strategy – System

S-6: Plan Review and Approval

RMF Step: Implement



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 Step: Assess

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

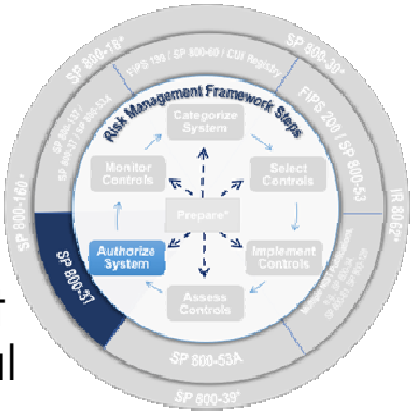
A-3: Control Assessments

A-4: Assessment Reports

A-5: Remediation Actions

A-6: Plan of Action and Milestones

RMF Step: Authorize



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 of operating a system or the use of common controls, is acceptable.

R-1: Authorization Package

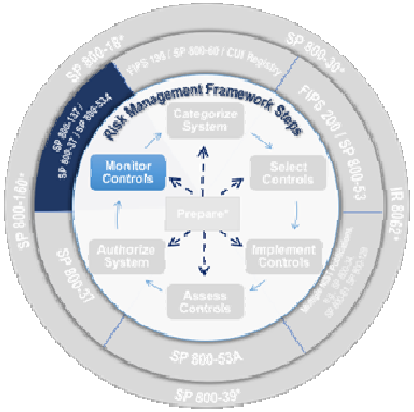
R-2: Risk Analysis and Determination

R-3: Risk Response

R-4: Authorization Decision

R-5: Authorization Reporting

RMF Step: Monitor



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