NIST Risk Management Framework Webcast Information

Questions and Comments

sec-cert@nist.gov

@usNISTgov
#NISTRMF

Please direct any ***technical issues*** (webcast sound, video, etc.) to:
webcast@nist.gov

Resources

https://go.usa.gov/xENcs

- Slides available for download
- Webcast recording will be available by **March 14, 2019**

Project website:
https://csrc.nist.gov/Projects/Risk-Management

NIST Risk Management Framework Webcast

A Flexible Methodology to Manage Information Security and Privacy Risk

February 28, 2019
1:00 PM – 3:00 PM Eastern

NIST RMF Webcast: Agenda

1:00 PM	Welcome and Introduction	Ron Ross
1:15 PM	Risk Management Framework, (NIST SP 800-37, Revision 2) Overview and "Deep Dive"	Kelley Dempsey Naomi Lefkovitz Victoria Yan Pillitteri
2:45 PM	Questions from the Audience	Please submit questions to sec-cert@nist.gov or @usNISTgov #NISTRMF

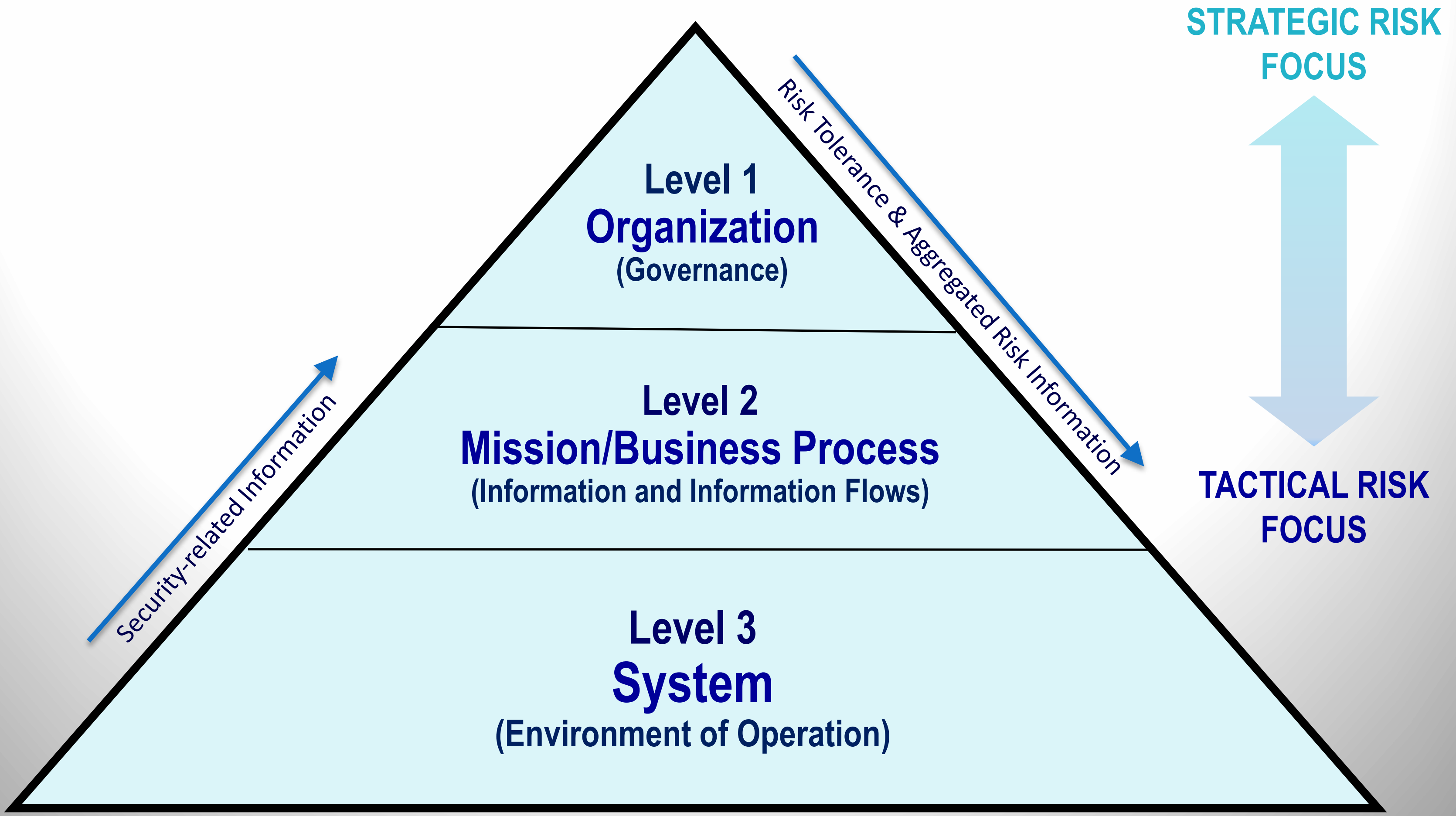
Standards/Guidelines for FISMA & RM

- **FIPS -** Federal Information Processing Standards
  - FIPS 199 – Standards for Security Categorization
  - FIPS 200 – Minimum Security Requirements
- **SPs** – Special Publications
  - 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/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
  - SP 800-160 – System Security Engineering
  - SP 800-161 – Supply Chain Risk Management
  - Many others for operational and technical implementations + NISTIRS

Risk can never be eliminated and so it must be MANAGED!!

Graphic copied from: http://www.featurepics.com/online/Risk-1109124.aspx

Three Risk Management Levels


STRATEGIC RISK FOCUS
Level 1
Organization
(Governance)
Risk Tolerance & Aggregated Risk Information
Security-related Information
Level 2
Mission/Business Process
(Information and Information Flows)
TACTICAL RISK FOCUS
Level 3
System
(Environment of Operation)

NIST SP 800-37 Rev 2

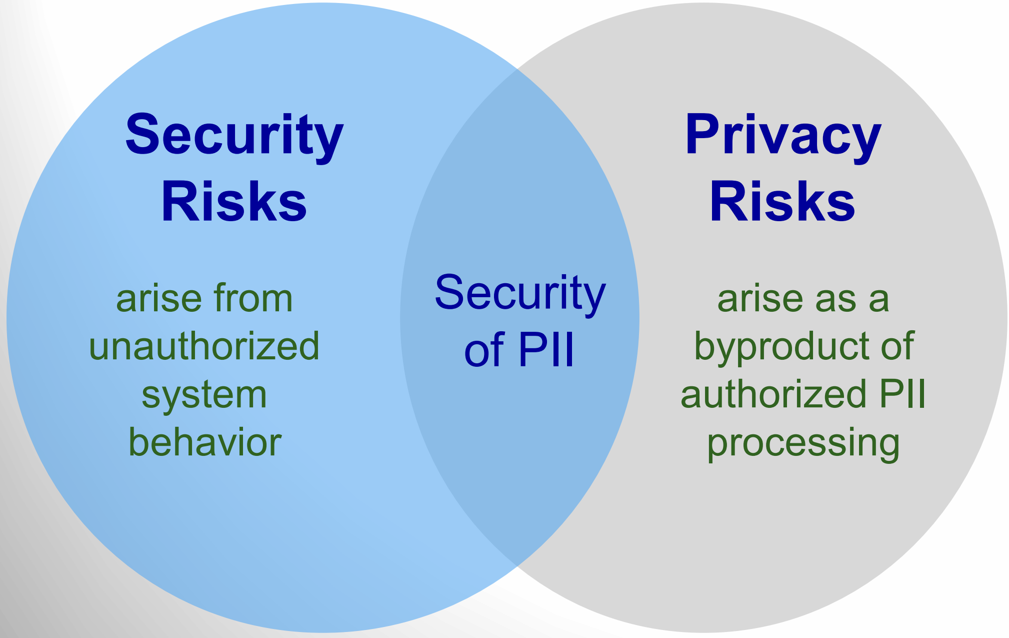
Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

- Published 12-20-18
- Provides a holistic risk management process
- Integrates privacy into the RMF
- Integrates RMF into SDLC
- Aligns CSF, security engineering, and supply chain considerations with the RMF
- Provides processes (tasks) for each RMF step

Purpose

- To ensure that managing risk from systems is consistent with mission/business objectives and the overall risk strategy established by the senior leadership through the risk executive (function)
- To ensure that security and privacy requirements, including necessary controls, are integrated into the organization’s enterprise architecture and system development life cycle processes
- To achieve more secure information and systems through the implementation of appropriate risk response strategies
- To establish **responsibility and accountability** for the security and privacy of organizational systems/information/environments of operation
- To provide senior leaders the necessary information to take credible, risk-based decisions with regard to the security and privacy of systems supporting organizational missions and business functions

Security & Privacy Risk Relationship



Security Risks

arise from unauthorized system behavior

Security of PII

Privacy Risks

arise as a byproduct of authorized PII processing

There is a clear recognition that security of PII plays an important role in the protection of privacy

Individual privacy cannot be achieved solely by securing PII

Authorized processing: system operations that handle PII (collection - disposal) to enable the system to achieve mission/business objectives

NISTIR 8062: Privacy Risk Model

Privacy Risk Factors:

Likelihood | Problematic Data Action | Impact

Examples of problems: embarrassment, loss of autonomy, discrimination, economic loss

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

RMF and CSF Alignment

- Inputs and Outputs reference CSF as applicable, e.g., CSF profile as potential output from Task P-4
- Task Outcome tables reference CSF sections, categories, or sub-categories as applicable
- References for tasks indicate relevant CSF sections (if any)

Security Engineering and RMF Alignment

- Task references list related security engineering processes from SP 800-160, as applicable
- Section 2.4 discusses system elements
  - ***System elements*** include technology or machine elements, human elements, and physical or environmental elements (i.e., information resources)
  - A ***system component*** is a system element implemented in hardware, software, or firmware
- Tasks focus on stakeholder requirements

Supply Chain and RMF Alignment

- Supply chain risk addressed as part of security risk
- Discussion of Supply Chain Risk Management (SCRM) within the RMF added in section 2.8
- SCRM addressed in Task discussions as applicable
- SCRM artifacts included in task Inputs and Outputs as applicable
- SCRM responsibilities noted in Appendix D

RMF Roles and Responsibilities

- Authorizing Official
- Authorizing Official Designated Representative
- Chief Acquisition Officer
- Chief Information Officer
- Common Control Provider
- Control Assessor
- Enterprise Architect
- Head of Agency
- Information Owner or Steward
- Mission or Business Owner
- Risk Executive (Function)
- Security or Privacy Architect
- Senior Accountable Official for Risk Management
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy
- System Administrator
- System Owner
- System Security or Privacy Officer
- System Security or Privacy Engineer
- System User

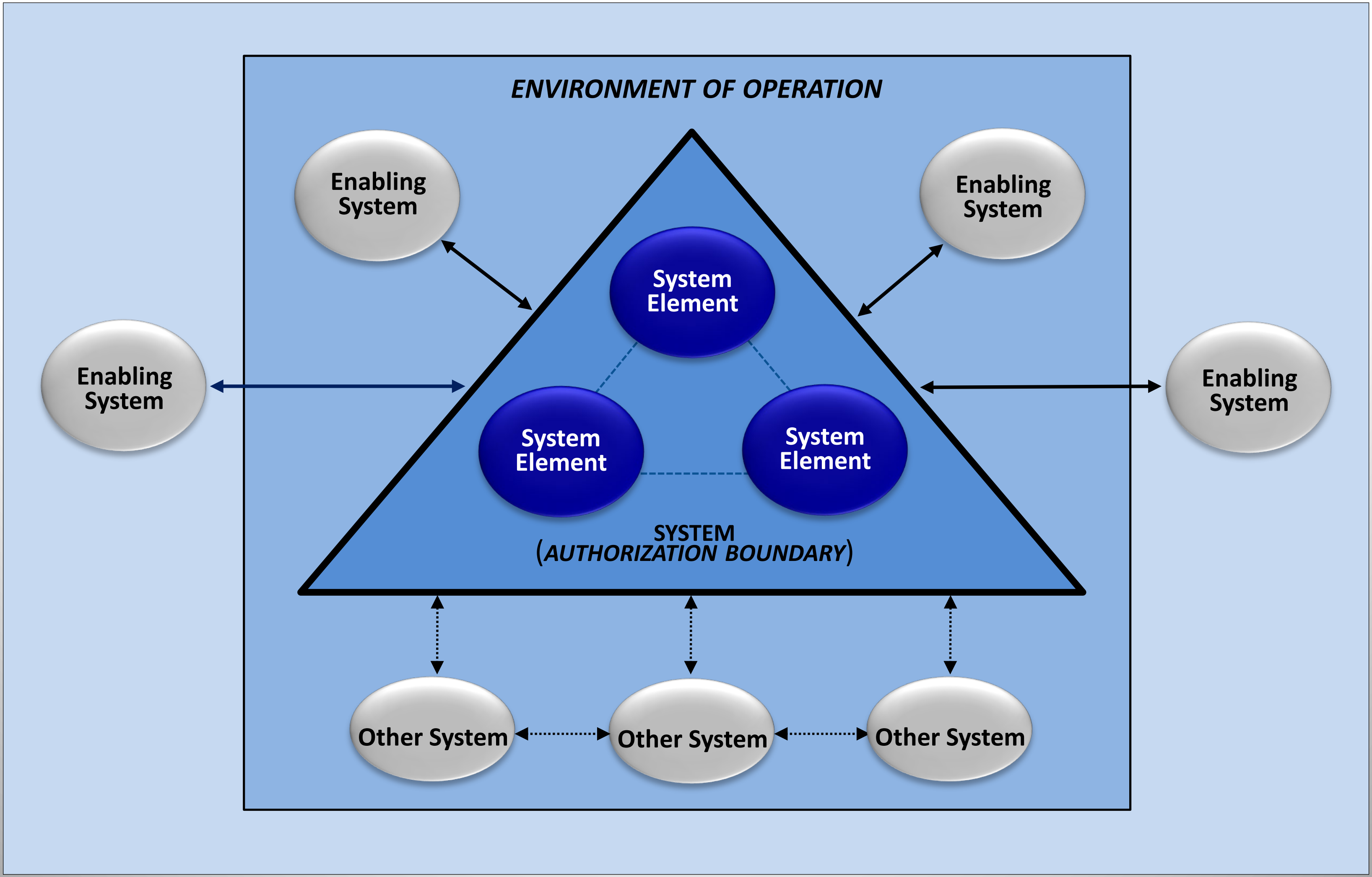
Authorization Boundaries

- Addressed in section 2.5 and Appendix G in 37R2
- Establishes the scope of protection for systems (i.e., what is to be protected as part of a given system)
- Defines the scope of the authorizing official's ***responsibility and accountability*** for protecting information resources and individuals' privacy
- Established during Task P-11 (***before*** security categorization and development of security plans)

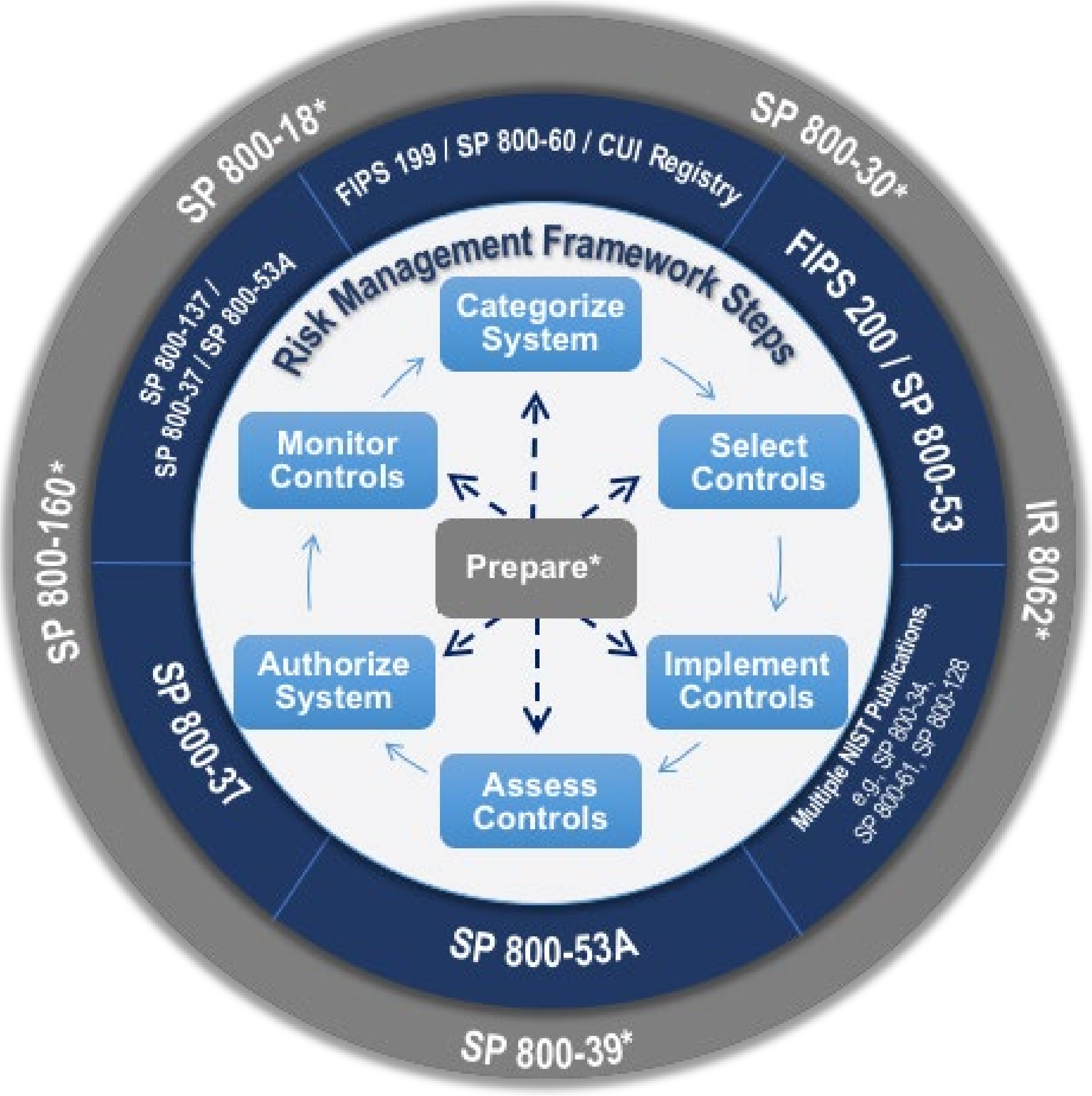
Authorization Boundary Considerations

- System elements:
  - Are under same direct management
  - Support same mission or business functions
  - Process/store/transmit similar information types
  - Reside in same/very similar operating environments
- Organization-wide activity that considers:
  - Mission/business requirements
  - Security and privacy requirements
  - Costs to the organization (WRT potential loss)

RMF Rev 2 Conceptual View of a System



Risk Management Framework Rev 2



Risk Management Framework Steps

Categorize System

Select Controls

Implement Controls

Assess Controls

Authorize System

Monitor Controls

Prepare*

FIPS 199 / SP 800-60 / CUI Registry

FIPS 200 / SP 800-53

Multiple NIST Publications, e.g., SP 800-34, SP 800-61, SP 800-128

SP 800-53A

SP 800-37

SP 800-137 / SP 800-37 / SP 800-53A

SP 800-18*

SP 800-30*

IR 8062*

SP 800-39*

SP 800-160*

RMF 2.0 Task Outcomes

Tasks	Outcomes
Task I-1 **CONTROL IMPLEMENTATION**	- Controls specified in the security and privacy plans are implemented. [*Cybersecurity Framework: PR.IP-1*] - Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. [*Cybersecurity Framework: PR.IP-2*]
Task I-2 **BASELINE CONFIGURATION**	- The configuration baseline is established. [*Cybersecurity Framework: PR.IP-1*] - The security and privacy plans are updated based on information obtained during the implementation of the controls. [*Cybersecurity Framework: Profile*]

RMF Task Structure (1 of 2)

- **Task Section:** Describes the specific RMF task within the appropriate step in the Risk Management Framework
- **Potential Inputs:** Lists information that **may** be needed to complete the task

New

- **Expected Outputs:** Describes the end result of task completion
- **Primary Responsibility Section:** Lists the individual or group within the organization having primary responsibility for ensuring completion of the RMF task

RMF Task Structure (2 of 2)

- **Supporting Roles Section:** Lists the supporting roles within the organization that may help with or provide input for task completion
- **SDLC Phase Section:** Lists the phase of the SDLC when the RMF task is typically executed (not in Prepare)
- **Discussion Section:** Provides additional information about the RMF task
- **References Section:** Provides general references to NIST security standards and guidelines that may be consulted for additional information

RMF 2.0 Task Structure (example)

RISK ASSESSMENT—ORGANIZATION LEVEL

Task P-3 Assess organization-wide security and privacy risk and update the results on an ongoing basis.

Potential Inputs: Risk management strategy; mission or business objectives; current threat information; system-level security and privacy risk assessment results; supply chain risk assessment results; previous organization-level risk assessment results; security- and privacy-related information from continuous monitoring; information sharing agreements or memoranda of understanding.

Expected Outputs: Organization-level risk assessment results.

Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Supporting Roles: Chief Information Officer; Mission or Business Owner; Authorizing Official or Authorizing Official Designated Representative.

Discussion: Risk assessment at the organizational level is focused on risk to mission or business objectives and leverages aggregated information from system-level risk…..

References: NIST SP 800-30; NIST SP 800-39 (Organization Level, Mission/Business Process Level); NIST SP 800-161; NIST IR 8062.

RMF Step: Prepare

New

- Added in Revision 2
- Addresses tasks to be completed ***before*** categorization
- Incorporates guidance from SPs 800-39 and 800-160 and OMB policy (Circular A-130, etc.)
- Formalizes tasks that were previously vaguely described or overlooked
- Tasks for Organizational and/or Missions/Business Process Level
- Tasks for System Level

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.

RMF Tasks: **Prepare - Org & M/B Process Levels**

(1 of 2)

- *P-1:* **Risk Management Roles**

  Identify and assign individuals to specific roles associated with security and privacy risk management

- *P-2:* **Risk Management Strategy**

  Establish a risk management strategy for the organization that includes a determination of risk tolerance

- *P-3:* **Risk Assessment - Organization**

  Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis

RMF Tasks: **Prepare - Org & M/B Process Levels**

(2 of 2)

- *P-4:* **Organizationally-tailored Control Baselines and CSF Profiles** (optional)

  Establish, document, and publish organizationally-tailored control baselines and/or cybersecurity framework profiles

- *P-5:* **Common Control Identification**

  Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems

- *P-6:* **Impact Level Prioritization** (optional)

  Prioritize organizational systems within the same impact level

- *P-7:* **Continuous Monitoring Strategy - Organization**

  Develop and implement an organization-wide strategy for continuously monitoring control effectiveness

RMF Tasks: **Prepare - System Level** (1 of 3)

- *P-8:* **Mission or Business Focus**

  Identify the missions, business functions, and mission/business processes that the system is intended to support

- *P-9:* **System Stakeholders**

  Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system

- *P-10:* **Asset Identification**

  Identify assets that require protection

- *P-11:* **Authorization Boundary**

  Determine the authorization boundary of the system

RMF Tasks: **Prepare - System Level** (2 of 3)

- *P-12:* **Information Types**

  Identify the types of information to be processed, stored, or transmitted by the system

- *P-13:* **Information Life Cycle**

  Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system

- *P-14:* **Risk Assessment - System**

  Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis

- *P-15:* **Requirements Definition**

  Define the security and privacy requirements for the system and the environment of operation

RMF Tasks: **Prepare - System Level** (3 of 3)

- *P-16:* **Enterprise Architecture**

  Determine the placement of the system within the enterprise architecture

- *P-17:* **Requirements Allocation**

  Allocate security and privacy requirements to the system and to the environment of operation

- *P-18:* **System Registration**

  Register the system with organizational program or management offices

NIST Special Publication 800-30*

Revision 1

Guide for Conducting Risk Assessments

- Supports risk assessments conducted:
  - at any risk management level; and
  - at any point in the RMF process
- Supports focused or broad risk assessments
- Uses a **qualitative** approach
- Four risk factors:
  - Threats
  - Vulnerabilities
  - Likelihoods
  - Impacts

NIST Special Publication 800-39*

Managing Information Security Risk:
Organization, Mission, and Information System View

- Supports an integrated, organization-wide security risk management program (all RMF steps and RM levels)
- Defines three security risk management levels and discusses risk management at the three levels
- Four components:
  - Framing risk
  - Assessing risk
  - Responding to risk
  - Monitoring risk

NIST Special Publication 800-60, Rev 1*

Guide for Mapping Types of Information and Information Systems to Security Categories

- Supports RMF Prepare and Categorize Steps
- Volume 1 provides guidance on the process
- Volume 2 provides a catalog of information types and provisional categorizations (impact levels)
- UPDATE: Also use the **CUI Registry**
- Inventory and categorize all information types processed, stored, or transmitted by the system
- Apply the high water mark concept to categorize the system overall

NIST Special Publication 800-160*

Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

- Supports all RMF steps, but starts with, or even before, the RMF Prepare step
- Integrates considerations for security and trustworthiness into existing systems engineering processes as defined in ISO standard 15288
- Multiple volumes
  - Volume 1: Main process volume as above
  - Volume 2: Cyber Resiliency Considerations (draft)
  - More volumes planned……

NIST Special Publication 800-161*

Supply Chain Risk Management Practices for
Federal Information Systems and Organizations

- Supports all RMF steps and RM levels
- Focused on information and communications technology (ICT) products and services
- Provides guidance on:
  - Identifying/assessing/mitigating ICT supply chain risk
  - Supply chain risk management (SCRM) plan development
  - Integrating ICT supply chain risk management into existing risk management activities
  - ICT SCRM-relevant controls from 800-53

NIST Interagency Report 8062*

An Introduction to Privacy Engineering and Risk Management in Federal Systems

- Supports all RMF steps and RM levels
- Introduces privacy engineering and privacy risk management concepts using:
  - common terms;
  - privacy engineering objectives; and
  - a privacy risk model
- Addresses individuals' privacy protection needs not related to confidentiality (e.g., PII creation, collection, use, processing, retention, and dissemination)

NIST Interagency Report 8179*

Criticality Analysis Process Model: Prioritizing Systems and Components

- Supports all RMF steps and RM levels
- Provides a structured method for prioritizing programs, systems, and components based on their importance
- Used as a component of holistic and comprehensive risk management (all types of risk)
- Five main processes:
  - Define criticality analysis procedures
  - Conduct program-level criticality analysis
  - Conduct system/subsystem-level criticality analysis
  - Conduct component/sub-component-level criticality analysis
  - Conduct detailed review of criticality for the above three

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.

RMF Tasks: **Categorize** Information & System

- *C-1:* **System Description**

  Document the characteristics of the system

- *C-2:* **Security Categorization**

  Categorize the system and document the security categorization results

- *C-3:* **Security Categorization Review and Approval**

  Review and approve the security categorization results and decision

New

NIST Special Publication 800-18*

Revision 1

Guide for Developing Security Plans for Federal Information Systems

- Guidance for developing system security plans
  - Structure and content
  - Template
- Supports all RMF steps, but **begins during Categorize Step**
- Is a **LIVING** document (update as changes are made)
- Used to record information about the system
  - System boundary/diagram/information flow
  - Roles and responsibilities
  - **Security control implementation details**
  - Rationale/justification for risk-based decisions (scoping)
  - Other documents may be referenced

FIPS 199*

Standards for Security Categorization of Federal Information and Information Systems

- In the context of ***security objectives*** from FISMA
  - Confidentiality – unauthorized disclosure
  - Integrity – unauthorized modification/destruction
  - Availability – disruption of access to/use of information
- Defines three ***impact levels:***
  - Low – loss would have a ***limited*** adverse impact
  - Moderate – loss would have a ***serious*** adverse impact
  - High – loss would have a catastrophic adverse impact

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.

RMF Tasks: **Select** Controls (1 of 2)

- *S-1:* **Control Selection**

  Select the controls for the system and environment of operation

- *S-2:* **Control Tailoring**

  Tailor the controls selected for the system and environment of operation

  New

- *S-3:* **Control Allocation**

  Allocate security and privacy controls to the system and to the environment of operation

  Revised

RMF Tasks: Select Controls (2 of 2)

- *S-4:* **Document Planned Control Implementations**

  Document the controls for the system and environment of operation in security and privacy plans

  New

- *S-5:* **Continuous Monitoring Strategy - System**

  Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy

  Revised

- *S-6:* **Plan Review and Approval**

  Review and approve the security and privacy plans for the system and environment of operation

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 types of 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*

Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

- A **catalog** of security controls
- Supports RMF Select Step 2
- Defines three security baselines (L, M, H)
- Initial version published in early 2005
- Revision 4 final was published 30 April 2013
- Revision 5 is in initial public draft

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

RMF Tasks: **Implement** Controls

- *I-1:* **Control Implementation**

  Implement the controls as specified in security and privacy plans

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

  Revised

  Document changes to planned control implementations based on the as-implemented state of the controls

NIST Special Publication 800-128*

Guide for Security-Focused Configuration Management of Information Systems

- Implementation guidance for Configuration Management (CM) family controls from 800-53
- Four Phases
  1. Planning
  2. Identifying and Implementing Configurations
  3. Controlling Configuration Change
  4. SecCM Monitoring

NIST Special Publication 800-34*

Revision 1

Contingency Planning Guide for Federal Information Systems

- Implementation guidance for Contingency Planning (CP) family controls from 800-53
- Business Impact Analysis
- Identifies three phases:
  - Activation/Notification Phase
  - Recovery Phase
  - Reconstitution Phase
- Roles and responsibilities
- Suggested appendices for contingency plans

NIST SP 800-61*

Revision 2

Computer Security Incident Handling Guide

- Implementation guidance for Incident Response (IR) family controls from 800-53
- Identifies four phases:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-Incident Activity
- Coordination and information sharing
- Also see SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

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

RMF Tasks: **Assess** Controls (1 of 2)

- *A-1:* **Assessor Selection** New

  Select the appropriate assessor or assessment team for the type of control assessment to be conducted

- *A-2:* **Assessment Plan**

  Develop, review, and approve plans to assess implemented controls

- *A-3:* **Control Assessments**

  Assess the security controls in accordance with the assessment procedures defined in the security assessment plan

RMF Tasks: **Assess** Controls (2 of 2)

- *A-4:* **Assessment Reports**

  Prepare the assessment reports documenting the findings and recommendations from the control assessments

- *A-5:* **Remediation Actions**

  Conduct initial remediation actions on the controls and reassess remediated controls

- *A-6:* **Plan of Action and Milestones** Moved

  Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports

NIST Special Publication 800-53A*

Revision 4

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

- Supports RMF Assess Step
- Is a *companion* document to 800-53
- Is updated to be consistent with 800-53 updates
- Describes high level procedures for assessing security controls for effectiveness
- Defines/provides assessment objectives, methods, and objects

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

RMF Tasks: **Authorize** the System

- *R-1:* **Authorization Package**

  Assemble the authorization package and submit the package to the authorizing official for an authorization decision

- *R-2:* **Risk Analysis and Determination** Revised

  Analyze and determine the risk from the operation or use of the system or the provision of common controls

- *R-3:* **Risk Response** New

  Identify and implement a preferred course of action in response to the risk determined

- *R-4:* **Authorization Decision**

  Determine if the risk from the operation or use of the system or the provision or use of common controls is acceptable

- *R-5:* **Authorization Reporting** New

  Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.

RMF **Monitor** Step Purpose

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

RMF Tasks: **Monitor** Controls (1 of 2)

- *M-1:* **System and Environment Changes**

  Monitor the system and its environment of operation for changes that impact the security and privacy posture of the system

- *M-2:* **Ongoing Assessments**

  Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy

- *M-3:* **Ongoing Risk Response**

  Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones

- *M-4:* **Authorization Package Updates**

  Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process

RMF Tasks: **Monitor** Controls (2 of 2)

- *M-5:* **Security and Privacy Reporting**

  Report the security status of the system (including the effectiveness of security controls employed within and inherited by the system) to appropriate organizational officials on an ongoing basis in accordance with the organization-defined monitoring strategy

- *M-6:* **Ongoing Authorization**

  Review the reported security status of the system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable

- *M-7:* **System Disposal**

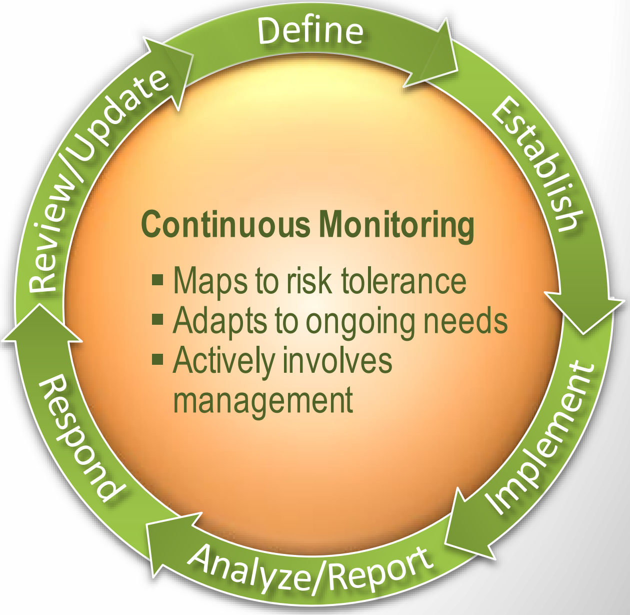
  Implement a system decommissioning strategy which executes required actions when a system is removed from service

NIST Special Publication 800-137*

Information Security Continuous Monitoring for Federal Information Systems and Organizations

- Supports RMF Monitor Step
- Management level guidance on developing an information security continuous monitoring (ISCM) strategy and implementing an ISCM program
- ISCM is **maintaining ongoing awareness** of information security, vulnerabilities, and threats to **support organizational risk management decisions**

ISCM Process Steps*



1. Define continous monitoring strategy
2. Establish continuous monitoring program
   a) Determine metrics
   b) Determine monitoring frequencies
   c) Develop ISCM architecture
3. Implement the monitoring program
4. Analyze security-related information (data) and report findings
5. Respond with mitigation actions OR reject/avoid, transfer, or accept risk
6. Review and update monitoring strategy and program

ISCM Frequency Criteria*

1. Control volatility
2. System categorization/impact levels
3. Controls/assessment objects providing critical functions
4. Controls with identified weaknesses
5. Organizational risk tolerance
6. Threat information
7. Vulnerability information
8. Risk Assessment results
9. Output of monitoring strategy reviews
10. Reporting requirements

NIST Interagency Report 8011*

Automation Support for Ongoing Assessment

- Supports RMF Monitor Step
- Implementation level support for automation of ongoing assessment
  - Desired State Specification in a databased format as defined by the organization
  - Actual State (as discovered by automated tools)
  - Defect Checks (compares desired state to actual state)
- Multiple volumes based on security capabilities
  - Volume 1 – **Overview**
  - Volume 2 – **Hardware Asset Management**
  - Volume 3 – **Software Asset Management**
  - Volume 4 – **Vulnerability Management (in draft)**

Automation: The Need for Caution*

- Automated tools may lead to a false sense of security by **not** providing a complete picture of the overall security posture

- Automated tools must be installed and configured correctly and require ongoing maintenance for accuracy and integrity

SP 800-37 Rev 2 Supporting Appendices

- A: References
- B: Glossary
- C: Acronyms
- D: Roles and Responsibilities
- E: Summary of RMF Tasks
- **F: System and Common Control Authorizations**
- G: Authorization Boundary Considerations
- H: System Life Cycle Considerations

Authorization Types

- Initial Authorization
- Ongoing Authorization
- Reauthorization

Initial Authorization

- Initial (start-up) risk determination and risk acceptance
- Based on a complete, zero-based review of the system or of common controls
- System-Level zero-based review includes:
  - Assessment of all implemented system-level controls
  - Review of the security status of inherited common controls
- Common control zero-based review includes:
  - Assessment of any controls that contribute to the provision of a common control or set of common controls, i.e., not just the control itself but associated policies, procedures, etc.

Ongoing Authorization

- Subsequent (follow-on) risk determinations and risk acceptance decisions
- Occurs at agreed-upon and documented frequencies (time-driven) **and** when organization-defined thresholds are exceeded (event-driven)
- Dependent on a robust and mature continuous monitoring program to provide ongoing understanding and ongoing acceptance of security and privacy risk

Ongoing Authorization

- Specific conditions required to support ongoing authorization:
  1. An initial authorization to operate or common control authorization has been issued based on a complete, zero-based review; and
  2. An organizational continuous monitoring program is in place that monitors all implemented controls with appropriate degree of rigor and at the org-specified frequencies
- Security-related info from monitoring provides current information that AOs need to maintain situational awareness and make informed authorization (risk) decisions
- Security-related info supporting ongoing authorization is ideally made available to AOs as a SEIM-style report
- Security-related info from manual or automated monitoring may be used

Reauthorization

- Static, single point-in-time risk determination and risk acceptance that occurs after the initial authorization
- May be time-driven or event-driven
- Is a separate activity from ongoing authorization
- Under ongoing authorization, reauthorization is an event-driven action initiated in response to increased risk
- Is conducted with a similar level of effort as the initial authorization and may be:
    - a complete, zero-based assessment; or
    - a targeted assessment based on the type of event that triggered the reauthorization action
- Reauthorization actions may lead to a review of the ISCM strategy which could affect ongoing authorization

Authorization Decisions

- Authorization to Operate
- Common Control Authorization
- Authorization to Use
- Denial of Authorization

Authorization to Operate

- Issued by the Authorizing Official after determining that the risk to organizational operations, assets, individuals, other organizations, and the Nation is acceptable
- An authorization termination date is specified or, if under ongoing authorization, a time-driven authorization frequency is specified
- The Authorizing Official may include operating restrictions as part of the authorization to operate

Common Control Authorization

- Similar to the authorization to operate for systems but issued for common controls
- A common control authorization termination date is specified or, if under ongoing authorization, a time-driven authorization frequency is specified
- Common controls implemented as part of a system do not require a separate common control authorization

Authorization to Use

- Employed when an organization, after reviewing an existing authorization package, accepts the ATO **issued by an AO from another federal entity**
- The authorization to use is issued by an official with the same level of responsibility and authority for risk management as an AO that issues an ATO
- The authorization to use indicates acceptance of risk by the customer org with respect to customer's info
- Remains in effect as long as customer org continues to accept the risk as indicated in provider org package

Denial of Authorization

- The authorizing official denies authorization to operate, common control authorization, or authorization to use when existing risk is determined to be unacceptable
- Denial of authorization indicates that there are significant deficiencies in controls
  - Required controls are not implemented
  - Implemented controls are not operating as intended
- Authorizing officials should not feel pressured into accepting unacceptable risk (OPM breach!)

Other Authorization Options

- Type authorization
  - Single authorization for a common version of a system
  - For a system comprised of identical instances of architecture, software, information types, etc.
  - Often used in conjunction with a facility authorization
- Facility authorization
  - Authorizes common controls provided in a specific environment of operation
  - Provided at a specified impact level
- Traditional or Joint Authorization Approaches

Contact Information

FISMA Project Leader and NIST Fellow
Dr. Ron Ross: ron.ross@nist.gov

Senior Information Security Specialist
Kelley Dempsey: kelley.dempsey@nist.gov

Team Lead and Sr Computer Scientist
Victoria Yan Pillitteri: victoria.yan@nist.gov

Information Security Specialists
Ned Goren: nedim.goren@nist.gov

Jody Jacobs: jody.jacobs@nist.gov

RMF Team Email: sec-cert@nist.gov

RMF website:
https://csrc.nist.gov/Projects/Risk-Management

Privacy Engineering Project Leader and Senior Privacy Policy Advisor
Naomi Lefkovitz: Naomi.lefkovitz@nist.gov

Privacy Risk Strategists
Ellen Nadeau: ellen.nadeau@nist.gov

Kaitlin Boeckl: kaitlin.boeckl@nist.gov

Administrative Support
Jeff Brewer: jeffery.brewer@nist.gov

Privacy Team Email: privacyeng@nist.gov

Privacy Engineering website:
https://csrc.nist.gov/Projects/Privacy-Engineering

NIST RMF Webcast: Q&A

Due to limited time during the webcast, we will answer selected questions live.
However, the NST team will respond to all inquiries via email or Twitter in the coming weeks.

Questions and Comments

sec-cert@nist.gov

@usNISTgov
#NISTRMF

*Please direct any **technical issues*** (webcast sound, video, etc.) to: webcast@nist.gov

Resources

https://go.usa.gov/xENcs

- Slides available for download
- Webcast recording will be available by **March 14, 2019**

Project website:
https://csrc.nist.gov/Projects/Risk-Management