

NIST Special Publication 800-37

*Applying the Risk Management Framework to
Federal Information Systems*

UCDMO Conference

September 1-2, 2009

Dr. Ron Ross

*Computer Security Division
Information Technology Laboratory*



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Introduction



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Unified Information Security Framework

The Generalized Model

**Unique
Information
Security
Requirements**

The “Delta”



**Common
Information
Security
Requirements**

Foundational Set of Information Security Standards and Guidance

- Standardized risk management process
- Standardized security categorization (criticality/sensitivity)
- Standardized security controls (safeguards/countermeasures)
- Standardized security assessment procedures
- Standardized security authorization process

National security and non national security information systems

Common Security Authorization Process

- NIST Special Publication 800-37, Revision 1

Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

- Developed by Joint Task Force Transformation Initiative Working Group

- *Office of the Director of National Intelligence*
- *Department of Defense*
- *Committee on National Security Systems*
- *National Institute of Standards and Technology*

- Final Public Draft (September 2009)

Purpose

Special Publication 800-37, Revision 1

- Provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of:
 - Security categorization;
 - Security control selection and implementation;
 - Security control assessment;
 - Information system authorization; and
 - Security control monitoring.

Target Audience

Special Publication 800-37, Revision 1

- Individuals with information system development and integration responsibilities.
- Individuals with information system and security management and oversight responsibilities.
- Individuals with information system and security control assessment and monitoring responsibilities.
- Individuals with information security implementation and operational responsibilities.

The Fundamentals



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Main Streaming Information Security

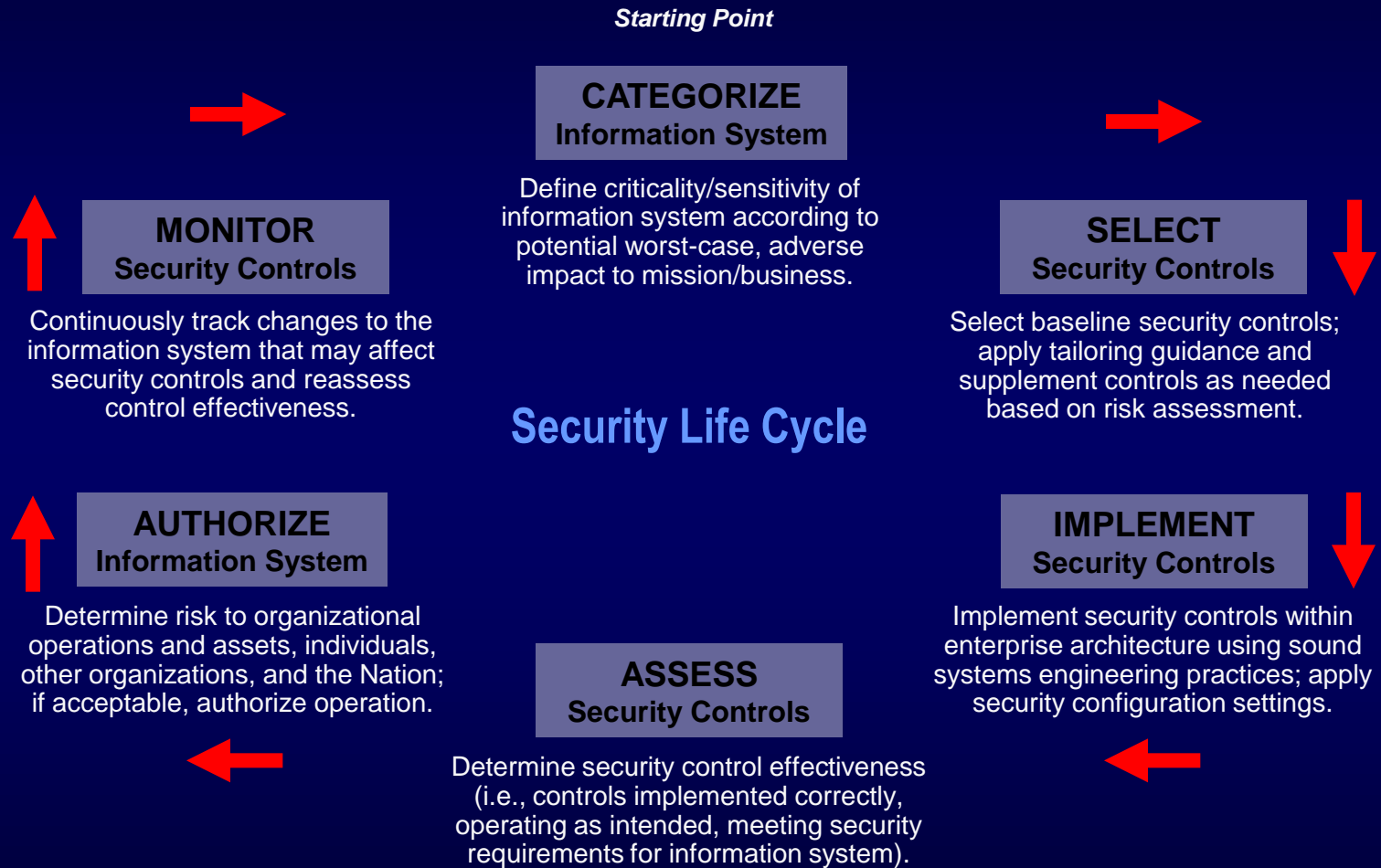
- Information security requirements must be considered *first order requirements* and are critical to mission and business success.
- An effective organization-wide information security program helps to ensure that security considerations are specifically addressed in the *enterprise architecture* for the organization and are integrated early into the *system development life cycle*.

System Development Life Cycle

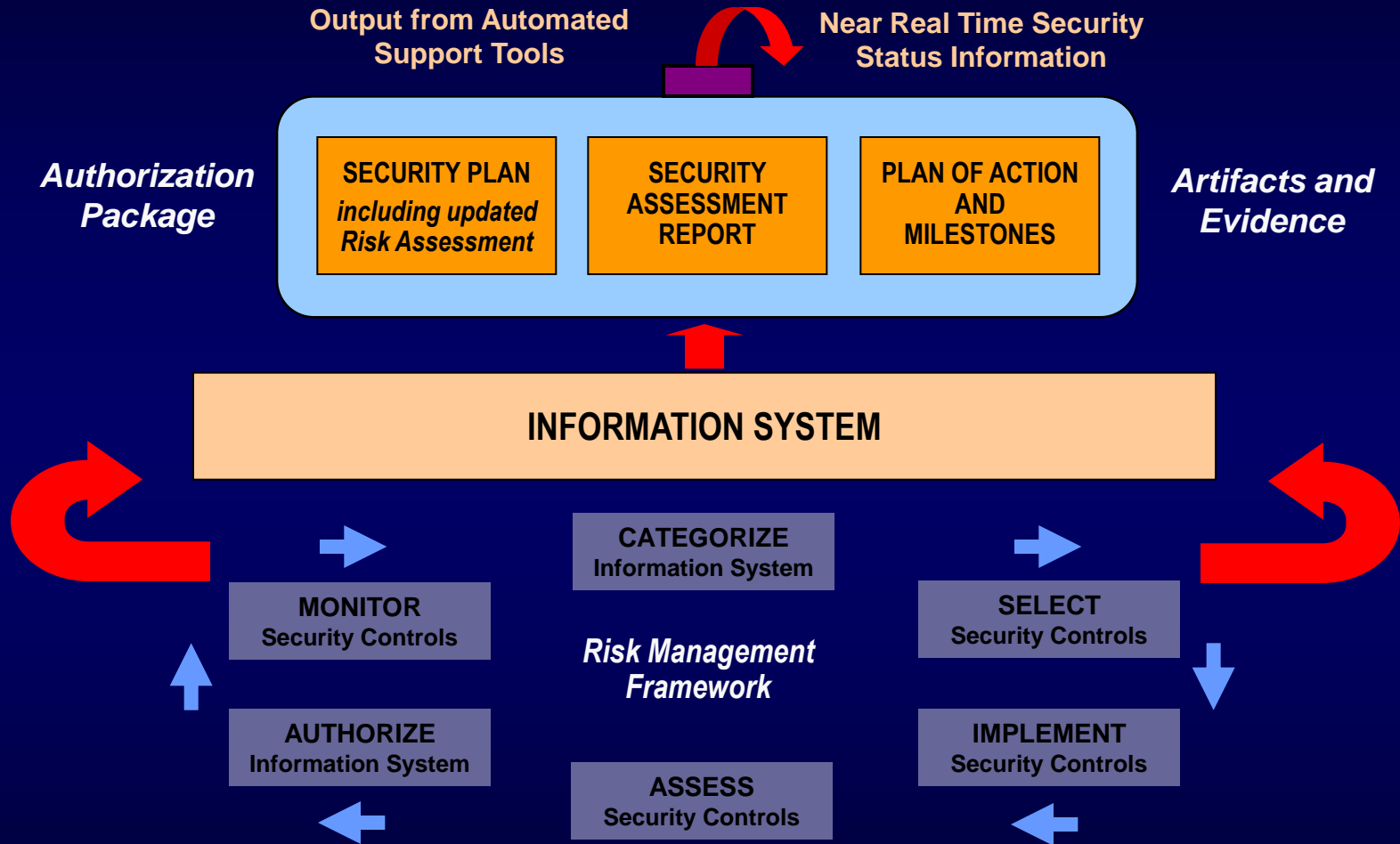
- System Initiation Phase
- System Development / Acquisition Phase
- System Implementation Phase
- System Operations / Maintenance Phase
- System Disposal Phase

Integrating security requirements into the SDLC is the most efficient and cost-effective method for an organization to ensure that its protection strategy is achieved and that authorization activities are not isolated or decoupled from the management processes employed by the organization to develop, implement, operate, and maintain information systems supporting ongoing missions or business functions...

Risk Management Framework



Applying the Risk Management Framework to Information Systems



Risk Management Roles

- Authorizing Official
- Authorizing Official Designated Representative
- Chief Information Officer
- Senior Agency Information Security Officer
- Risk Executive (Function)
- Information System Owner

Risk Management Roles

- Common Control Provider
- Information Owner/Steward
- Information System Security Officer
- Information System Security Engineer
- Security Control Assessor
- User Representatives

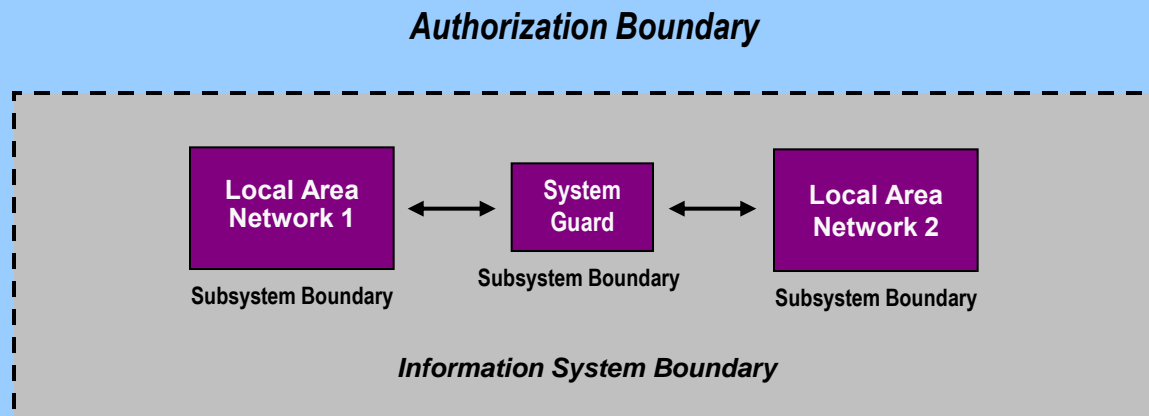
Authorization Boundaries

- Define the scope of protection for information systems (i.e., what the organization agrees to protect under its direct control or within the scope of its responsibilities).
- Include the people, processes, and technologies that are part of the systems supporting the organization's missions and business processes.
- Need to be established before information system security categorization and the development of security plans.

Authorization Boundaries

- Generally information system resources that are under the same direct management control (e.g., budgetary, programmatic, or operational authority and associated *responsibility and accountability*).
- May also be helpful to consider if the information resources being identified as an information system:
 - Have the same function or mission objective and essentially the same operating characteristics and information security needs; and
 - Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).

Large and Complex Systems



- Security plan reflects information system decomposition with security controls assigned to each subsystem component.
- Security assessment procedures tailored for the security controls in each subsystem component and for the combined system level.
- Security control assessment performed on each subsystem component and on system-level controls not covered by subsystem security control assessments.
- Security authorization conducted on the information system as a whole.

Security Control Inheritance

- Authorizing officials and information system owners are becoming increasingly dependent on security controls provided by organizational entities that are outside of their authorization boundaries, for example:
 - Organizational networks;
 - Facilities management office;
 - Human resources office;
 - Shared/external service providers.
- These security controls, often referred to as *common controls*, are typically not under the direct control of the information system owners and authorizing officials whose systems *inherit* those controls.

Security Control Inheritance

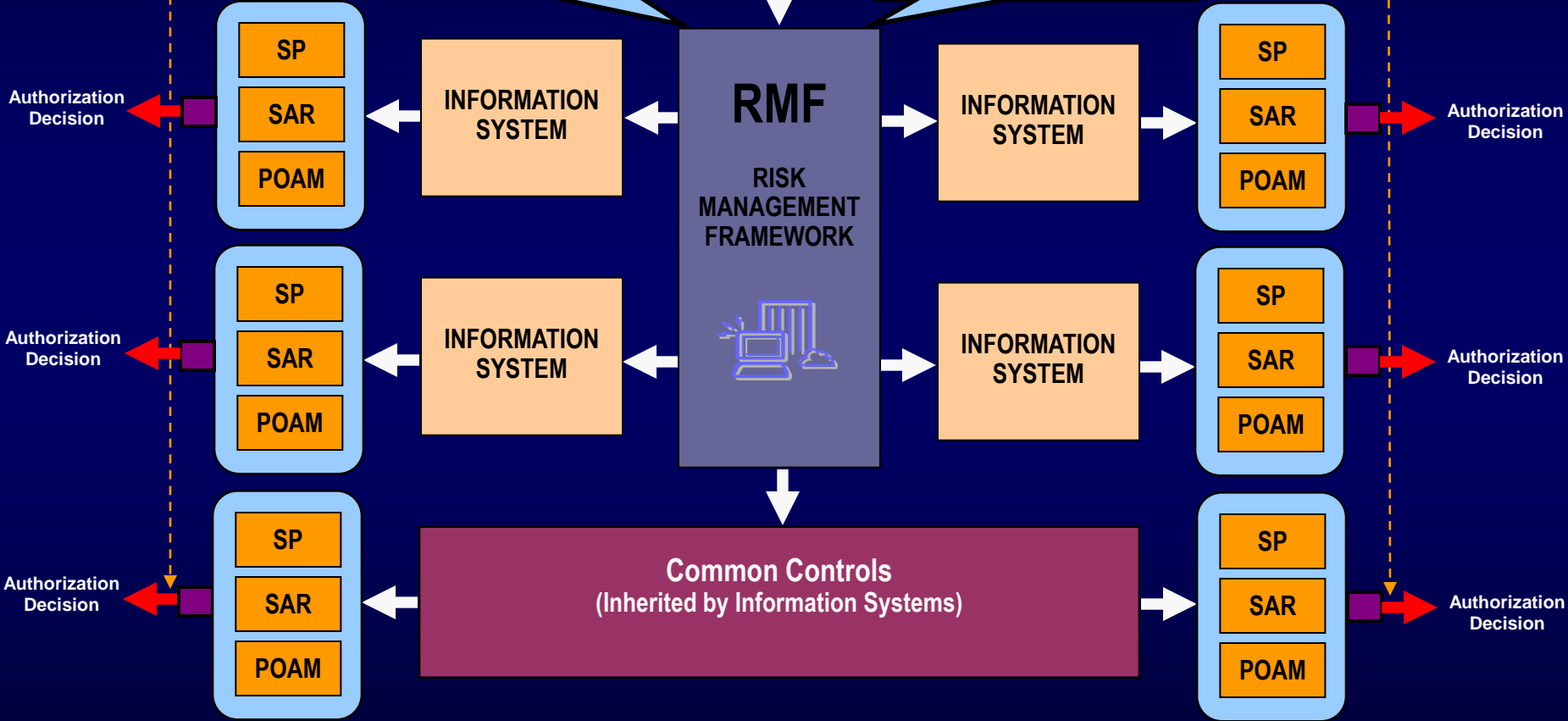
- Common controls provided by an information system owner are documented in a security plan.
- Common controls provided by entities other than information system owners are documented in a security plan or equivalent document.

Bottom line: Every security control within an organization has an entity assigned responsibility for development, implementation, assessment for effectiveness, and authorization/approval.

RISK EXECUTIVE FUNCTION
Enterprise-wide Oversight, Monitoring, and Risk Management

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations



Security Authorization Package

- Security Plan

- *Provides an overview of the security requirements and describes the security controls in place or planned for meeting those requirements.*

- Security Assessment Report

- *Provides the results of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements.*

- Plan of Action and Milestones

- *Describes the specific measures that are planned: (i) to correct weaknesses or deficiencies noted in the security controls during the security control assessment; and (ii) to address known vulnerabilities in the information system.*

Security Authorization Decisions

- Authorization to Operate

- *Based on a review of the information system authorization package, the authorizing official deems the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.*

- Denial of Authorization to Operate

- *Based on a review of the information system authorization package, the authorizing official deems the risk to organizational operations and assets, individuals, other organizations, and the Nation is unacceptable.*

Authorization Decision Document

- Authorization Decision
 - *Provides an authorization to operate or denial of authorization to operate.*
- Terms and Conditions for the Authorization
 - *Provides a description of any limitations or restrictions placed on the operation of the information system that must be followed by the system owner.*
- Authorization Termination Date
 - *Indicates when the security authorization expires and reauthorization is required.*

Reauthorization Actions

■ Time Driven

- *Reauthorization occurs when authorization termination date is reached.*
- *Maximum authorization periods are determined by federal and organizational policies.*

■ Event Driven

- *Reauthorization occurs when there is significant change to the information system or its environment of operation.*
- *Routine changes to an information system or its environment of operation can be handled by the organization's continuous monitoring program.*
- *Change in authorizing official may trigger a reauthorization; but not automatically.*

Continuous Monitoring Programs

- An effective continuous monitoring program includes:
 - *Configuration management and control processes for information systems;*
 - *Security impact analyses on actual or proposed changes to information systems and environments of operation;*
 - *Assessment of selected security controls based on continuous monitoring strategy;*
 - *Security status reporting to appropriate organizational officials;*
 - *Active involvement by authorizing officials in the ongoing management of information system-related security risks.*

The Process



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

RMF Task Structure

- **Task Section**
 - *Describes the specific task within the appropriate step in the Risk Management Framework.*
- **Primary Responsibility Section**
 - *Lists the individual or group within the organization having primary responsibility for executing the RMF task.*
- **Supporting Roles Section**
 - *Lists the supporting roles within the organization that may be necessary to help the individual or group with primary responsibility for executing the RMF task.*
- **SDLC Phase Section**
 - *Lists the particular phase of the SDLC when the RMF task is typically executed.*

RMF Task Structure

- Supplemental Guidance Section
 - *Provides supplemental guidance for executing the RMF task including additional information from relevant supporting security policies, instructions, standards, and guidelines.*
- References Section
 - *Provides general references to security standards and guidelines that should be consulted for additional information with regard to executing the RMF task.*

RMF Tasks

RMF Step 1: Categorize Information System

- **SYSTEM DESCRIPTION**
 - *Task 1-1: Describe the information system (including system boundary) and document the description in the security plan.*
- **SYSTEM REGISTRATION**
 - *Task 1-2: Register the information system with appropriate organizational program/management offices.*
- **SECURITY CATEGORIZATION**
 - *Task 1-3: Determine the security category for the information system and document the category in the security plan.*

RMF Tasks

RMF Step 2: Select Security Controls

- **COMMON CONTROL IDENTIFICATION**
 - *Task 2-1: Identify the common controls inherited by the information system and document the controls in a security plan (or equivalent document).*
- **SECURITY CONTROL SELECTION**
 - *Task 2-2: Select the security controls for the information system and document the controls in the security plan.*
- **SECURITY PLAN APPROVAL**
 - *Task 2-3: Review and approve the security plan.*

RMF Tasks

RMF Step 3: Implement Security Controls

- **SECURITY CONTROL IMPLEMENTATION**
 - *Task 3-1: Implement the security controls specified in the security plan.*
- **SECURITY CONTROL DOCUMENTATION**
 - *Task 3-2: Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).*

RMF Tasks

RMF Step 4: Assess Security Controls

- **SECURITY ASSESSMENT PREPARATION**
 - *Task 4-1: Develop, review, and approve a plan to assess the security controls.*
- **SECURITY CONTROL ASSESSMENT**
 - *Task 4-2: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.*
- **SECURITY ASSESSMENT REPORT**
 - *Task 4-3: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.*

RMF Tasks

RMF Step 5: Authorize Information System

- **REMEDIATION ACTIONS**

- *Task 5-1: Conduct initial remediation actions, if necessary, based on the findings and recommendations of the security assessment report.*

- **PLAN OF ACTIONS AND MILESTONES**

- *Task 5-2: Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.*

- **SECURITY AUTHORIZATION PACKAGE**

- *Task 5-3: Assemble the authorization package and submit to authorizing official for adjudication.*

RMF Tasks

RMF Step 5: Authorize Information System

- **RISK DETERMINATION**

- *Task 5-4: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.*

- **RISK ACCEPTANCE**

- *Task 5-5: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.*

RMF Tasks

RMF Step 6: Monitor Security Controls

- **MONITORING STRATEGY**
 - *Task 6-1: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the information system and its environment of operation.*
- **SYSTEM AND ENVIRONMENT CHANGES**
 - *Task 6-2: Determine the security impact of proposed/actual changes to the information system and its environment of operation.*
- **ONGOING SECURITY CONTROL ASSESSMENTS**
 - *Task 6-3: Assess a selected subset of the security controls in the information system and its environment of operation including those controls affected by changes to the system/environment in accordance with the monitoring strategy.*

RMF Tasks

RMF Step 6: Monitor Security Controls

- **ONGOING REMEDIATION ACTIONS**
 - *Task 6-4: Conduct selected remediation actions based on the results of ongoing monitoring activities and the outstanding items in the plan of action and milestones.*
- **CRITICAL UPDATES**
 - *Task 6-5: Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.*
- **SECURITY STATUS REPORTING**
 - *Task 6-6: Report the security status of the information system and its environment of operation to appropriate organizational officials periodically in accordance with the organization-defined monitoring strategy.*

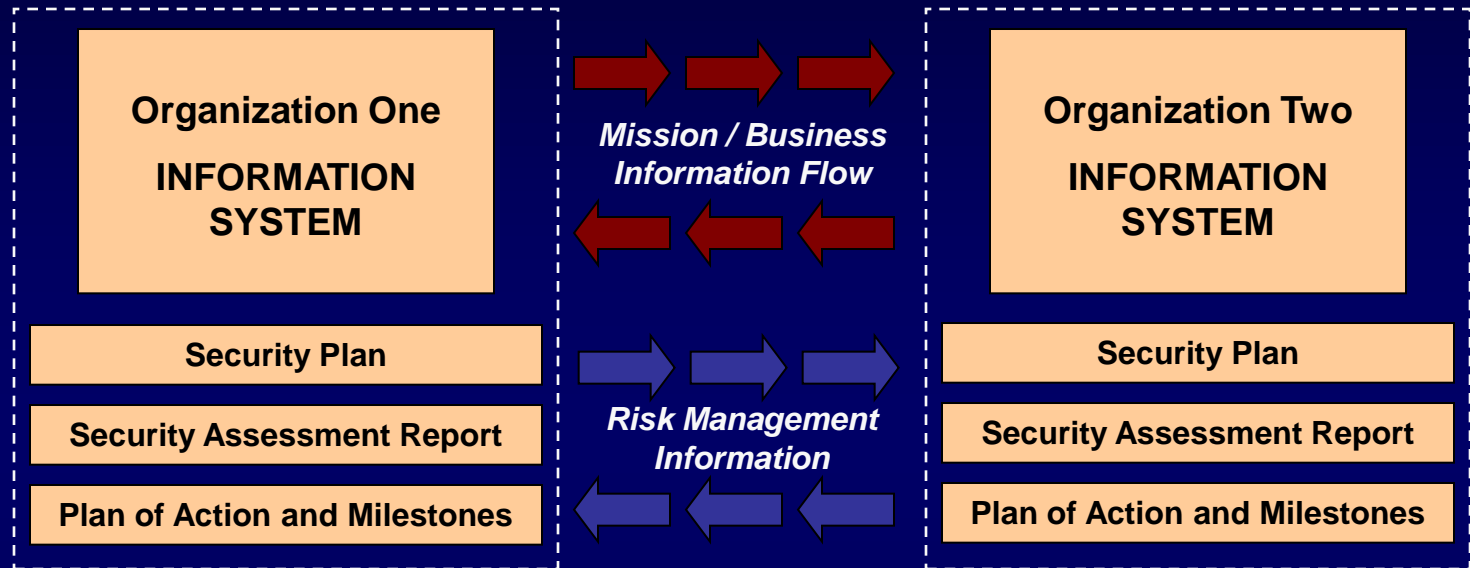
RMF Tasks

RMF Step 6: Monitor Security Controls

- **ONGOING RISK DETERMINATION AND ACCEPTANCE**
 - *Task 6-7: Periodically review the reported security status of the information system and its environment of operation to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.*
- **SYSTEM REMOVAL AND DECOMMISSIONING**
 - *Task 6-8: Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.*

Summary

Trust and Reciprocity



Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

The objective is to achieve transparency of prospective partner's information security programs and processes...establishing trust relationships based on common, shared risk management principles.

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Matt Scholl
(301) 975-2941
matthew.scholl@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov

