

NIST SP 800-37, Revision 1

Applying Risk Management to Information Systems

(Transforming the Certification and Accreditation Process)

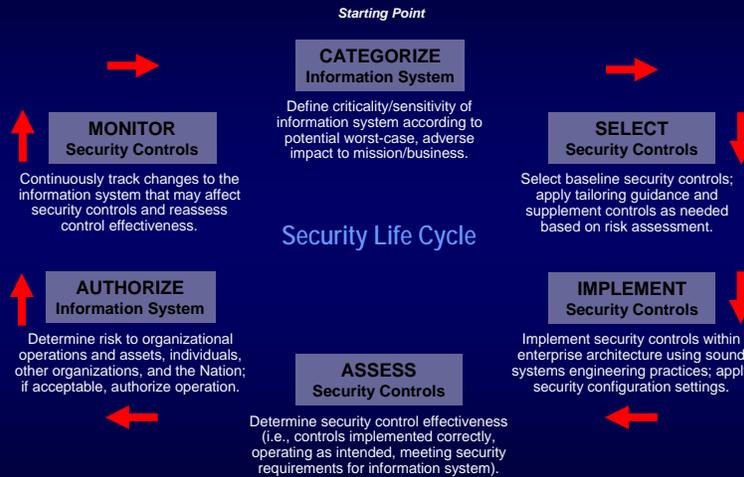
NIST ICS Security Workshop

September 24, 2010

Dr. Ron Ross
*Computer Security Division
Information Technology Laboratory*

Introduction

Risk Management Framework



Common Risk Management 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 (November 2009)
- Final Publication (February 2010)

Purpose

- Provide guidelines for applying the Risk Management Framework to federal information systems—
 - To ensure that managing risk from information 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 information security requirements, including necessary security controls, are integrated into the organization's enterprise architecture and system development life cycle processes.
 - To support consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk-related information, and reciprocity of authorization results.
 - To achieve more secure information and information systems through the implementation of appropriate risk mitigation strategies.

Applicability

- Federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.
- National security systems with the approval of federal officials exercising policy authority over such systems.

State, local, and tribal governments, as well as private sector organizations are encouraged to consider using these guidelines, as appropriate.

Target Audience

- Individuals with mission/business ownership responsibilities or fiduciary responsibilities.
- Individuals with information system development and integration responsibilities.
- Individuals with information system and/or security management/oversight responsibilities.
- Individuals with information system and security control assessment and monitoring responsibilities.
- Individuals with information security implementation and operational responsibilities.

Characteristics of RMF-Based Process

(1 of 3)

- Promotes near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes.
- Integrates information security more closely into the enterprise architecture and system development life cycle.
- Provides equal emphasis on the security control selection, implementation, assessment, and monitoring, and the authorization of information systems.

Characteristics of RMF-Based Process

(2 of 3)

- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems.

Characteristics of RMF-Based Process

(3 of 3)

- Encourages the use of automation to:
 - Increase consistency, effectiveness, and timeliness of security control implementation and functionality; and
 - Provide senior leaders the necessary information to take credible, risk-based decisions with regard to the information systems supporting their core missions and business functions.

The Fundamentals

Mainstreaming 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

(1 of 2)

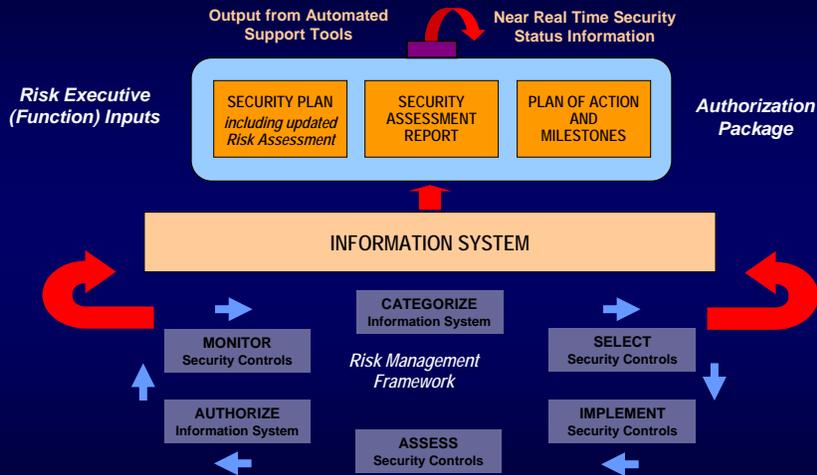
- RMF steps are carried out within the five phases of the SDLC.
 - System Initiation Phase
 - System Development / Acquisition Phase
 - System Implementation Phase
 - System Operation / Maintenance Phase
 - System Disposal Phase
- Flexibility on types of SDLC models employed by the organization (e.g., spiral, waterfall, agile development).

System Development Life Cycle

(2 of 2)

- Integrating information security requirements into the SDLC provides the most efficient and cost-effective method for an organization to ensure that:
 - Cost, schedule, and performance requirements are satisfied.
 - Missions and business operations supported by the information system are adequately protected.
 - Security-related activities are carried out as early as possible and not repeated unnecessarily.
 - Risk management activities are not isolated or decoupled from the management processes employed to develop, implement, operate, and maintain the information system.

Applying the Risk Management Framework to Information Systems



Information System Boundaries

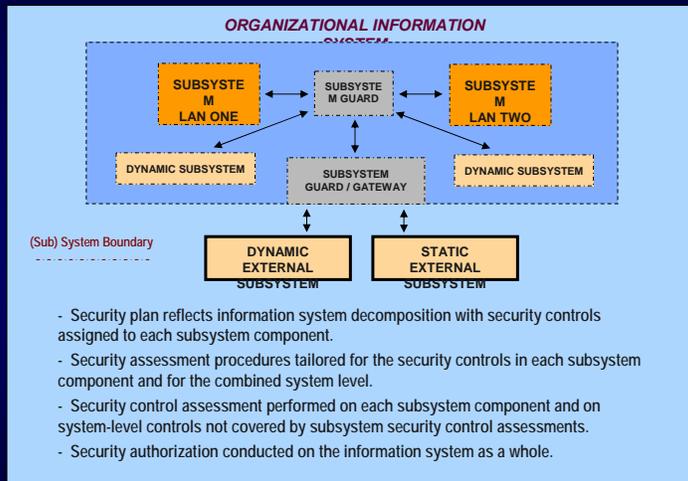
- Define the scope of protection for information systems (i.e., what the organization agrees to protect under its direct control or within the scope of its responsibilities).
- Include the people, processes, and technologies that are part of the systems supporting the organization's missions and business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

Large and Complex Systems

- From a centralized development, implementation, and operations perspective—
 - The organization examines the purpose of the information system and considers the feasibility of decomposing the complex system into more manageable components, or *subsystems*.
- From a distributed development, implementation, and operations perspective—
 - The organization recognizes that multiple entities, possibly operating under different policies, may be contributing to the development, implementation, and/or operations of the subsystems that comprise the overall information system.

Large and Complex Systems

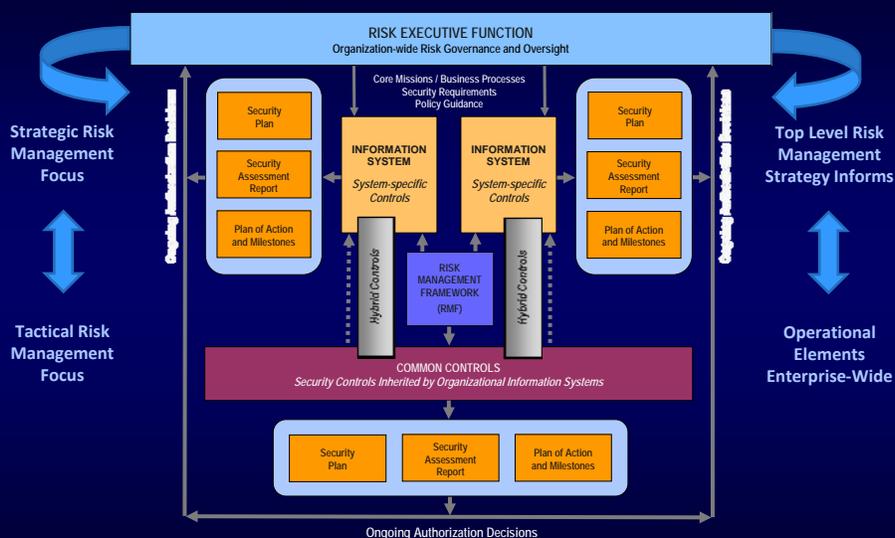
(Including System of Systems)



Security Control Allocation

- Security controls are defined to be *system-specific*, *hybrid*, or *common*.
- Security controls are *allocated* to specific components of organizational information systems as system-specific, hybrid, or common controls.
- Security control allocations are consistent with the organization's *enterprise architecture* and *information security architecture*.

Security Control Accountability



The Process

RMF Task Structure

(1 of 2)

- Task Section
 - *Describes the specific RMF 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

(2 of 2)

- 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 NIST security standards and guidelines that should be consulted for additional information with regard to executing the RMF task.*
 - *Provides specific national security system references to CNSS policies and instructions that should be consulted for additional information with regard to executing the RMF task when the general references are either insufficient or inappropriate for national security application.*

RMF Step 1 Tasks

Categorize Information System

- Security Categorization
 - **Task 1-1:** *Categorize the information system and document the results of the security categorization in the security plan.*
- Information System Description
 - **Task 1-2:** *Describe the information system (including system boundary) and document the description in the security plan.*
- Information System Registration
 - **Task 1-3:** *Register the information system with appropriate organizational program/management offices.*

Milestone Checkpoint #1

- Has the organization completed a *security categorization* of the information system including the information to be processed, stored, and transmitted by the system?
- Are the results of the security categorization process for the information system consistent with the organization's *enterprise architecture* and commitment to protecting organizational *mission/business processes*?
- Do the results of the security categorization process reflect the organization's *risk management strategy*?
- Has the organization adequately described the *characteristics* of the information system?
- Has the organization *registered* the information system for purposes of management, accountability, and oversight?

RMF Step 2 Tasks

Select Security Controls

- **Common Control Identification**
 - *Task 2-1: Identify the security controls that are provided by the organization as common controls for organizational information systems 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.*
- **Monitoring Strategy**
 - *Task 2-3: 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.*
- **Security Plan Approval**
 - *Task 2-4: Review and approve the security plan.*

Milestone Checkpoint #2

(1 of 3)

- Has the organization allocated all security controls to the *information system* as system-specific, hybrid, or common controls?
- Has the organization used its *risk assessment* (either formal or informal) to inform and guide the security control selection process?
- Has the organization identified *authorizing officials* for the information system and all common controls inherited by the system?
- Has the organization *tailored* and *supplemented* the baseline security controls to ensure that the controls, if implemented, adequately mitigate risks to organizational operations and assets, individuals, other organizations, and the Nation?

Milestone Checkpoint #2

(2 of 3)

- Has the organization addressed *minimum assurance requirements* for the security controls employed within and inherited by the information system?
- Has the organization consulted information system owners when identifying common controls to ensure that the security capability provided by the *inherited* controls is sufficient to deliver adequate protection?
- Has the organization *supplemented* the *common controls* with system-specific or hybrid controls when the security control baselines of the common controls are less than those of the information system inheriting the controls?
- Has the organization *documented* the common controls inherited from external providers?

Milestone Checkpoint #2

(3 of 3)

- Has the organization developed a *continuous monitoring strategy* for the information system that reflects the organizational risk management strategy and commitment to protecting critical missions and business functions?
- Have appropriate organizational officials *approved* security plans containing system-specific, hybrid, and common controls?

RMF Step 3 Tasks

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).*

Milestone Checkpoint #3

(1 of 2)

- Has the organization *allocated* security controls as system-specific, hybrid, or common controls consistent with the enterprise architecture and information security architecture?
- Has the organization demonstrated the use of sound *information system and security engineering methodologies* in integrating information technology products into the information system and in implementing the security controls contained in the security plan?
- Has the organization documented how *common controls* inherited by organizational information systems have been implemented?

Milestone Checkpoint #3

(2 of 2)

- Has the organization documented how *system-specific* and *hybrid* security controls have been implemented within the information system taking into account specific technologies and platform dependencies?
- Has the organization taken into account the *minimum assurance requirements* when implementing security controls?

RMF Step 4 Tasks

Assess Security Controls

- 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.*
- Remediation Actions
 - **Task 4-4:** *Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate..*

Milestone Checkpoint #4

(1 of 2)

- Has the organization developed a comprehensive *plan* to assess the security controls employed within or inherited by the information system?
- Was the assessment plan *reviewed* and *approved* by appropriate organizational officials?
- Has the organization considered the appropriate level of assessor *independence* for the security control assessment?
- Has the organization provided all of the essential supporting *assessment-related materials* needed by the assessor(s) to conduct an effective security control assessment?
- Has the organization examined opportunities for *reusing assessment results* from previous assessments or from other sources?

Milestone Checkpoint #4

(2 of 2)

- Did the assessor(s) complete the *security control assessment* in accordance with the stated assessment plan?
- Did the organization receive the completed *security assessment report* with appropriate findings and recommendations from the assessors)?
- Did the organization take the necessary *remediation actions* to address the most important weaknesses and deficiencies in the information system and its environment of operation based on the findings and recommendations in the security assessment report?
- Did the organization update appropriate *security plans* based on the findings and recommendations in the security assessment report and any subsequent changes to the information system and its environment of operation?

RMF Step 5 Tasks

Authorize Information System

- **Plan of Action and Milestones**
 - *Task 5-1: 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 5-2: Assemble the security authorization package and submit the package to the authorizing official for adjudication.*
- **Risk Determination**
 - *Task 5-3: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.*
- **Risk Acceptance**
 - *Task 5-4: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.*

Milestone Checkpoint #5

(1 of 2)

- Did the organization take the necessary *remediation actions* to address the most important weaknesses and deficiencies in the information system and its environment of operation based on the findings and recommendations in the security assessment report?
- Did the organization develop an appropriate *authorization package* with all key documents including the security plan, security assessment report, and plan of action and milestones (if applicable)?

Milestone Checkpoint #5

(2 of 2)

- Did the final *risk determination* and *risk acceptance* by the authorizing official reflect the risk management strategy developed by the organization and conveyed by the risk executive (function)?
- Was the *authorization decision* conveyed to appropriate organizational personnel including information system owners and common control providers?

RMF Step 6 Tasks

Monitor Security Controls

- **Information System and Environment Changes**
 - **Task 6-1:** Determine the security impact of proposed or actual changes to the information system and its environment of operation.
- **Ongoing Security Control Assessments**
 - **Task 6-2:** Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.
- **Ongoing Remediation Actions**
 - **Task 6-3:** Conduct selected remediation actions based on the results of ongoing monitoring activities, assessment of risk, and the outstanding items in the plan of action and milestones.
- **Key Updates**
 - **Task 6-4:** Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

RMF Step 6 Tasks

Monitor Security Controls

- **Security Status Reporting**
 - **Task 6-5:** Report the security status of the information 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.
- **Ongoing Risk Determination and Acceptance**
 - **Task 6-6:** Review the reported security status of the information 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.
- **Information System Removal and Decommissioning**
 - **Task 6-7:** Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

Milestone Checkpoint #6

(1 of 2)

- Is the organization effectively monitoring changes to the *information system* and its *environment of operation* including the effectiveness of deployed *security controls* in accordance with the continuous monitoring strategy?
- Is the organization effectively analyzing the *security impacts* of identified changes to the information system and its environment of operation?
- Is the organization conducting *ongoing assessments of security controls* in accordance with the monitoring strategy?
- Is the organization taking the necessary *remediation actions* on an ongoing basis to address identified weaknesses and deficiencies in the information system and its environment of operation?

Milestone Checkpoint #6

(2 of 2)

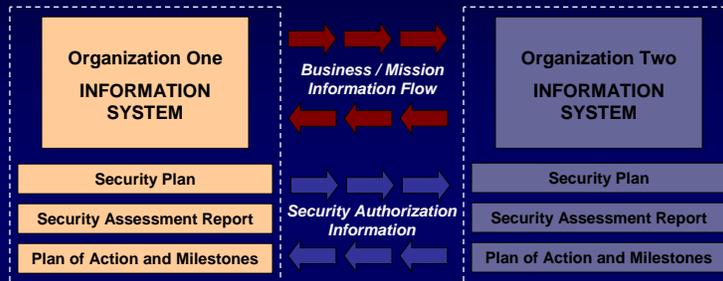
- Does the organization have an effective process in place to report the *security status* of the information system and its environment of operation to the authorizing officials and other designated senior leaders within the organization on an ongoing basis?
- Is the organization updating critical *risk management documents* based on ongoing monitoring activities?
- Are authorizing officials conducting *ongoing security authorizations* by employing effective continuous monitoring activities and communicating updated risk determination and acceptance decisions to information system owners and common control providers?

Summary

Supporting Appendices

- References
- Glossary
- Acronyms
- Roles and Responsibilities
- Summary of RMF Tasks
- Security Authorization
- Continuous Monitoring
- Operational Scenarios
- Security Controls in External Environments

Recognition of Authorization Results



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 authorization 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

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

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

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov