RMF Select Step
Student Guide

May 2023

Center for Development of Security Excellence

Table of Contents

Course Introduction

Introduction

Welcome to the Risk Management Framework, or RMF, Select Step.

This course focuses on the Select Step, and by the end of the course, you will be able to define the Select Step in the RMF.

The purpose of the Select Step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation.

Objectives

Before you begin, consider the following course learning objectives.

- Describe the purpose of the Select Step in the RMF
- Identify tasks, inputs and outputs, roles and responsibilities within the Select Step.

Lessons:

The course is divided into two lessons:

Lesson 1: RMF Select Step: Policies and Guidelines

Lesson 2: Select Step Tasks, Inputs & Outputs, Roles and Responsibilities

Lesson 1: Introduction to Policies and Guidelines

Lesson Introduction

The RMF was developed as a result of a partnership between the National Institute of Standards and Technology, or NIST, the Department of Defense, or DOD, the Office of the Director of National Intelligence, or ODNI, and the Committee on National Security Systems.

In this lesson, you will learn the defining aspects of the Select Step, and the associated policies and guidelines.

The purpose of **NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System** is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations such as mission, functions, image, and reputation, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems.

NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, contains updates to the RMF, such as the integration of privacy risk management processes and the incorporation of supply chain risk management processes.

NIST Special Publication 800-30, Guidance for Conducting Risk Assessments, provides guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39.

This policy provides guidance for carrying out each of the steps in the Risk Assessment Process, such as preparing for the assessment, conducting the assessment, and communicating the results of the assessment.

DODI 8510.01, Risk Management Framework for DOD Systems establishes the use of the RMF, an integrated, enterprise-wide decision structure for cybersecurity risk management that includes and integrates DOD mission areas, or MAs, in accordance with DODD 8115.01(Information Technology Portfolio management)

Committee on National Security Systems Instruction (CNSSI) 1253: Security Categorization and Control Selection for National Security Systems, describes the process of the categorization process.

The *CNSSI No. 1253* is a companion document to the NIST publications relevant to the categorization step. The CNSSI collaborates with NIST to ensure NIST SP 800-53 contains security controls to meet the requirements of National Security Systems (NSS)

and provides a common foundation for information security across the U.S. Federal Government.

The NIST Special publication (SP) 800-53B, Control Baselines for Information Systems and Organizations, provides security and privacy control baselines for the Federal Government.

This publication also includes a new privacy baseline, aimed at "addressing and managing privacy risks that arise from processing PII based on privacy program responsibilities under OMB Circular A-130."

This instruction also provides NSS-specific information on developing and applying overlays for the national security community and parameter values for NIST SP 800-53 security controls that are applicable to all.

NIST Special Publication 800-60 Volume 1 Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories contains the basic guidelines for mapping types of information and information systems to security categories.

The 800-60 Volume 1 Revision 1 addresses the Federal Information Security Modernization Act, FISMA, direction to develop guidelines recommending the types of information and information systems to be included in each category of potential security impact. This guideline is intended to help agencies consistently map security impact levels to types of information and information systems

The NIST SP 800-60 Volume 2, Revision 1; this document is a reference resource rather than a tutorial. The document discusses information attributes that may result in variances from the provisional security impact level assignment. Describes how to establish a system security categorization based on the system's use, connectivity, and aggregate information content.

Federal Information Processing Standards (FIPS) Publication 199 outlines the **Standards for Security Categorization of Federal Information and Information Systems.** This document identifies the purpose of the Select Step. It requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.

The document provides guidance for the potential impact values assigned to the respective security objectives and are the highest values from among the security categories that have been determined for each type of information resident on those information systems.

FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems is the second of the mandatory security standards. The publication identifies the purpose of the Select Step. It specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal

Government. It identifies the risk-based process for selecting the Security Controls necessary to satisfy the minimum-security requirements.

Review Activity

Knowledge Check

The purpose of the Select Step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation.

- True
- False

Lesson 1 Conclusion

Lesson Conclusion

You have completed this lesson. You should now be able to define Policy and Guidelines associated with the Select Step.

Lesson 2: Tasks, Inputs, Outputs, Roles and Responsibilities

Introduction of Tasks

In this lesson, we will look at the Tasks, Inputs and Outputs, Roles and Responsibilities outlined in the Select Step. The Select Step includes six tasks, which have an alpha designator of **"S"** preceding the task number.

- S-1: Control Selection
- S-2: Control Tailoring
- S-3: Control Allocation
- S-4: Documentation of Planned Control Implementations
- S-5: Continues Monitoring Strategy-System
- S-6: Plan Review and Approval

Each task contains a set of inputs that are required to implement the tasks and a set of outputs as a result.

The first Select Task to be discussed is Task S-1

Task S-1: Control Selection

Task S-1 is the first of the six tasks in the Select Step. This task allows the selection of controls for the system and the environment of operation.

- Control baselines are necessary to protect the system commensurate with risk.
- Controls are selected for the system and the environment of operation.
- There are two approaches for the initial selection of controls:

    - A baseline control selection approach
    - An organization-generated control selection approach

The baseline control selection approach uses control baselines, which are pre-defined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. The CNSSI 1253 Appendix D is the National Security System (NSS) Security Control baseline.

The organization-generated control selection approach differs from the baseline selection approach because the organization does not start with a pre-defined set of controls. Rather, the organization uses its own selection process to select controls.

Regardless, in both the baseline control selection approach and organization-generated control selection approach, organizations develop a well-defined set of security and privacy requirements using a life cycle-based systems engineering process.

Task S-1 Potential Inputs

Task S-1 Inputs include:

- Security categorization
- Organization-and system- level risk assessment results
- System element information
- System component inventory
- List of security and privacy requirements allocated to the system, system elements, and environment of operation
- List of contractual requirements allocated to external providers of the system or system element
- Business impact analysis or criticality analysis
- Risk management strategy
- Organizational security and privacy policy
- Federal or organization-approved or mandated baselines or overlays and
- Cybersecurity Framework Profiles

Task S-1 Expected Outputs

The expected output for Task S-1 include the controls selected for the system and environment of operation.

Task S-1 Roles and Responsibilities

The primary responsibility for Task S-1 is carried out by the ***System Owner*** and the ***Common Control*** **provider.**

The System Owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner is responsible for addressing the operational interests of the user community.

The Common Control Provider is an individual, group, or organization that is responsible for the implementation, assessment, and monitoring of common controls.

The supporting roles for Task S-1 include the:

- Authorizing Official or Authorizing Official Designated Representative
- Information Owner or Steward
- System Security Engineer
- Privacy Engineer

- System Security Officer, and the
- System Privacy Officer

Review Activity

Knowledge Check S-1

Try answering this question.

Privacy programs use security and privacy control baselines to manage the privacy risks arising from unauthorized system activity or behavior, as well as from authorized activities.

- True
- False

Task S-2: Control Tailoring

Task S-2 Tailor the controls selected for the system and the environment of operation.

- After selecting the applicable control baselines, organizations tailor the controls based on various factors. For example, missions or business functions, threats, security and privacy risks, including supply chain risks, type of system, or risk tolerance.
- Organizations determine the amount of detail to include in justifications or supporting rationale required for tailoring decisions. For example, the justification or supporting rationale for scoping decisions related to a high-impact system or high value asset may necessitate greater specificity than similar decisions for a low-impact system.
- Organizations use risk assessments to inform and guide the tailoring process. Threat information from security risk assessments provides information on adversary capabilities, intent, and targeting that may affect organizational decisions regarding the selection of security controls, including the associated costs and benefits.
- Privacy risk assessments, including the contextual factors therein, will also influence tailoring when an information system processes Personal Identifiable Information PII.

Task S-2 Potential Inputs

To complete Task S-2, inputs include:

- Initial control baselines
- Organization - and system-level risk assessment results
- System element information
- System component inventory

- List of security and privacy requirements allocated to the system, system elements, and environment of operation
- Business impact analysis or criticality analysis
- Risk management strategy
- Organizational security and privacy policies
- Federal or organization-approved or mandated overlays

Task S-2 Expected Outputs

The Expected Outputs from Task-2 include:

- The List of tailored controls for the system and environment of operation, such as, tailored control baselines.

Task S-2 Roles and Responsibilities

Task S-2 Primary Responsibility is carried out by the System Owner and the Common Control Provider.

The System Owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner is responsible for addressing the operational interests of the user community.

The Common Control Provider is an individual, group, or organization that is responsible for the implementation, assessment, and monitoring of common controls.

The supporting roles for Task S-2 include the:

- Authorizing Official or Authorizing Official Designated Representative
- Information Owner or Steward
- Systems Security Engineer
- Privacy Engineer
- System Security Officer, and
- System Privacy Officer

Review Activity

Knowledge Check S-2

How many tasks are there in the entire Select Step within the Risk Management Framework?

- 7
- 5

- 6
- 1

Task S-3: Control Allocation

The task description is to allocate security and privacy controls to the system and to the environment of operation.

The organization designates controls as;

System-specific, hybrid, or common, and allocates the controls to the system elements, such as machine, physical, or human elements responsible for providing a security or privacy capability.

Controls are allocated to a system or an organization consistent with the organization's enterprise architecture and security or privacy architecture and the allocated security and privacy requirements. Not all controls need to be allocated to every system element. Controls providing a specific security or privacy capability are only allocated to system elements that require that capability.

Security and privacy requirements allocated to the system, system elements, and the environment of operation guide and inform control allocation to system elements.

Common controls that are made available by the organization during the RMF Prepare-Organization Level step are selected for inheritance; hybrid controls are also selected.

- Common controls satisfy security and privacy requirements allocated to the organization and provide a protection capability that is inherited by one or more systems.
- Hybrid controls satisfy security and privacy requirements allocated to the system and to the organization and provide a protection capability that is partially inherited by one or more systems.
- System-specific controls satisfy security and privacy requirements allocated to the system and provide a protection capability for that system. Controls can be allocated to specific system elements rather than to every element within a system.

Task S-3 Potential Inputs

To complete Task S-3, inputs include:

- Security categorization
- Organization- and system-level risk assessment results
- Organizational policy on system registration
- Enterprise architecture

- Security and privacy architectures
- Security and privacy requirements
- List of security and privacy requirements allocated to the system, system elements, and the environment of operation
- List of common control providers and common controls available for inheritance
- System description
- System element information
- System component inventory
- Relevant laws, executive orders, directives, regulations, and policies.

Task S-3 Expected Outputs

The Expected Outputs for Task S-3 include:

A List of security and privacy controls allocated to the system, system elements, and the environment of operation.

Task S-3 Roles and Responsibilities

Task S-3 Primary Responsibility is carried out by the Security Architect, the Privacy Architect, the System Security Officer and the System Privacy Officer.

The Security or Privacy Architect is an individual, group, or organization responsible for ensuring that stakeholder protection needs and the corresponding system requirements necessary to protect organizational missions and business functions and individuals' privacy are adequately addressed in the enterprise architecture. This includes reference models, segment architectures, and solution architectures, such as systems supporting mission and business processes.

The System Security or Privacy Officer is an individual responsible for ensuring that the security and privacy posture is maintained for an organizational system. They work in close collaboration with the system owner and serve as a principal advisor on all matters, technical and otherwise, involving the controls for the system.

The Supporting Roles include the:

- The Authorizing Official or Authorizing Official Designated Representative
- The Chief Information Officer
- The Mission or Business Owner
- The Senior Agency Information Security Officer
- The Senior Agency Official for Privacy, and
- The System Owner

Review Activity

Knowledge Check S-3

Select all that apply: List the three types of control designations:

- System-specific
- Hybrid
- Common
- Privacy

Task S-4: Documentation of Planned Control Implementations

Task S-4: Document the controls for the system and environment of operation in security and privacy plans.

Security and privacy plans contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements.

The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control.

Organizations may develop a consolidated plan that incorporates security and privacy plans or maintain separate plans. If developing a consolidated plan, privacy programs collaborate with security programs to ensure that the plan reflects the selection of controls that provide protections with respect to managing the confidentiality, integrity, and availability of PII; and delineates roles and responsibilities for control implementation, assessment, and monitoring.

For separate system security plans and privacy plans, organizations cross-reference the controls in all plans to help maintain accountability and awareness.

Documentation of planned control implementations allows for the traceability of decisions prior to and after the deployment of the system. To the extent possible, organizations reference existing documentation either by vendors or other organizations that have employed the same or similar systems or system elements, use automated support tools, and coordinate across the organization to reduce redundancy and increase the efficiency and cost-effectiveness of control documentation.

For controls that are mechanism-based, organizations take advantage of the functional specifications provided by or obtainable from manufacturers, vendors, and systems integrators. This includes any documentation that may assist the organization during the development, implementation, assessment, and monitoring of controls.

Task S-4 Potential Inputs

To complete Task S-4 inputs, include:

- Security categorization
- Organization- and system-level risk assessment results
- System element information
- System component inventory
- Business impact or criticality analysis
- List of security and privacy requirements
- Risk management strategy
- List of selected controls
- Organizational security, privacy,
- The Supply Chain Risk management SCRM policies.

Task S-4 Expected Outputs

The Expected Outputs for Task S-4 include: The Security and privacy plans for the system.

Task S-4 Roles and Responsibilities

Task S-4 Primary Responsibilities are carried out by the System Owner and the Common Control Provider.

The ***system owner*** is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner is responsible for addressing the operational interests of the user community.

The ***common control provider*** is an individual, group, or organization that is responsible for the implementation, assessment, and monitoring of common controls.

The supporting Roles for Task S-4 include:

- Authorizing Official or Authorizing Official Designated Representative
- Information Owner or Steward
- Systems Security Engineer
- Privacy Engineer
- System Security Officer and the
- System privacy officer

Review Activity

Knowledge Check S-4

Try answering this question.

"Security Categorization" is a valid input for Task S-4: Document the controls for the system and environment of operation in security and privacy plans.

- True
- False

Task S-5: Continuous Monitoring Strategy – System

Task S-5: Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy.

An important aspect of risk management is the ongoing monitoring of controls implemented within or inherited by an information system. An effective continuous monitoring strategy at the system level is developed and implemented in coordination with the organizational continuous monitoring strategy early in the System Development Life Cycle (SDLC), such as, during initial system design or procurement decision. The system-level continuous monitoring strategy is consistent with and supplements the continuous monitoring strategy for the organization.

For controls that are not addressed by the organizational continuous monitoring strategy, the system-level continuous monitoring strategy identifies the criteria for determining the frequency with which controls are monitored post-implementation and the plan for the ongoing assessment of those controls. The criteria are established by the system owner or common control provider in collaboration with other organizational officials, for example, the authorizing official or designated representative; senior accountable official for risk management or risk executive function; senior agency information security officer; senior agency official for privacy; and chief information officer.

The frequency criteria at the system level reflect ***organizational priorities*** and the importance of the system to the organization's operations and assets, individuals, other organizations, and the Nation.

The Authorizing Official or ***Designated Representative*** approves:

The continuous monitoring strategy and the minimum frequency with which each control is to be monitored.

The approval of the strategy can be obtained in conjunction with The Security and Privacy Plan approval. The monitoring of controls begins at the start of the operational phase of the SDLC and continues through the disposal phase.

Task S-5 Potential Inputs

Potential Inputs for Task S- 5 include;

- Organizational risk management strategy
- Organizational continuous monitoring strategy
- Organization- and system-level risk assessment results
- Security and privacy plans
- Organizational security and privacy policies

Task S-5 Expected Outputs

The Expected Outputs for Task S-5 include a Continuous monitoring strategy for the system including time-based trigger for ongoing authorization

Task S-5 Roles and Responsibilities

The primary responsibility for Task S-5 is carried out by *the System Owner* and the *Common Control Provider.*

The ***system owner*** is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner is responsible for addressing the operational interests of the user community

The ***common control provider*** is an individual, group, or organization that is responsible for the implementation, assessment, and monitoring of common controls.

Supporting roles for Task S-5 include:

- Senior Accountable Official for Risk Management or Risk Executive (Function)
- Chief Information Officer
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy
- Authorizing Official or Authorizing Official Designated Representative
- Information Owner or Steward
- Security Architect
- Privacy Architect
- Systems Security Engineer
- Privacy Engineer
- System Security Officer and the
- System Privacy Officer

Review Activity

Knowledge Check S-5

Try answering this question.

System level continuous monitoring strategy identifies criteria for those controls not addressed by the _____ level:

- Risk
- Organizational
- Security
- implementation

Task S-6: Plan Review and Approval

Task S-6: Review and approve the security and privacy plans for the system and the environment of operation.

The security and privacy plan review are conducted by the authorizing official or designated representative with support from the senior accountable official for risk management or risk executive (function), chief information officer, senior agency information security officer, and senior agency official for privacy. The security and privacy plan review determines if the plans are complete, consistent, and satisfy the stated security and privacy requirements for the system. Based on the results from this review, the authorizing official or designated representative may recommend changes to the security and privacy plans. If the plans are unacceptable, the system owner or common control provider makes appropriate changes to the plans. If the plans are acceptable, the authorizing official or designated representative approves the plans.

The acceptance of the security and privacy plans represents an important milestone in the SDLC and risk management process. The authorizing official or designated representative, by approving the plans, agrees to the set of controls, such as, system-specific, hybrid, or common controls, and the description of the proposed implementation of the controls to meet the security and privacy requirements for the system and the environment in which the system operates.

The approval of the plans allows the risk management process to proceed to the RMF Implement step. The approval of the plans also establishes the level of effort required to successfully complete the remainder of the RMF steps and provides the basis of the security and privacy specifications for the acquisition of the system or individual system elements.

Task S-6 Potential Inputs

Potential Inputs to complete Task S-6, include:

- Security and privacy plans
- organization- and system-level risk assessment results

Task S-6 Expected Outputs

The Expected Outputs from Task S-6 include:

The Security and privacy plans approved by the authorizing official.

Task S-6 Roles and Responsibilities

The primary responsibility for Task S-6 is carried out by the ***Authorizing Official*** and the ***Authorizing Official Designated Representative***.

The authorizing official is a senior official or executive with the authority to formally assume responsibility and accountability for operating a system; providing common controls inherited by organizational systems; or using a system, service, or application from an external provider.

The authorizing official designated representative is an organizational official designated by the authorizing official who is empowered to act on behalf of the authorizing official to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations. This includes carrying out many of the activities related to the execution of the RMF. The only activity that cannot be delegated by the authorizing official to the designated representative is the authorization decision and signing of the associated authorization decision document, such as, the acceptance of risk.

The supporting roles include:

- Senior Accountable Official for Risk Management or Risk Executive Function
- Chief Information Officer
- Chief Acquisition Officer
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy.

Review Activity

Knowledge Check S-6

Try answering this question.

The acceptance of the security and privacy plans represents an important milestone in the SDLC and _____ process:

- Risk Management

- Approval
- Security
- implementation

You have completed the Select Step Task, Input and Outputs, Roles and Responsibilities Lesson.

Course Conclusion

Conclusion

Congratulations on completing Risk Management Framework (RMF) Select Step course. You should now be able to perform all the listed activities:

Course Learning Objectives:

- Describe the purpose of the Select Step in the RMF
- Identify tasks, inputs and outputs, roles and responsibilities within the Select Step.

For more information on the RMF Select Step, please visit the Course Resources link. To receive credit for this course, you must take the course examination.

Appendix A: Answer Key

Lesson 1: Review Activity

Knowledge Check – Policies and Guidelines

The purpose of the Select Step is to Select, tailor, and document the controls necessary to protect the information commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation.

☒ True
☐ False

Feedback: *The purpose of the **Select** Step is to Select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation.*

Lesson 2: Review Activity

Knowledge Check S-1

Privacy programs use security and privacy control baselines to manage the privacy risks arising from both unauthorized system activity and behavior, as well as from authorized

activities.

☒ True

☐ False

Feedback: *Privacy programs use security and privacy control baselines to manage the privacy risks arising from both unauthorized system activity and behavior, as well as from authorized activities.*

Knowledge Check S-2

How many tasks are there in the entire Select Step within the Risk Management Framework?

☐ 7

☐ 5

☒ 6

☐ 1

Feedback: *There are 6 tasks in the Select Step within the Risk Management Framework.*

Knowledge Check S-3

Select all that apply: List the three types of control designations:

☐ System-specific

☒ Hybrid

☒ Common

☐ Privacy

Feedback: *The three types of control designations: System-specific, Hybrid, and Common*

Knowledge Check S-4

“Security Categorization” is a valid input for Task S-4: Document the controls for the system and environment of operation in security and privacy plans.

☒ True

☐ False

Feedback*: “Security Categorization” is a valid input for Task S-4: Document the controls for the system and environment of operation in security and privacy plans.*

Knowledge Check S-5

System level continuous monitoring strategy identifies criteria for those controls not addressed by the _____ level:

☐ Risk
☒ Organizational
☐ Security
☐ Implementation

Feedback: *System level continuous monitoring strategy identifies criteria for those controls not addressed by the organizational level.*

Knowledge Check S-6

The acceptance of the security and privacy plans represents an important milestone in the SDLC and _____ process:

☒ Risk Management
☐ Approval
☐ Security
☐ Implementation

***Feedback**: The acceptance of the security and privacy plans represents an important milestone in the SDLC and risk management process.*