RMF Prepare Step

Student Guide

April 2022

Center for Development of Security Excellence

Table of Contents

Course Introduction

Introduction

Introduction

The Risk Management Framework, or RMF, provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. Managing organizational risk is paramount to effective information security and privacy programs. The RMF can be applied to any type of system or technology and within any type of organization regardless of size or sector.

In this course, you will gain an understanding of the new and updated policy regarding the RMF. This includes information regarding the RMF Prepare Step, Tasks, Potential Inputs, Expected Outputs and roles and responsibilities.

Key Topics:

- Defining RMF
- RMF policies
- RMF Prepare Step
- Tasks, Potential Inputs, and Expected Outputs
- Roles and Responsibilities

Lessons and Objectives

The course is divided into three lessons: RMF Prepare Step; Prepare Step Tasks, Potential Inputs & Expected Outputs; and Prepare Step Roles and Responsibilities.

Before we begin, consider the following course learning objectives.

Course Learning Objectives:

- Describe the purpose of the Prepare Step in the Risk Management Framework (RMF)
- Identify tasks, potential inputs, and expected outputs within the Prepare Step
- Identify roles and responsibilities in the Prepare Step

Lesson 1: RMF Prepare Step

Lesson Introduction

Lesson Introduction

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

Please take a moment to review the lesson learning objectives.

- Define Risk Management Framework
- Identify policies and guidelines for the Prepare Step in the RMF

Defining the RMF

Defining the RMF

The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.

The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels.

Execution of the RMF and its associated tasks links essential risk management processes at the system level to risk management processes at the organization level.

In addition, it establishes responsibility and accountability for the controls implemented within an organization's information systems and the controls inherited by those systems.

Seven-Step Process

The RMF Process comprises seven sequential steps. This includes the Prepare Step, Categorize Step, Select Step, Implement Step, Assess Step, Authorize Step, and Monitor Step. The organization requesting authorization or various personnel will execute each step according to its associated tasks.

Personnel could include the Information System Owner, or ISO, and Key Management Personnel.

Risk Management Framework (RMF) Prepare Step

Risk Management Framework (RMF) Prepare Step

This course focuses on the Prepare Step, which is the first of the RMF process. This means that Prepare Step tasks are to be completed by the organization before the Categorize Step and support all subsequent RMF steps.

The addition of the Prepare Step is one of the key changes to the RMF—incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes.

The purpose of the Prepare Step is to carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the RMF.

The intention is to provide the information and resources necessary to manage information security and privacy risk to the organization.

Screen text:

Prepare step is implemented to help security and privacy risk management processes to become:

- Effective
- Efficient
- Cost-effective

Policies and Guidelines

RMF Policies

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.

Policies pertaining to the RMF include NIST Special Publication 800-137, Information Security Continuous Monitoring, or ISCM, for Federal Information Systems and Organizations; NIST Special Publication 800-30, Guide for Conducting Risk Assessments; NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy; NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View; and DODI 8510.01, Risk Management Framework, or RMF, for DOD Information Technology, or IT.

Let’s have a brief overview of each policy.

RMF Policies (cont.)

The guideline, NIST Special Publication 800-137, is intended to assist organizations in the development of an information security continuous monitoring, or ISCM, strategy and the implementation of an ISCM program. The program provides awareness of vulnerability, visibility of assets, and effectiveness of security control.

NIST Special Publication 800-30 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.

NIST Special Publication 800-37 Revision 2, contains updates to the RMF, such as the integration of privacy risk management processes and the incorporation of supply chain risk management processes. Revision 2 also includes a set of organization- and system-level tasks that are designed to prepare information system owners to conduct system-level risk management activities.

The purpose of NIST Special Publication 800-39 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. Special Publication 800-39 provides a structured yet flexible approach for managing risk.

DODI 8510.01 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 and DODI 8510.01.

Screen text:

DODD 8115.01, Information Technology Portfolio Management

Review Activity

Knowledge Check 1

Before we conclude the lesson, try answering this question.

Which of the following correctly describes the Risk Management Framework (RMF)?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ A process for managing security and privacy risk
- ○ A security program that supports all DOD activities
- ○ A subfield of the federal government designed to provide security guidelines
- ○ A process for supporting all security efforts for the DOD

Knowledge Check 2

Now try this question.

Which of the following policies establishes the RMF as an integrated enterprise-wide decision structure for cybersecurity risk management?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- ○ DODI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT)
- ○ NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- ○ DODI 8500.01 Cybersecurity

Lesson Conclusion

Lesson Conclusion

You have completed the RMF Prepare Step lesson.

Lesson 2: Prepare Step Tasks, Potential Inputs, and Expected Outputs

Introduction

Objectives

In this lesson, you will learn about the tasks, potential inputs, and expected outputs associated with the Prepare Step.

Take a moment to review the lesson learning objectives

- Describe organization-level and system-level tasks in the Prepare Step.
- Describe potential inputs and expected outputs associated with tasks in the Prepare Step.

Prepare Step

Prepare Step Objectives

The Prepare Step includes 18 tasks which have an alpha designator of "P" preceding the task number.

For example, the first Prepare task will be Task P-1.

These tasks are divided in two categories: Organization-level and System-level.

The main objectives for institutionalizing these tasks are as follows:

- To facilitate effective communication between senior leaders and executives at the organization and mission and business process levels and system owners at the operational level.
- To facilitate organization-wide identification of common controls and the development of organizationally- tailored control baselines, reducing the workload on individual system owners and the cost of system development and asset protection.
- To reduce the complexity of the information technology, or IT, and operations technology, or OT, infrastructure using Enterprise Architecture concepts and models to consolidate, optimize, and standardize organizational systems, applications, and services.
- To reduce the complexity of systems by eliminating unnecessary functions and security and privacy capabilities that do not address security and privacy risk and
- To identify, prioritize, and focus resources on the organization's high value assets, or HVA, that require increased levels of protection—taking measures commensurate with the risk to such assets.

The aforementioned objectives allow organizations to simplify RMF execution, employ innovative approaches for managing risk, and increase the level of automation when carrying out certain tasks.

Furthermore, organizations who implement the RMF will be able to use the tasks and outputs of the Organization-Level and System-Level Prepare step to promote a consistent starting point within organizations to execute the RMF.

Other outcomes include maximizing the use of common controls and automated tools; decreasing the level of effort for low-impact systems if those systems cannot adversely affect higher-impact systems; and employing organizationally-tailored control baselines to increase the speed of security and privacy plan development and the consistency of security and privacy plan content.

Organization-Level Tasks

Organization-Level Tasks

The organization that requests the authorization is responsible for implementing the organization-level tasks.

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

Within the organization-level, there are seven tasks:

- Task P-1, Risk Management Roles
- Task P-2, Risk Management Strategy
- Task P-3, Risk Assessment – Organization
- Task P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles
- Task P-5, Common Control Identification
- Task P-6, Impact-Level Prioritization, and
- Task P-7, Continuous Monitoring Strategy—Organization.

Let's review the potential inputs and expected outputs of P-1 through P-7.

Review each task to learn more.

Task P-1, Risk Management Roles

Task P-1, Risk Management Roles, identifies and assigns individuals to specific roles associated with security and privacy risk management.

Organizations ensure there are no conflicts of interest when assigning multiple risk management roles. For example, an Authorizing Official, or AO, cannot also be assigned as a system owner for systems the individual is authorizing.

The potential inputs for this task are organizational security and privacy policies and procedures and organizational charts.

As a result, the expected outputs of Task P-1 are documented Risk Management Framework role assignments.

Task P-2, Risk Management Strategy

Task P-2, Risk Management Strategy, establishes a risk management strategy for the organization, including a determination of risk tolerance.

The risk management strategy informs risk-based decisions including approaches for monitoring risk over time, acceptable risk assessment methodologies, and how threats and the risk tolerance are used for decision-making.

Risk tolerance is the degree of risk or uncertainty that is acceptable to an organization. Risk tolerance affects all parts of the organization's risk management process, having a direct impact on the risk management decisions made by senior leaders or executives throughout the organization and providing important constraints on those decisions.

Potential inputs of Task P-2 include an organizational mission statement, organizational policies, and organizational risk assumptions, constraints, priorities, and trade-offs.

The expected outputs are a risk management strategy and statement of risk tolerance inclusive of information security and privacy risk.

Task P-3, Risk Assessment—Organization

Task P-3, Risk Assessment—Organization, is meant to assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.

Risk assessments are applied to identify, estimate, and prioritize the risk from an organization's operations to an organization's mission, functions, reputation, assets, individuals, and the Nation.

Some of the potential inputs include a risk management strategy, risk assessment results, supply chain risk assessment results, and security and privacy information from continuous monitoring.

The inclusive list of potential inputs for this task is listed below.

Potential inputs:

- Risk management strategy
- Mission objectives
- Risk assessment results
- Current threat information
- System-level security and privacy risk assessment results
- Supply chain risk assessment results
- Previous organization-level security and privacy risk assessment results
- Information sharing agreements or memoranda of understanding
- Security and privacy information from continuous monitoring

The expected output is organization-level risk assessment results.

Task P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles

Task P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles, is an optional task for organizations to complete.

This task is meant to establish, document, and publish organizationally-tailored control baselines and/or Cybersecurity Framework Profiles.

Organizationally-tailored control baselines address an organizational business need for a specialized set of controls to reduce risk.

Some of the potential inputs include mission or business objectives, organization- and system-level risk assessment results, mission or business objectives, privacy architecture, and a list of common control providers and common controls available for inheritance.

The inclusive list of potential inputs for this task is listed below.

Potential inputs:

- Documented security and privacy requirements directing the use of organizationally-tailored control baselines
- Mission or business objectives
- Enterprise architecture
- Security architecture
- Privacy architecture
- Organization- and system-level risk assessment results
- List of common control providers and common controls available for inheritance
- NIST Special Publication 800-53B control baselines

At the completion of this task, the expected outputs are a list of approved or directed organizationally-tailored control baselines and NIST Cybersecurity Framework, or CSF, Profiles.

Task P-5, Common Control Identification

Task P-5, Common Control Identification, was established to identify, document, and publish common controls available for inheritance by organizational systems.

Common controls are controls that can be inherited by one or more information systems. Examples include personnel security controls, policies and procedures, and acquisition controls.

The potential inputs associated with Task P-5 are documented security and privacy requirements, existing common control providers and associated security and privacy plans, information security and privacy program plans, and organization- and system-level security and privacy risk assessment results.

As a result, the expected outputs are a list of common control providers and common controls available for inheritance and security and privacy plans, or equivalent documents, that provide a description of the common control implementation to include inputs, expected behavior, and expected outputs.

Task P-6, Impact-Level Prioritization

Task P-6, Impact Level Prioritization, is an optional task for organizations to complete. This task can only be implemented after organizational systems have been categorized. These systems are divided into three subcategories: low-moderate systems, moderate-moderate systems, and high-moderate systems.

The prioritization of its systems gives an organization an opportunity to make informed decisions regarding control selection and the tailoring of control baselines when responding to identified risks.

The potential inputs of Task P-6 include security categorization information for organizational systems, system descriptions, organization- and system-level risk assessment results, mission or business objectives, and Cybersecurity Framework Profiles.

As an expected output of Task P-6, organizational systems are prioritized into low-, moderate-, and high-impact sub-categories.

Task P-7, Continuous Monitoring Strategy—Organization

Task P-7, Continuous Monitoring Strategy—Organization, was established to develop and implement an organization-wide strategy for monitoring control effectiveness.

An important aspect of risk management is the ability to monitor the security and privacy posture across the organization and the effectiveness of controls implemented within or inherited by organizational systems on an ongoing basis. An effective organization-wide continuous monitoring strategy is essential to efficiently and cost-effectively carry out such monitoring.

The potential inputs associated with Task P-7 are a risk management strategy, organization- and system-level risk assessment results, and organizational security and privacy policies.

The expected output is an implemented organizational continuous monitoring strategy.

Review Activity

Knowledge Check 1

Before we continue, try answering this question

Which of the following correctly describes the purpose of Task P-7 (Continuous Monitoring Strategy)?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ To establish a risk management strategy for the organization
- ○ To identify a strategy for organization-wide security and monitoring
- ○ To develop an organization-wide strategy for monitoring control effectiveness
- ○ To assess organization-wide security and privacy risk and update the risk assessment results

Knowledge Check 2

Now try this question.

Which of the following correctly describes the Task P-3 (Risk Assessment—Organization)?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ To establish a risk management strategy for the organization
- ○ To identify a strategy for organization-wide security and monitoring
- ○ To assess the organization-wide strategy for monitoring risk
- ○ To assess organization-wide security and privacy risk and update the risk assessment results

Knowledge Check 3

Match the expected output to the correct task.

Check your answer in the Answer Key at the end of this Student Guide.

Task P-4 (Organizationally-Tailored Control Baselines and Cybersecurity Framework Profile) _____

Task P-6 (Impact-Level Prioritization) _____

Task P-1 (Risk Management Roles) _____

A. Documented Risk Management Framework role assignments

B. List of approved or directed organizationally-tailored control baselines

C. Organizational systems prioritized into low-, moderate-, and high-impact sub-categories

System-Level Tasks

System-Level Tasks

Next, we will review the system-level tasks associated with the Prepare Step.

Tasks P-8 through P-18 are the responsibility of either the Information System Security Manager, or ISSM, or the Information System Security Office, or ISSO, with assistance from the Information System Owner, or ISO, and the Key Management Personnel, or KMP.

Similar to the organization-level tasks, each system-level task contains a set of potential inputs that is required to implement the tasks and a set of expected outputs as a result.

Within the system level, there are eleven tasks:

- Task P-8, Mission or Business Focus
- Task P-9, System Stakeholders
- Task P-10, Asset Identification
- Task P-11, Authorization Boundary
- Task P-12, Information Types
- Task P-13, Information Life Cycle
- Task P-14, Risk Assessment—System
- Task P-15, Requirements Definition
- Task P-16, Enterprise Architecture
- Task P-17, Requirement Allocation, and
- Task P-18, System Registration

Let's review the tasks, potential inputs and expected outputs of P-8 through P-18.

Review each task to learn more.

Task P-8, Mission or Business Focus

Task P-8, Mission or Business Focus, identifies the missions, business functions, and mission and business processes that the system is intended to support.

The prioritization of missions and business functions drives investment strategies, funding decisions, resource prioritization, and risk decisions—and thus affects the existing enterprise architecture and development of the associated security and privacy architectures.

The potential inputs associated with Task P-8 include an organizational mission statement; organizational policies; mission and business process information; system stakeholder information, Cybersecurity Framework Profiles, requests for proposal or other acquisition documents, and a concept of operations.

The expected outputs are missions, business functions, and mission and business

processes that the system will support.

Task P-9, System Stakeholders

Task P-9, System Stakeholders, identifies stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.

Stakeholders could include individuals, organizations, or representatives that have an interest in the system throughout the system's life cycle. It also includes all aspects of the supply chain.

Some of the potential inputs associated with Task P-9 include an organizational mission statement, organizational security and privacy policies and procedures, organizational charts, and information about individuals, internal and external, that have an interest in and decision-making responsibility for the system.

The inclusive list of potential inputs for this task is listed below.

Potential inputs:

- Organizational mission statement
- Mission or business objectives
- Missions, business functions, and mission/business processes that the system will support
- Other mission/business process information
- Organizational security and privacy policies and procedures
- Organizational charts
- Information about individuals or groups (internal and external) that have an interest in and decision-making responsibility for the system.

The expected output is a list of system stakeholders.

Task P-10, Asset Identification

Task P-10, Asset Identification, identifies assets that require protection. Assets are tangible and intangible items that are of value to achievement of mission or business objectives.

Tangible assets are physical in nature and include environmental elements such as non-digital information and facilities, human elements, and technology/machine elements. In contrast, intangible assets are not physical in nature and include mission and business processes, digital information and data, software, and services.

Potential inputs associated with Task P-10 include missions, business functions, and mission and business processes the information system will support; business impact

analyses; internal stakeholders; system stakeholder information; system information; and information about other systems that interact with the system.

The expected output is a set of assets to be protected.

Task P-11, Authorization Boundary

Task P-11, Authorization Boundary, determines the authorization boundary of the system. Authorization boundaries establish the scope of protection for information systems—that is, what the organization agrees to protect under its management control or within the scope of its responsibilities.

A clear delineation of authorization boundaries is important for accountability and for security categorization, especially in situations where lower-impact systems are connected to higher-impact systems, or when external providers are responsible for the operation or maintenance of a system.

The potential inputs associated with Task P-11 are system design documentation, network diagrams, system stakeholder information, asset information, network and/or enterprise architecture diagrams, and organizational structure, such as charts and related information.

The expected output is a documented authorization boundary.

Task P-12, Information Types

Task P-12, Information Types, identifies the types of information processed, stored, and transmitted by the system. Identifying the types of information needed to support organizational missions, business functions, and mission/business processes is an important step in developing security and privacy plans for the system and a precondition for determining the security categorization.

The potential inputs associated with Task P-12 are system design documentation, assets to be protected, mission and business process information, and system design documentation.

The expected output is a list of information types for the system.

Task P-13, Information Life Cycle

Task P-13, Information Life Cycle, identifies and understands all stages of the information life cycle for each information type processed, stored, or transmitted by the system.

The information life cycle describes the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.

Identifying and understanding how each information type is processed during all stages of the life cycle helps organizations identify considerations for protecting the information, informs the organization's security and privacy risk assessments, and informs the selection and implementation of controls.

Some of the potential inputs associated with Task P-13 are missions, business functions, and mission and business processes the system will support; authorization boundary information; system design documentation; and a list of system information types.

The inclusive list of potential inputs for this task is listed below.

Potential inputs:

- Missions, business functions, and mission/business processes the system will support
- System stakeholder information
- Authorization boundary information
- Information about other systems that interact with the system
- System design documentation
- System element information
- List of system information types

As a result of Task P-13, the expected outputs are documentation of the stages through which information passes in the system. Such documentation includes data flow diagrams, entity relationship diagrams, database schemas, and data dictionaries.

Task P-14, Risk Assessment--System

The next task, Task P-14, Risk Assessment—System, was established to conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.

Assessment of security risk includes identification of threat sources and threat events affecting assets, whether and how the assets are vulnerable to the threats, the likelihood that an asset vulnerability will be exploited by a threat, and the impact (or consequence) of loss of the assets.

As a key part of the risk assessment, assets are prioritized based on the adverse impact or consequence of asset loss.

Some of the potential inputs associated with Task P-14 are assets to be protected, business impact analyses or criticality analyses, information about other systems that interact with the system, provider information, system design documentation, and organizational-level risk assessment results.

The inclusive list of potential inputs for this task is listed below.

Potential inputs:

- Assets to be protected
- Missions, business functions, and mission/business processes the system will support
- Business impact analyses or criticality analyses
- System stakeholder information
- Information about other systems that interact with the system
- Provider information
- Threat information
- Data map
- System design documentation
- Cybersecurity Framework Profiles
- Risk Management Strategy
- Organizational-level risk assessment results.

The expected outputs are security and privacy risk assessment reports.

Task P-15, Requirements Definition

Task P-15, Requirements Definition, defines the security and privacy requirements for the system and the environment of operation. Security and privacy requirements are obtained from many sources such as laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments.

These requirements are an important part of the formal expression of the required characteristics of the system, inform the selection of controls for a system, and the tailoring activities associated with those controls.

Some of the potential inputs associated with Task P-15 are system design documentation; missions, business functions, and mission and business processes the system will support; Cybersecurity Framework Profiles; supply chain information; threat information; and laws, executive orders, directives, regulations, or policies that apply to the system.

The inclusive list of potential inputs for this task is listed below.

Potential inputs:

- System design documentation

- Organization- and system-level risk assessment results
- Known set of stakeholder assets to be protected
- Missions, business functions, and mission/business processes the system will support
- Business impact analyses or criticality analyses
- System stakeholder information
- Data map of the information life cycle for PII
- Cybersecurity Framework Profiles
- Information about other systems that interact with the system
- Supply chain information
- Threat information
- Laws, executive orders, directives, regulations, or policies that apply to the system
- Risk management strategy

The expected outputs are documented security and privacy requirements.

Task P-16, Enterprise Architecture

Task P-16, Enterprise Architecture, determines the placement of the system within the enterprise architecture. Enterprise architecture is a management practice which maximizes the effectiveness of the mission and business process and resources to achieve success. It provides an opportunity for organizations to consolidate, standardize, and optimize information and technology assets.

Potential inputs associated with Task P-16 are security and privacy requirements, organization- and system-level risk assessment results, enterprise architecture information, security architecture information, privacy architecture information, and asset information.

The expected outputs are updated enterprise architecture, updated security architecture, updated privacy architecture, plans to use cloud-based systems, and shared systems, services, or applications.

Task P-17, Requirements Allocation

Task P-17, Requirements Allocation, allocates security requirements to the system and to the environment of operation. Security and privacy requirements are allocated to guide and inform control selection and implementation for the organization, system, system elements, and/or environment of operation.

The potential inputs are organization- and system-level risk assessment results, documented security and privacy requirements, a list of common control providers and common controls available for inheritance, a system description, system element information, system component inventory, and relevant laws, executive orders, directives, regulations, and policies.

The expected output is a list of security and privacy requirements allocated to the system, system elements, and the environment of operation.

Task P-18, System Registration

The last step of the system-level tasks, Task P-18, System Registration, registers the system with organizational program or management offices.

System registration, in accordance with organizational policy, serves to inform the governing organization of plans to develop the system or the existence of the system; the key characteristics of the system; and the expected security and privacy implications for the organization due to the operation and use of the system.

The potential inputs of Task P-18 are the organizational policy on system registration and the system information.

The expected output is a registered system in accordance with organizational policy.

Review Activity

Knowledge Check 1

Before we conclude the lesson, try answering this question.

Which of the following potential inputs is associated with Task P-8 (Mission or Business Focus)?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ System stakeholder information
- ○ Enterprise architecture diagram
- ○ Business impact analyses
- ○ Organizational structure

Knowledge Check 2

Now try this question.

Which of the following correctly describes the purpose of Task P-15 (Requirements Definition)?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ To conduct a system-level assessment of the organization
- ○ To define the organization-wide strategy for monitoring risk
- ○ To define the security and privacy requirements for the system
- ○ To assess the requirements for organization-wide privacy and security

Knowledge Check 3

Match the expected output to the correct task.

Check your answer in the Answer Key at the end of this Student Guide.

Task P-12 (Information Types) _____

Task P-4 (Risk Assessment - System) _____

Task P-18 (System Registration) _____

A. Registered system in accordance with organizational policy

B. Security and privacy risk assessment reports

C. A list of information types for the system

Lesson Conclusion

Lesson Conclusion

You have completed the Prepare Step Tasks, Potential Inputs, and Expected Outputs lesson.

Lesson 3: Prepare Step Roles and Responsibilities

Lesson Introduction

Lesson Introduction

In this lesson, Prepare Step Roles and Responsibilities, you will learn the organization-level and system-level roles within the Prepare Step.

Please take a moment to review the lesson learning objectives.

Lesson 3 Learning Objectives:

- Summarize the organization-level roles within the Prepare Step
- Select the appropriate role that corresponds with a given responsibility within the system-level tasks

Organization-Level Roles

Organization-Level Roles

In Lesson 2, you learned about the tasks within the Prepare Step. Each task is the primary responsibility of certain members in the organization. Before we go through the roles associated with each task, let's have a brief overview of the primary roles within organization-level tasks.

Within the organization level, there are seven primary roles or responsibilities: Head of Agency, Chief Information Officer, Risk Executive (Function), Senior Agency Information Security Officer, Senior Agency Official for Privacy, Senior Accountable Official for Risk Management, and the Mission or Business Owner.

The Head of Agency is responsible and accountable for providing information security protections commensurate with the risk to organizational operations and assets, individuals, other organizations, and the Nation.

The Chief Information Officer is an organizational official responsible for designating a senior agency information security officer, developing and maintaining security policies and procedures, and overseeing personnel with significant responsibilities for security.

The Risk Executive (Function) provides a comprehensive, organization-wide approach to risk management.

The Senior Agency Information Security Officer is an organizational official responsible for carrying out the Chief Information Officer security responsibilities under the Federal Information Security Modernization Act, or FISMA.

The Senior Agency Official for Privacy is the senior official or executive with agency-wide

responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risk.

The Senior Accountable Official for Risk Management is the head of the agency, or an individual designated by the head of the agency.

The Senior Accountable Official for Risk Management leads and manages the Risk Executive (Function) in an organization and is responsible for aligning information security and privacy risk management processes with strategic, operational, and budgetary planning processes.

Lastly, the Mission or Business Owner is the senior official or executive within an organization with specific mission or line of business responsibilities. They are key stakeholders that have a significant role in establishing organizational mission and business processes, protection needs, and security and privacy requirements.

Tasks P-1 through P-4

In Task P-1, it is the primary responsibility of the Head of Agency, Chief Information Officer, and Senior Agency Official for Privacy to assign individuals to specific roles.

The supporting roles include the Authorizing Official or AO, the AODR, Senior Accountable Official for Risk Management or Risk Executive (Function), and Senior Agency Information Security Officer.

Task P-2, Risk Management Strategy, is the primary responsibility of the Head of Agency.

The supporting roles include 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.

In Task P-3, Risk Assessment— Organization, it is the primary responsibility of the Senior Accountable Official for Risk Management or Risk Executive (Function), Senior Agency Information Security Officer, and Senior Agency Official for Privacy to assess risk and update assessment results.

Supporting roles include the Chief Information Officer, Mission or Business Owner, and AO or Authorizing Official Designated Representative, or AODR.

Task P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles, is the primary responsibility of either the Mission or Business Owner, Senior Accountable Official for Risk Management, or Risk Executive (Function).

The supporting roles for Task P-4 include the Chief Information Officer; AO or AODR; Senior Agency Information Security Officer; and Senior Agency Official for Privacy.

Task P-1, Risk Management Roles
Primary Responsibility: Head of Agency; Chief Information Officer; Senior Agency Official for Privacy.
Supporting Roles: Authorizing Official (AO) or Authorizing Official Designated Representative (AODR); Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer.

Task P-2, Risk Management Strategy
Primary Responsibility: Head of Agency.
Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Task P-3, Risk Assessment— Organization
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 (AO) or Authorizing Official Designated Representative (AODR).

Task P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional)
Primary Responsibility: Mission or Business Owner; Senior Accountable Official for Risk Management or Risk Executive (Function).

Tasks P-5 through P-7

Task P-5 is the primary responsibility of the Senior Agency Information Security Officer and Senior Agency Official for Privacy. The supporting roles are the Mission or Business Owner; Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; AO or AODR; Common Control Provider; and System Owner.

Task P-6, Impact-Level Prioritization, is the primary responsibility of the Senior Accountable Official for Risk Management or Risk Executive (Function) to prioritize the organizational system. Supporting roles include the Senior Agency Information Security Officer; Senior Agency Official for Privacy; Mission or Business Owner; System Owner; Chief Information Officer; and AO or AODR.

Like Task P-6, Task P-7, Continuous Monitoring Strategy - Organization, is the primary responsibility of the Senior Accountable Official for Risk Management or Risk Executive (Function). Supporting roles include the Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Mission or Business Owner; System Owner; and AO or AODR.

Task P-5, Common Control Identification
Primary Responsibility: Senior Agency Information Security Officer; Senior Agency Official for Privacy.
Supporting Roles: Mission or Business Owner; Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Authorizing Official (AO) or Authorizing Official Designated Representative (AODR); Common Control Provider; System Owner.

Task P-6, Impact-Level Prioritization (Optional)
Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function).
Supporting Roles: Senior Agency Information Security Officer; Senior Agency Official for Privacy; Mission or Business Owner; System Owner; Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative.

Task P-7, Continuous Monitoring Strategy - Organization
Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function).
Supporting Roles: Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Mission or Business Owner; System Owner; Authorizing Official (AO) or Authorizing Official Designated Representative (AODR).

Review Activity

Knowledge Check 1

Which of the following are considered primary roles within organization-level tasks?

Before we continue, try answering this question.

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Mission or Business Owner
- ○ Head of Agency
- ○ System Owner
- ○ Chief Information Officer

Knowledge Check 2

Now try this question.

Fill in the blank: The _____ is an individual or group within an organization that provides a comprehensive, organization-wide approach to risk management.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Mission Owner
- ○ Risk Executive (Function)
- ○ System Owner
- ○ Head of Agency

Knowledge Check 3

How about this one.

Fill in the blank: The _____ is the head of the agency or an individual designated by the head of the agency.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Risk Executive (Function)
- ○ Head of Agency
- ○ System Owner
- ○ Senior Accountable Official for Risk Management

System-Level Roles

System-Level Roles

Next, we'll review the eight primary roles or responsibilities within the system-level tasks.

These include the Mission or Business Owner, AO, Enterprise Architect, Information Owner or Steward, System Owner, Senior Agency Official for Privacy, System Security or Privacy Officer, and the Security or Privacy Architect.

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

The Enterprise Architect is responsible for working with the organization's leadership and subject matter experts to build a holistic view of the organization's missions and business functions, processes, and information.

The Information Owner or Steward is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

The System Owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system.

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

Lastly, the Security or Privacy Architect is 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.

Tasks P-8 through P-13 Roles

In Task P-8, Mission or Business Focus, it is the primary responsibility of the Mission or Business Owner.

Supporting roles for Task P-8 include the AO or AODR; System Owner; Information Owner or Steward; Chief Information Officer; Senior Agency Information Security Officer; and Senior Agency Official for Privacy.

It is the primary responsibility of the Mission or Business Owner or System Owner to identify stakeholders in Task P-9.

The supporting roles include the Chief Information Officer; AO or AODR; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy; and Chief Acquisition Officer.

Task P-10, Asset Identification, is the primary responsibility of the System Owner. The supporting roles are the AO or AODR, Mission or Business Owner; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy; and System Administrator.

It is the primary responsibility of the AO to determine the authorization boundary in Task P-11. Supporting roles for Task P-11 are the Chief Information Officer; System Owner; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; and Enterprise Architect.

In Task P-12, it is the primary responsibility of the System Owner and Information Owner or Steward to identify types of information to be processed and stored. The supporting roles are the Mission or Business Owner, System Security Officer, and System Privacy Officer.

Task P-13, Information Life Cycle, is the primary responsibility of the Senior Agency Official for Privacy, System Owner, and Information Owner or Steward. Supporting roles include the Chief Information Officer; Mission or Business Owner; Security Architect; Privacy Architect; Enterprise Architect; Systems Security Engineer; and Privacy Engineer

Task P-8, Mission or Business Focus
Primary Responsibility: Mission or Business Owner.
Supporting Roles: Authorizing Official (AO) or Authorizing Official Designated Representative (AODR); System Owner; Information Owner or Steward; Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Task P-9, System Stakeholders
Primary Responsibility: Mission or Business Owner; System Owner.
Supporting Roles: Chief Information Officer; Authorizing Official (AO) or Authorizing Official Designated Representative (AODR); Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Chief Acquisition Officer.

Task P-10, Asset Identification
Primary Responsibility: System Owner.
Supporting Roles: Authorizing Official (AO) or Authorizing Official Designated Representative (AODR); Mission or Business Owner; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Administrator.

Task P-11, Authorization Boundary
Primary Responsibility: Authorizing Official.
Supporting Roles: Chief Information Officer; System Owner; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Enterprise Architect

Task P-12, Information Types
Primary Responsibility: System Owner; Information Owner or Steward.
Supporting Roles: Mission or Business Owner; System Security Officer; System Privacy Officer

Task P-13, Information Life Cycle
Primary Responsibility: Senior Agency Official for Privacy; System Owner; Information Owner or Steward.
Supporting Roles: Chief Information Officer; Mission or Business Owner; Security Architect; Privacy Architect; Enterprise Architect; Systems Security Engineer; Privacy Engineer.

Tasks P-14 through P-18 Roles

Task P-14, Risk Assessment—System, is the primary responsibility of the System Owner, System Security Officer, and System Privacy Officer.

Supporting roles include the Senior Accountable Official for Risk Management or Risk Executive (Function); AO or AODR; Mission or Business Owner; Information Owner or Steward; and Control Assessor.

In Task P-15, it is the primary responsibility of the Mission or Business Owner, System Owner, Information Owner or Steward, and System Privacy Officer to define the security and privacy requirements for the system. The supporting roles for Task P-15 are the AO, AODR, System Security Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Chief Acquisition Officer; Security Architect; Privacy Architect; and Enterprise Architect.

Task P-16, Enterprise Architecture, is the primary responsibility of the Mission or Business Owner, Enterprise Architect, and Security or Privacy Architect. Supporting roles include the Chief Information Officer; AO or AODR; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner; and Information Owner or Steward.

In Task P-17, the Security Architect, System Security Officer, and System Privacy Officer allocate security and privacy requirements to the system.

Some of the supporting roles include the Chief Information Officer; AO or AODR; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; and System Owner.

Lastly, Task P-18, System Registration, is the primary responsibility of the System Owner. The supporting roles include the Mission or Business Owner, Chief Information Officer, System Security Officer, and System Privacy Officer.

Task P-14, Risk Assessment—System
Primary Responsibility: System Owner; System Security Officer; System Privacy Officer.
Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Authorizing Official (AO) or Authorizing Official Designated Representative (AODR); Mission or Business Owner; Information Owner or Steward; Control Assessor.

Task P-15, Requirements Definition
Primary Responsibility: Mission or Business Owner; System Owner; Information Owner or Steward; System Privacy Officer.
Supporting Roles: Authorizing Official (AO) or Authorizing Official Designated Representative (AODR); System Security Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Chief Acquisition Officer; Security Architect; Privacy Architect; Enterprise Architect.

Task P-16, Enterprise Architecture
Primary Responsibility: Mission or Business Owner; Enterprise Architect; Security Architect; Privacy Architect.
Supporting Roles: Chief Information Officer; Authorizing Official (AO) or Authorizing Official Designated Representative (AODR); Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner; Information Owner or Steward.

Task P-17, Requirements Allocation
Primary Responsibility: Security Architect; Privacy Architect; System Security Officer; System Privacy Officer.
Supporting Roles: Chief Information Officer; Authorizing Official (AO) or Authorizing Official Designated Representative (AODR); Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner.

Task P-18, System Registration
Primary Responsibility: System Owner.
Supporting Roles: Mission or Business Owner; Chief Information Officer; System Security Officer; System Privacy Officer.

Review Activity

Knowledge Check 1

Match the primary responsibility to the corresponding task.

Check your answer in the Answer Key at the end of this Student Guide.

Task P-18 (System Registration) _____

Task P-12 (Information Types) _____

Task P-11 (Authorization Boundary) _____

Task P-2 (Risk Management Strategy) _____

Task P-5 (Common Control Identification) _____

A. Head of Agency
B. System Owner
C. Senior Agency Information Security Officer and Senior Agency Official for Privacy
D. Authorizing Official (AO)
E. System Owner and Information Owner or Steward

Lesson Conclusion

You have completed the Prepare Step Roles and Responsibilities lesson.

Course Conclusion

Conclusion

Summary

Congratulations on completing the RMF Prepare Step course. You should now be able to perform all the listed activities.

Course Learning Objectives:

- Describe the purpose of the Prepare Step in the Risk Management Framework (RMF)
- Identify tasks, potential inputs, and expected outputs within the Prepare Step
- Identify roles and responsibilities in the Prepare Step

For more information on the RMF Prepare Step Task, Potential Inputs, Expected Outputs, and Roles, please visit the Course Resources.

Course Conclusion

To receive credit for this course, you must take the course examination.

You have completed the Risk Management Framework (RMF) Prepare Step course.

.

Appendix A: Answer Key

Lesson 1 Review Activity

Knowledge Check 1

Which of the following correctly describes the Risk Management Framework (RMF)?

- ○ A process for managing security and privacy risk *(correct response)*
- ○ A security program that supports all DOD activities
- ○ A subfield of the federal government designed to provide security guidelines
- ○ A process for supporting all security efforts for the DOD

Feedback: *The Risk Management Framework (RMF) is a process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.*

Knowledge Check 2

Which of the following policies establishes the RMF as an integrated enterprise-wide decision structure for cybersecurity risk management?

- ○ NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- ○ DODI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT) *(correct response)*
- ○ NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- ○ DODI 8500.01 Cybersecurity

Feedback: *DODI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT) establishes the RMF as an integrated enterprise-wide decision structure for cybersecurity risk management.*

Lesson 2 Review Activity

Knowledge Check 1

Which of the following correctly describes the purpose of Task P-7 (Continuous Monitoring Strategy)?

- ○ To establish a risk management strategy for the organization
- ○ To identify a strategy for organization-wide security and monitoring
- ○ To develop an organization-wide strategy for monitoring control effectiveness *(correct response)*
- ○ To assess organization-wide security and privacy risk and update the risk assessment results

Feedback: *Task P-7 (Continuous Monitoring Strategy) is intended to develop an organization-wide strategy for monitoring control effectiveness.*

Knowledge Check 2

Which of the following correctly describes the Task P-3 (Risk Assessment—Organization)?

- ○ To establish a risk management strategy for the organization
- ○ To identify a strategy for organization-wide security and monitoring
- ○ To assess the organization-wide strategy for monitoring risk
- ○ To assess organization-wide security and privacy risk and update the risk assessment results *(correct response)*

Feedback: *Task P-3 (Risk Assessment—Organization) is intended to assess organization-wide security and privacy risk and update the risk assessment results.*

Knowledge Check 3

Match the expected output to the correct task.

Task P-4 (Organizationally-Tailored Control Baselines and Cybersecurity Framework Profile) __B__

Task P-6 (Impact-Level Prioritization) __C__

Task P-1 (Risk Management Roles)__A__

A. Documented Risk Management Framework role assignments

B. List of approved or directed organizationally-tailored control baselines

C. Organizational systems prioritized into low-, moderate-, and high-impact sub-categories

Feedback: *The expected output of Task P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profile, is a list of approved or directed organizationally-tailored control baselines. The expected output of Task P-6, Impact-Level Prioritization, is organizational systems prioritized into low-, moderate-, and high-impact sub-categories. The expected output of Task P-1, Risk Management Roles, is documented*

Risk Management Framework role assignments.

Knowledge Check 4

Which of the following potential inputs is associated with Task P-8 (Mission or Business Focus)?

- ○ System stakeholder information *(correct response)*
- ○ Enterprise architecture diagram
- ○ Business impact analyses
- ○ Organizational structure

Feedback: *System stakeholder information is a potential input of Task P-8, Mission or Business Focus.*

Knowledge Check 5

Which of the following correctly describes the purpose of Task P-15 (Requirements Definition)?

- ○ To conduct a system-level assessment of the organization
- ○ To define the organization-wide strategy for monitoring risk
- ○ To define the security and privacy requirements for the system *(correct response)*
- ○ To assess the requirements for organization-wide privacy and security

Feedback: *Task P-15, Requirements Definition, is intended to define the security and privacy requirements for the system.*

Knowledge Check 6

Match the expected output to the correct task.

Task P-12 (Information Types) __C__

Task P-4 (Risk Assessment - System) __B__

Task P-18 (System Registration) __A__

A. Registered system in accordance with organizational policy

B. Security and privacy risk assessment reports

C. A list of information types for the system

Feedback: *In Task P-12, Information Types, an expected output is a list of information types for the system. An expected output of Task P-14, Risk Assessment – System, is security and privacy risk assessment reports. In Task P-18, System Registration, an expected output is a registered system in accordance with organizational policy.*

Lesson 3 Review Activity

Knowledge Check 1

Which of the following are considered primary roles within organization-level tasks?

- ○ Mission or Business Owner *(correct response)*
- ○ Head of Agency *(correct response)*
- ○ System Owner
- ○ Chief Information Officer *(correct response)*

Feedback: *The Head of Agency, Mission or Business Owner, and Chief Information Officer are primary roles within organization-level tasks.*

Knowledge Check 2

Fill in the blank: The _____ is an individual or group within an organization that provides a comprehensive, organization-wide approach to risk management.

- ○ Mission Owner
- ○ Risk Executive (Function) *(correct response)*
- ○ System Owner
- ○ Head of Agency

Feedback: *The Risk Executive (Function) is an individual or group within an organization that provides a comprehensive, organization-wide approach to risk management.*

Knowledge Check 3

Fill in the blank: The _____ is the head of the agency or an individual designated by the head of the agency.

- ○ Risk Executive (Function)
- ○ Head of Agency
- ○ System Owner
- ○ Senior Accountable Official for Risk Management *(correct response)*

Feedback: *The Senior Accountable Official for Risk Management is the head of the agency, or an individual designated by the head of the agency.*

Knowledge Check 4

Match the primary responsibility to the corresponding task.

Task P-18 (System Registration) __B__

Task P-12 (Information Types) __E__

Task P-11 (Authorization Boundary) __D__

Task P-2 (Risk Management Strategy) __A__

Task P-5 (Common Control Identification) __C__

A. Head of Agency

B. System Owner

C. Senior Agency Information Security Officer and Senior Agency Official for Privacy

D. Authorizing Official (AO)

E. System Owner and Information Owner or Steward

Feedback: *Task P-18, System Registration, is the primary responsibility of the System Owner. Task P-12, Information Types, is the primary responsibility of the System Owner and Information Owner or Steward. Task P-11, Authorization Boundary, is the primary responsibility of the Authorizing Official (AO). The Head of Agency has the primary responsibility over Task P-2, Risk Management Strategy. Task P-5, Common Control Identification, is the primary responsibility of the Senior Agency Information Security Officer and Senior Agency Official for Privacy.*