INTRODUCTION TO THE RISK MANAGEMENT FRAMEWORK

Student Guide

Lesson: Course Introduction

RMF Topics

The Risk Management Framework or RMF is the common information security framework for the federal government. RMF aims to improve information security, strengthen the risk management processes, and encourage reciprocity among federal agencies.

The topics we will cover include:

- Policies and regulations that govern the Department of Defense, or DOD, RMF process
- Categories of DOD Information Technology affected by the RMF
- The seven steps in the implementation of RMF
- RMF applicability to the DOD Acquisition Process

Course Objectives

At the end of this course, you will be able to identify policies and regulations that govern the DOD RMF process, define the categories of DOD information affected by the RMF, understand the Seven Step Implementation process of RMF, and recognize RMF applicability to the DOD Acquisition Process.

Please allow 30 minutes for completion of this course. Follow the on-screen instructions to advance through the course. You will also find options for course resources and transcripts of the course material.

To receive a certificate of completion for this course, you must take the final exam.

Lesson 1: RMF Introduction

RMF Introduction

Let’s begin by looking back to see how the DOD transformation to the Risk Management Framework started.

RMF Introduction (Continued)

Information Technology and systems are integral to operations at DOD. While these systems have brought great benefits to our Mission and Business functions, they also represent a vulnerability to our Organizational Operations.

DOD Systems are subject to threats that can have adverse effects on the confidentiality, integrity or availability of information processed, stored, or transmitted by DOD systems

RMF Policies and Regulations

The Risk Management Framework, supported by the National Institute of Standards and Technology, or NIST, 800-series publications and used by other federal agencies under the Federal Information Security Modernization Act, provides a structured, yet flexible approach for managing risk resulting from the incorporation of information systems into the mission and business processes of an organization.

Policy Alignment

DOD aligned Cybersecurity and risk management policies, procedures, and guidance with Joint Transformation NIST documents to create the basis for a unified information security framework for the Federal government.

Policy Partnerships

DOD participates in Committee on National Security Systems and NIST policy development as a vested stakeholder with the goals to create a more standardized approach tocybersecurity and to protect the unique requirements of DOD missions and warfighters.

RMF Guidance Alignment

The RMF knowledge service is DOD's official repository for enterprise RMF policy and implementation guidelines. The RMF knowledge service provides Cybersecurity practitioners and managers with a single authorized source for execution and implementation guidance, community forums, and the latest information and developments in the RMF.

DOD RMF Decisions Structure

Under the RMF, technical and non-technical features of DOD Information systems are comprehensively evaluated in the intended environment. This allows an Authorizing Official, or AO, to determine whether the system is approved to operate at an acceptable level of security risk based on the implementation of an approved set of technical, managerial, and procedural countermeasures or mitigation. We’ll explore the specifics of the framework, which consists of seven steps under the Implementation Guidance portion of this course.

Lesson 2: RMF Governance

RMF Governance

Now, let's talk about the governance of the risk management framework under the Department of Defense.

RMF Governance Overview

The DOD RMF governance structure implements the three-tiered approach to cybersecurity risk management described in NIST SP 800-39, synchronizes and integrates RMF activities across all phases of the IT life cycle, and spans logical and organizational entities.

DOD RMF Guidance

The complex, many-to-many relationships among mission or business processes and the information systems supporting those processes require a holistic, organization-wide view for managing risk. A holistic approach requires the management of risk at both the enterprise-level and system-level. This approach takes into account the organization as a whole, including strategic goals and objectives and relationships between mission/business processes and the supporting information systems.

Organizational culture and infrastructure should also be considered. The security controls and safeguards selected by the organization must take into account:

- Potential mission or business impacts;
- Risk to organizational operations and assets, individuals, other organizations, and the Nation.

These roles and responsibilities have been delegated enterprise wide and are arranged into tiers.

Guidance Tier 1

Tier 1 is the Office of Secretary of Defense and or Strategic Level and it addresses risk management at the DOD enterprise level.

The key governance elements in Tier 1 are:

- DOD Senior Information Security Officer, or SISO
- Risk Executive Function
- DOD Cybersecurity Architecture
- The RMF Technical Advisory Group (TAG)
- The Knowledge Service (KS)

TIER 1

Per current 8510.01 this information is listed for a TIER 1 Organization:

DOD SISO

- Directs and oversees the cybersecurity risk management of DOD IT and directs and coordinates the DOD Cybersecurity Program, which includes establishing and maintaining the RMF
- Advises and informs the principal authorizing officials (PAOs) and their representatives.
- Oversees the RMF TAG and the online KS.

Risk Executive Function

The Risk Executive Function consists of the DOD ISRMC supported by the DSAWG.

DOD Cybersecurity Architecture

The DOD Cybersecurity architecture consists of strategies, standards, and plans that have been developed for achieving an assured integrated, and survivable information enterprise.

The RMF TAG

The RMF TAG provides implementation guidance for the RMF by interfacing with the DOD Component cybersecurity programs, cybersecurity communities of interest (COIs), and other entities (e.g., DSAWG) to address issues that are common across all entities.

The KS

The KS is a dynamic online knowledge base that supports the RMF implementation, planning, and execution by functioning as the authoritative source for RMF procedures and guidance.

Guidance Tier 2

Tier 2 is the Mission Area and Component levels and addresses risk management at these levels.

The key governance element in Tier 2 is the Principal Authorizing Official, or PAO, DOD Component Chief Information Officer, or CIO, and DOD Component SISO.

TIER 2

PAO

A PAO is appointed for each of the DOD Mission Areas (MAs) Warfighting Mission Area (WMA), Business Mission Area (BMA), Enterprise Information Environment Mission Area (EIEMA), and DOD Portion of the Intelligence MA (DIMA)) and their representatives are members of the DOD ISRMC.

DOD Component CIO

Each DOD Component CIO, supported by the DOD Component SISO, is responsible for administration of the RMF within the DOD Component cybersecurity program.

DOD Component SISO

The DOD Component SISOs have authority and responsibility for security controls assessment and must establish and manage a coordinated security assessment process for information technologies governed by the DOD Component cybersecurity program.

Guidance Tier 3

Tier 3, Information System, or IS, and Platform Information Technology, or PIT Systems, consists of an AO as well as that IS or PIT System Cybersecurity Program.

TIER 3

AO

The DOD Component heads are responsible for the appointment of trained and qualified AOs for all DOD ISs and PIT systems within their Component. AOs should be appointed from senior leadership positions within business owner and mission owner organizations to promote accountability in authorization decisions that balance mission and business needs and security concerns.

IS or PIT System Cybersecurity Program

The system cybersecurity program consists of the policies, procedures, and activities of the ISO, PM/SM, UR, ISSM, and IS security officers (ISSOs) at the system level. The system cybersecurity program implements and executes policy and guidance from TIER 1 and TIER 2 and augments them as needed.

Knowledge Check 1: RMF Policy & Governance

What Policy governs Cybersecurity?

Select the best answer.

- ○ NIST SP 800-37
- ○ DODI 8510.01
- ○ DODI 8500.01
- ○ CNSSI 1253

Knowledge Check 2: RMF Policy & Governance

DOD participates in __________ and __________ as a vested stakeholder to create a more standardized approach to Cybersecurity.

Select the best answer.

- ○ Platform and Organization
- ○ TIER 1 and TIER 3
- ○ CNSS and NIST
- ○ RMF and NISPOM

Knowledge Check 3: RMF Policy & Governance

What factors do organizations need to take into account when implementing a holistic approach to organizational risk management?

Select the best answer.

- ○ Supporting Information Systems
- ○ Relationships between mission/business process
- ○ Strategic Goals and Objectives
- ○ All of the above

Lesson 3: DOD Information Technology

DOD Information Technology

Now that we have a good understanding of the policy and governance related to the Risk Management Framework, let's discuss the application of the RMF to DOD Information Technology.

DOD IT Defined

DOD Information Technology refers to all DOD owned IT or DOD controlled IT that receives, processes, stores, displays, or transmits DOD Information.

The forms of DOD IT range in size and complexity from individual hardware and software products to stand-alone systems to massive computing environments, enclaves, and networks.

IT products, services, and PIT are not authorized for operation through the full RMF process. These types of IT must be securely configured in accordance with applicable DOD policies and security controls and undergo special assessment of their functional and security-related capabilities and deficiencies.

Reciprocity

Cybersecurity reciprocity is an essential element in ensuring that IT capabilities are developed and fielded rapidly and efficiently across the DOD Information Enterprise. Applied appropriately, reciprocity reduces redundant testing, assessing and documentation, and the associated costs in time and resources. The DOD RMF presumes acceptance of existing test and assessment results and authorization documentation.

In order to facilitate reciprocity, the concepts in DOD Instruction 8510.01 paragraph 1a through 1e, Enclosure 5 are fundamental to a common understanding and must be adhered to. Let's review your understanding of DOD Information Technology.

Knowledge Check 4: DOD Information Technology

PIT Systems refer to:

Select the best answer.

- ○ Priority Information Technology
- ○ Proprietary Information Technology
- ○ Platform Information Technology
- ○ Process Information Technology

Knowledge Check 5: DOD Information Technology

What broad groups does DOD use to categorize information technology?

Select all that apply.

- ○ Information Systems
- ○ PIT
- ○ IT Services
- ○ IT Products

Lesson 4: Implementation Guidance

Implementation Guidance

Let’s discuss the application of the RMF Implementation Guidance.

Implementation Guidance (Continued)

Integrating information security into organizational infrastructure requires a carefully coordinated set of activities to ensure that fundamental requirements for information security are addressed and risk to the organization from information systems is managed efficiently and cost-effectively.

The Risk Management Framework methodology incorporates Federal Information System Modernization Act security standards and guidance to provide a holistic solution for managing risk to an organization's information and information systems.

RMF provides implementation guidance through a seven-step information system life cycle.

Let’s discuss the steps individually.

Prepare Step

Prepare is the first key step in the Risk Management Framework because of its effect on all other steps in the framework, from categorization of security controls to level of effort in assessing security control effectiveness.

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 Risk Management Framework.

The Prepare Step tasks are broken down by Organizational Level and System Level Tasks with specific tasks that lead to desired outcomes.

Table 1 provides a summary of tasks and expected outcomes for the RMF Prepare step at the organization level. Applicable Cybersecurity Framework constructs are also provided.

Tasks	Outcomes
TASK P-1 **RISK MANAGEMENT ROLES**	Individuals are identified and assigned key roles for executing the Risk Management Framework. [Cybersecurity Framework: **ID.AM-6; ID.GV-2**]
TASK P-2 **RISK MANAGEMENT STRATEGY**	A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [Cybersecurity Framework: **ID.RM; ID.SC]**]
TASK P-3 **RISK ASSESSMENT – ORGANIZATION**	An organization-wide risk assessment is completed or an existing risk assessment is updated. [Cybersecurity Framework: **ID-.RA; ID.SC-2**]
TASK P-4 **ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)**	Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [Cybersecurity Framework: **Profile**]
TASK P-5 **COMMON CONTROL IDENTIFICATION**	Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK P-6 **IMPACT-LEVEL PRIORITIZATION (OPTIONAL)**	A prioritization of organizational systems with the same impact level is conducted. [Cybersecurity Framework: **ID.AM-5**]
TASK P-7 **CONTINUOUS MONITORING STRATEGY – ORGANIZATION**	An organization-wide strategy for monitoring control effectiveness is developed and implemented. [Cybersecurity Framework: **DE.CM; ID.SC-4**]

Table 2 provides a summary of tasks and expected outcomes for the RMF Prepare step at the system level. Applicable Cybersecurity Framework constructs are also provided.

Tasks	Outcomes
TASK P-8 **MISSION OR BUSINESS FOCUS**	Missions, business functions, and mission/business processes that the system is intended to support are identified. [Cybersecurity Framework: Profile; Implementation Tiers; ID.BE]
TASK P-9 **SYSTEM STAKEHOLDERS**	The stakeholders having an interest in the system are identified. [Cybersecurity Framework: **ID.AM; ID.BE**]
TASK P-10 **ASSET IDENTIFICATION**	Stakeholder assets are identified and prioritized. [Cybersecurity Framework: **ID.AM**]
TASK P-11 **AUTHORIZATION BOUNDARY**	The authorization boundary [i.e., system] is determined.
TASK P-12 **INFORMATION TYPES**	The types of information processed, stored, and transmitted by the system are identified. [Cybersecurity Framework: **ID.AM-5**]
TASK P-13 **INFORMATION LIFE CYCLE**	All stages of the information life cycle are identified and understood for each information type [processed, stored, or transmitted by the system. [Cybersecurity Framework: ID.AM-3; ID.AM-4]
TASK P-14 **RISK ASSESSMENT – SYSTEM**	A system-level risk assessment is completed or an existing risk assessment is updated. [Cybersecurity Framework: **ID.RA; ID.SC-2**]
TASK P-15 **REQUIREMENTS DEFINITION**	Security and privacy requirements are defined and prioritized. [Cybersecurity Framework: **ID.GV; FR.IP**]
TASK P-16 **ENTERPRISE ARCHITECTURE**	The placement of the system within the enterprise architecture is determined.
TASK P-17 **REQUIREMENTS ALLOCATION**	Security and privacy requirements are allocated to the system and to the environment in which the system operates. [Cybersecurity Framework: **ID.GV**]
TASK P-18 **SYSTEM REGISTRATION**	The system is registered for purposes of management, accountability, coordination, and oversight. [Cybersecurity Framework: **ID.GV**]

Together, the tables represent the Prepare Step.

Categorization Step

Next is Categorize. The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

The Categorization Step is divided into three tasks with associated outcomes.

Tasks	Outcomes
TASK C-1 **SYSTEM DESCRIPTION**	The characteristics of the system are described and documented. [Cybersecurity Framework: Profile]
TASK C-2 **SECURITY CATEGORIZATION**	A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [Cybersecurity Framework: ID.AM-1; ID.AM-2; ID.AM-3; ID.AM-4; ID.AM-5] Security categorization results are documented in the security, privacy, and SCRM plans. [Cybersecurity Framework: Profile] Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. [Cybersecurity Framework: Profile] Security categorization results reflect the organization’s risk management strategy.
TASK C-3 **SECURITY CATEGORIZATION REVIEW AND APPROVAL**	The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.

Sample Control Baseline

Not all DOD Information Systems are National Security Systems or NSS; however, the same standards and process for categorizing NSS apply to non-NSS.

DOD Instruction 8510.01 requires all information systems and PIT systems for both NSS and non-NSS to be categorized in accordance with Committee on National Security Systems Information, or CNSSI, 1253.

The CNSSI 1253 System Categorization process builds on and is a companion document to NIST SP 800-53. It should be used as a tool to select and agree upon appropriate protections for an IS or PIT system.

Based upon Federal Information Processing Standard publication (FIPS) 199, Categorization of systems uses the three security objectives (confidentiality, integrity, and availability) with one impact value (low, moderate, or high) for each of the security objectives.

Security categorization results reflect the organization's risk management strategy. Results must be reviewed and approved by senior leaders in the organization.

Security Objective: Confidentiality

		Confidentiality		
ID	Title	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X
AC-2	Account Management	X	X	X
AC-2(1)	Account Management: Automated System Account Management	X	X	X
AC-2(2)	Account Management: Removal of Temporary/Emergency Accounts	X	X	X
AC-2(3)	Account Management: Disable Inactive Accounts	X	X	X
AC-2(4)	Account Management: Automated Audit Actions	+	X	X
AC-2(5)	Account Management: Inactivity Logout			
AC-2(6)	Account Management: Dynamic Privilege Management			
AC-2(7)	Account Management: Role-Based Schemes	+	+	+
AC-2(8)	Account Management: Dynamic Account Creation			
AC-2(9)	Account Management: Restrictions on Use of Shared Groups/Accounts	+	+	+
AC-2(10)	Account Management: Shared/Group Account Credential Termination	+	+	+
AC-2(11)	Account Management: Usage Conditions			
AC-2(12)	Account Management: Account Monitoring/Atypical Usage	+	+	X
AC-2(13)	Account Management: Disable Accounts for High-Risk Individuals	+	+	X
AC-3	Access Enforcement	X	X	X

L – Low
M – Medium
H – High
X – Security Controls from MIST Baselines
+ – Security Controls Added for Protection of NSS
Not all DOD ISs are NSS, however, the same standards and processes under the RMF also apply to ISs that are not NSSs.

Security Objective: Integrity

		Integrity		
ID	Title	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X
AC-2	Account Management	X	X	X
AC-2(1)	Account Management: Automated System Account Management	X	X	X
AC-2(2)	Account Management: Removal of Temporary/Emergency Accounts	X	X	X
AC-2(3)	Account Management: Disable Inactive Accounts	X	X	X
AC-2(4)	Account Management: Automated Audit Actions	+	X	X
AC-2(5)	Account Management: Inactivity Logout			
AC-2(6)	Account Management: Dynamic Privilege Management			
AC-2(7)	Account Management: Role-Based Schemes	+	+	+
AC-2(8)	Account Management: Dynamic Account Creation			
AC-2(9)	Account Management: Restrictions on Use of Shared Groups/Accounts	+	+	+
AC-2(10)	Account Management: Shared/Group Account Credential Termination	+	+	+
AC-2(11)	Account Management: Usage Conditions			
AC-2(12)	Account Management: Account Monitoring/Atypical Usage	+	+	X
AC-2(13)	Account Management: Disable Accounts for High-Risk Individuals	+	+	X
AC-3	Access Enforcement	X	X	X

L – Low
M – Medium
H – High
X – Security Controls from MIST Baselines
+ – Security Controls Added for Protection of NSS
Not all DOD ISs are NSS, however, the same standards and processes under the RMF also apply to ISs that are not NSSs.

Security Objective: Availability

		Availability		
ID	Title	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X
AC-2	Account Management			
AC-2(1)	Account Management: Automated System Account Management			
AC-2(2)	Account Management: Removal of Temporary/Emergency Accounts			
AC-2(3)	Account Management: Disable Inactive Accounts			
AC-2(4)	Account Management: Automated Audit Actions			
AC-2(5)	Account Management: Inactivity Logout	+	+	X
AC-2(6)	Account Management: Dynamic Privilege Management			
AC-2(7)	Account Management: Role-Based Schemes			
AC-2(8)	Account Management: Dynamic Account Creation			
AC-2(9)	Account Management: Restrictions on Use of Shared Groups/Accounts			
AC-2(10)	Account Management: Shared/Group Account Credential Termination			
AC-2(11)	Account Management: Usage Conditions			
AC-2(12)	Account Management: Account Monitoring/Atypical Usage			
AC-2(13)	Account Management: Disable Accounts for High-Risk Individuals			
AC-3	Access Enforcement			

L – Low
M – Medium
H – High
X – Security Controls from MIST Baselines
+ – Security Controls Added for Protection of NSS
Not all DOD ISs are NSS, however, the same standards and processes under the RMF also apply to ISs that are not NSSs.

Select Step

Next is Select. 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.

This table provides a summary of tasks and expected outcomes for the RMF Select step. Applicable Cybersecurity Framework constructs are also provided with specific inputs for each of the tasks that lead to the desired outcome.

Tasks	Outcomes
TASK S-1 **CONTROL SELECTION**	Control baselines necessary to protect the system commensurate with risk are selected. [*Cybersecurity Framework*: **Profile**]
TASK S-2 **CONTROL TAILORING**	Controls are tailored producing tailored control baselines. [*Cybersecurity Framework*: **Profile**]
TASK S-3 **CONTROL ALLOCATION**	Controls are designated as system-specific, hybrid, or common controls. Controls are allocated to the specific system elements (i.e., machine, physical, or human elements). [*Cybersecurity Framework*: **Profile; PR.IP**]
TASK S-4 **DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS**	Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents. [*Cybersecurity Framework*: **Profile**]
TASK S-5 **CONTINUOUS MONITORING STRATEGY—SYSTEM**	A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed. [*Cybersecurity Framework*: **ID.GV; DE.CM**]
TASK S-6 **PLAN REVIEW AND APPROVAL**	Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.

Security Control Catalog

Selecting a set of security and privacy controls to protect mission and business functions while managing security and privacy risks is a significant challenge for organizations. Correctly selected and implemented controls meet security and privacy requirements defined by applicable laws, executive orders, policies, regulations, and directives.

Tailoring of security controls is essential to address the diverse and specialized nature of DOD systems. Overlays can be applied for unique characteristics such as medical, Industrial Control or Weapon Systems while common controls are inherited from hosting environment and minimize complexity of control selection. This is a great use of the "build once/use many" approach.

Implement Step

Next is Implement. The purpose of the Implement step is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation.

This table provides a summary of tasks and expected outcomes for the RMF Implement step. Applicable Cybersecurity Framework constructs are also provided. As shown in the table with specific inputs for each of the tasks that lead to the desired outcome.

Tasks	Outcomes
TASK I-1 **CONTROL IMPLEMENTATION**	Controls specified in the security and privacy plans are implemented. [*Cybersecurity Framework*: **PR.IP-1**] Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. [*Cybersecurity Framework*: **PR.IP-2**]
TASK I-2 **UPDATE CONTROL IMPLEMENTATION INFORMATION**	Changes to the planned implementation of controls are documented. [*Cybersecurity Framework*: **PR.IP-1**] The security and privacy plans are updated based on information obtained during the implementation of the controls. [*Cybersecurity Framework*: **Profile**]

Assess Step

Next is Assess. The purpose of the Assess step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

This table provides a summary of tasks and expected outcomes for the RMF Assess step. Applicable Cybersecurity Framework constructs are also provided with specific inputs for each of the tasks that lead to the desired outcome.

Tasks	Outcomes
TASK A-1 **ASSESSOR SELECTION**	An assessor or assessment team is selected to conduct the control assessments. The appropriate level of independence is achieved for the assessor or assessment team selected.
TASK A-2 **ASSESSMENT PLAN**	Documentation needed to conduct the assessments is provided to the assessor or assessment team. Security and privacy assessment plans are developed and documented. Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.
TASK A-3 **CONTROL ASSESSMENTS**	Control assessments are conducted in accordance with the security and privacy assessment plans. Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered. Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.
TASK A-4 **ASSESSMENT REPORTS**	Security and privacy assessment reports that provide findings and recommendations are completed.
TASK A-5 **REMEDIATION ACTIONS**	Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions. [*Cybersecurity Framework*: **Profile**]
TASK A-6 **PLAN OF ACTION AND MILESTONES**	A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [*Cybersecurity Framework*: **ID.RA-6**]

Authorize Step

Next is Authorize. The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.

This Table provides a summary of tasks and expected outcomes for the RMF Authorize Step. Applicable Cybersecurity Framework constructs are also provided. As shown in the table with specific inputs for each of the tasks that lead to the desired outcome.

Tasks	Outcomes
TASK R-1 **AUTHORIZATION PACKAGE**	An authorization package is developed for submission to the authorizing official.
TASK R-2 **RISK ANALYSIS AND DETERMINATION**	A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.
TASK R-3 **RISK RESPONSE**	Risk responses for determined risks are provided. [*Cybersecurity Framework*: **ID.RA-6**]
TASK R-4 **AUTHORIZATION DECISION**	The authorization for the system or the common controls is approved or denied.
TASK R-5 **AUTHORIZATION REPORTING**	Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.

Monitor Step

Next is Monitor. The purpose of the Monitor step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions.

This table provides a summary of tasks and expected outcomes for the RMF Monitor Step. Applicable Cybersecurity Framework constructs are also provided. As shown in the diagram, there are specific inputs for each of the tasks that lead to the desired outcome.

Tasks	Outcomes
TASK M-1 **SYSTEM AND ENVIRONMENT CHANGES**	The information system and environment of operation are monitored in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **DE.CM; ID.GV**]
TASK M-2 **ONGOING ASSESSMENTS**	Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. *Cybersecurity Framework*: **ID.SC-4**]
TASK M-3 **ONGOING RISK RESPONSE**	The output of continuous monitoring activities is analyzed and responded to appropriately. [*Cybersecurity Framework*: **RS.AN**]
TASK M-4 **AUTHORIZATION PACKAGE UPDATES**	Risk management documents are updated based on continuous monitoring activities. [*Cybersecurity Framework*: **RS.IM**]
TASK M-5 **SECURITY AND PRIVACY REPORTING**	A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.
TASK M-6 **ONGOING AUTHORIZATION**	Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.
TASK M-7 **SYSTEM DISPOSAL**	A system disposal strategy is developed and implemented, as needed.

Knowledge Check 6: Implementation Guidance

What is the last step in the RMF Process? Select the best response.

- Prepare Step
- Monitor Step
- Categorize Step
- Assess Step

Knowledge Check 7: Implementation Guidance

To which step do the following tasks belong?

Information Types
System Registration
Asset Identification
System Stakeholders

- Assess Step
- Authorize Step
- Implement Step
- Prepare Step

Knowledge Check 8: Implementation Guidance

In what Step does the system disposal strategy developed and implemented as needed? Select the best response.

- Assess Step
- Prepare Step
- Monitor Step
- Implement Step

Lesson 5: RMF and DOD Acquisition

RMF and DOD IT Acquisition

Now that we have an understanding of the Risk Management Framework, let’s consider how it applies to the DOD IT Acquisition process.

RMF and the Defense Acquisition Management System

The RMF is designed to be complementary to and supportive of DOD's acquisition management system activities, milestones, and phases. RMF activities should be initiated as early as possible in the DOD acquisition process to increase security and decrease cost. Requirements development, procurement, and test and evaluation, also known as T&E, processes should be considered in applying the RMF to the acquisition of DOD IT. Threats to these systems should be designated consistent with the most severe risk to any individual component or subcomponent for consideration of requirements, acquisition, and testing and evaluation.

Summary

Risk management is critical to your organization’s ability to achieve its mission and goals. Because of the severity of the security threats faced by DOD organizations, use of the Risk Management Framework to implement information security safeguards for DOD information technology systems is essential.

Application of the Risk Management Framework will ensure that DOD Information Systems remain secure and that our organization is always mission ready.

Conclusion

This concludes the Introduction to the Risk Management Framework course. You should now be able to:

- Identify policies and regulations that govern the DOD RMF process,
- Define DOD Information Technology the categories of DOD information affected by the RMF
- Understand the Seven Step Implementation process of RMF
- Understand RMF applicability to the DOD Acquisition Process

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

Knowledge Check Answer Key

Knowledge Check 1: RMF Policy & Governance

What Policy governs Cybersecurity?

Select the best answer.

○ NIST SP 800-37
○ DODI 8510.01
✓ DODI 8500.01
○ CNSSI 1253

Knowledge Check 2: RMF Policy & Governance

DOD participates in __________ and __________ as a vested stakeholder to create a more standardized approach to Cybersecurity.

Select the best answer.

○ Platform and Organization
○ TIER 1 and TIER 3
● CNSS and NIST
○ RMF and NISPOM

Knowledge Check 3: RMF Policy & Governance

What factors do organizations need to take into account when implementing a holistic approach to organizational risk management?

Select the best answer.

○ Supporting Information Systems
○ Relationships between mission/business process
○ Strategic Goals and Objectives
● All of the above

Knowledge Check 4: DOD Information Technology

PIT systems refer to:

Select the best answer.

○ Priority Information Technology
○ Proprietary Information Technology
● Platform Information Technology
○ Process Information Technology

Knowledge Check 5: DOD Information Technology

What broad groups does DOD use to categorize information technology?

Select all that apply.

- ✓ Information Systems
- ✓ PIT
- ✓ IT Services
- ✓ IT Products

Knowledge Check 6: DOD Information Technology

What is the last step in the RMF Process?

Select the best response.

- ○ Prepare Step
- ● Monitor Step
- ○ Categorize Step
- ○ Assess Step

Knowledge Check 7: Implementation Guidance

To which step do the following tasks belong:

Information Types
System Registration
Asset Identification
System Stakeholders

- ○ Assess Step
- ○ Authorize Step
- ○ Implement Step
- ● Prepare Step

Knowledge Check 8: Implementation Guidance

In what Step does the system disposal strategy developed and implemented as needed?

Select the best response.

- ○ Assess Step
- ○ Prepare Step
- ● Monitor Step
- ○ Implement Step