RMF Monitor Step

Student Guide

June 2023

Center for Development of Security Excellence

Table of Contents

Course Introduction

Introduction

Risk Management Framework, or RMF, Monitor Step.

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

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.

Objectives

Before you begin, consider the following course learning objectives.

- Identify policies and guidelines for the Monitor Step in the RMF
- Identify the seven tasks and associated inputs, outputs, roles and responsibilities in the Monitor Step

Lessons:

The course is divided into two lessons:

Lesson 1: Policies and Guidelines

Lesson 2: Tasks, Potential Inputs & Expected Outputs, Roles and Responsibilities

Lesson 1: Introduction to Policies and Guidelines

Lesson Introduction

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

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

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

NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments provides guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39.

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

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

NIST Special publication (SP) 800-53A Revision 5, Assessing Security and Privacy Controls in Information Systems and Organizations provides guidance on assessing controls in information security program plans, privacy program plans, system security plans, and privacy plans.

NIST Special Publication 800-160 Volume 1: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, the purpose of this publication is:

- To provide a basis to formalize a discipline for systems security engineering in terms of its principles, concepts, and activities.

- To foster a common mindset to deliver security for any system, regardless of its scope, size, complexity, or stage of the system life cycle.
- To provide considerations and to demonstrate how systems security engineering principles, concepts, and activities can be effectively applied to systems engineering activities.
- To advance the field of systems security engineering by promoting it as a discipline that can be applied and studied
- To serve as a basis for the development of educational and training programs, including the development of individual certifications and other professional assessment criteria.

The NIST SP 800- 137; Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organization. The purpose this guideline is to assist organizations in the development of an ISCM strategy and the implementation of an ISCM program that provides awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls.

The ISCM strategy and program support ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance, as well as the ability to provide the information needed to respond to risk in a timely manner.

Review Activity

Knowledge Check 1

Which guide assists organizations in the development and the implementation of an ISCM program that provides awareness of threats of the deployed security controls?

- ○ a) NIST SP 800-37, R2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.
- ○ b) NIST SP 800-53A: Assessing Security and Privacy Controls in Information Systems and Organizations
- ○ c) NIST SP 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations
- ○ d) NIST SP 800 – 128: Guide for Security-Focused Configuration Management of Information Systems

Lesson 1 Conclusion

Lesson Conclusion

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

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

Introduction of Tasks

In this lesson, we will look at the Tasks, Inputs and Outputs, Roles and Responsibilities outlined in the Monitor Step. The Monitor Step includes seven tasks, which have an alpha designator of “M” preceding the task number.

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

- M-1: System and Environment Change
- M-2: Ongoing Assessments
- M-3: Ongoing Risk Response
- M-4: Authorization Package Updates
- M-5: Security and Privacy Reporting
- M-6: Ongoing Authorization
- M-7: System Disposal

The first Monitor Task to be discussed is Task M-1

Task M-1: System and Environment Changes

The task description is to monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.

Systems and environments of operation are in a constant state of change with changes occurring in the technology or machine elements, human elements, and physical or environmental elements.

Changes to the **technology or machine elements** include upgrades to:

- Hardware
- Software
- Firmware

Changes to the **human elements** include:

- Staff turnover
- Reduction in force

Physical and Environment: Modifications to surrounding physical and environmental elements include:

- Changes in the location of the facility or

- Physical access controls protecting the facility

Changes made by external providers can be difficult to detect.

A discipline and structured approach to managing, controlling, and documenting changes to system and environments of operation, and adherence with terms and conditions of the authorization, is an essential element of security and privacy programs.

Organizations establish configuration management and control processes to support configuration and change management.

Common activities within organizations can cause changes to systems or the environments of operation and these changes can have a significant impact on the security and privacy posture of systems.

Examples include:

- Installing hardware
- Disposing of hardware
- Changes to configurations
- Installing patches outside of the established configuration change control process

Unauthorized changes may occur because of:

- Purposeful attacks by adversaries
- Inadvertent errors by authorized personnel

In addition to adhering to the established configuration management process, organizations monitor for unauthorized changes to systems and analyze information to determine the root.

In addition to monitoring for unauthorized changes, organizations **continuously** monitor systems and environments of operation for any authorized changes that impact the privacy posture of systems.

Once the root cause of an ***unauthorized change*** or an ***authorized change*** that impacts the privacy posture of the system has been determined, organizations respond accordingly

For example, if the root cause of an unauthorized change is determined to be an adversarial attack, multiple actions could be taken such as

- o Invoking incident response processes
- o Adjusting intrusion detection and prevention tools and firewall configurations
- o Implementing additional or stronger controls to reduce the risk of future attacks.

If the root cause of an unauthorized change is determined to be a failure of staff to adhere to established configuration management processes, remedial training for certain individuals may be warranted.

Task M-1 Potential Inputs

Potential Inputs for Task M-1 include:

- Organizational continuous monitoring strategy

- Organizational configuration management policy and procedures
- Organizational policy and procedures for handling unauthorized system changes
- Security and privacy plans
- Configuration change requests/approvals
- System design documentation
- Security and privacy assessment reports
- Plans of action and milestones
- Information from automated and manual monitoring tools

Task M-1 Expected Output

The expected output for Task M-1 include updated security and privacy plans; updated plans of action and milestones; updated security and privacy assessment reports

Task M-1 Primary Responsibility

Primary Responsibilities for Task M-1 include the

- System Owner, or SO or the
- Common Control Provider
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Based on guidance from **the authorizing official, or AO, the System Owner or Common Control Provider** informs organizational officials of the need to conduct the authorization, ensures that resources are available for the effort, and provides the required system access, information, and documentation to Security Control Assessors, or SCA.

The System Owner or Common Control Provider receives the security and privacy assessment results from the control assessors. After taking appropriate steps to reduce or eliminate vulnerabilities or security and privacy risks, the SO or Common Control Provider assembles the authorization package and submits the package to the AO or the Authorizing Official Designated Representative, or AODR, for Adjudication.

The Senior Agency Information Security Officer, or SAISO, is responsible for coordinating with the senior agency official for privacy to ensure coordination between privacy and information security programs.

The role possesses the qualifications to administer security program functions; maintains security duties as a primary responsibility; and heads an office with the specific mission and resources to assist the organization in achieving trustworthy, secure information and systems in accordance with the requirements in the Federal Information Security Modernization Act, or FISMA.

The role may serve as AODR or as a SCA. The role is an inherent U.S. Government function and is therefore assigned to Government personnel only.

Organizations may also refer to the Senior Agency Information Security Officer or chief information security officer.

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 Agency Official for Privacy is responsible for Coordinating with the SAISO to ensure coordination of privacy and information security activities.

Reviewing and approving the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information.

Conducting and documenting the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency.

Establishing and maintaining a privacy continuous monitoring program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with privacy requirements and manage privacy risks.

Task M-1 Supporting Roles

The supporting roles for Task M-1 include the:

- Senior Accountable Official for Risk Management or Risk Executive Function
- Authorizing Official or Authorizing Official Designated Representative
- Information Owner or Steward
- System Security Officer
- System Privacy Officer

Review Activity

Knowledge Check 2

Task M-1

Try answering this question.

Common activities within organizations can cause changes to systems or the environments of operation. Changes can have a significant impact on the security and privacy posture of systems. Select all activities that can cause a change to the systems or the environment.

- ○ a) Installing hardware
- ○ b) Disposing of hardware
- ○ c) Opening a Spreadsheet
- ○ d) Viewing Presentation

Task M-2: Ongoing Assessments

The description of Task M-2 is to assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy.

The implementation of a robust and comprehensive continuous monitoring program helps an organization understand the security and privacy posture of its information systems.

The organizational continuous monitoring strategy addresses monitoring requirements at the organization, mission/business process, and information system levels

The system-level continuous monitoring strategy is consistent with, and supplements, the continuous monitoring strategy for the organization.

The system-level strategy addresses monitoring those controls for which monitoring is not provided as part of the continuous monitoring strategy and implementation for the organization.

After an initial system or common control authorization, the organization assesses all controls on an ongoing basis.

Ongoing assessment of the control effectiveness is part of the continuous monitoring activities of the organization.

The monitoring frequency for each control is based on the:

Organizational continuous monitoring strategy and can be supplemented by the system-level continuous monitoring strategy

Additionally, reference Task S-5 from the Select Step for supplemental system level continuous monitoring strategy.

Adherence to the terms and conditions specified by the authorizing official as part of the authorization decision are also monitored. Review Task M-1.

Ongoing control assessment continues as the information generated as part of continuous monitoring is correlated, analyzed, and reported to senior leaders.

Security Control Assessor independence during continuous monitoring introduces efficiencies into the process and may allow for reuse of assessment results in support of ongoing authorization and when reauthorization is required.

To satisfy the annual Federal Information Security Modernization Action (FISMA).

Security Assessment Requirement, organizations can use

- Assessment results from control assessments that occurred during authorization
- Ongoing authorization

- Reauthorization
- During continuous monitoring
- During testing and evaluation of systems as part of the System Development Life Cycle, or SDLC
- An audit (provided the assessment results are current and relevant to the determination of control effectiveness), and obtained by Security Control Assessors (with the required degree of independence).

Existing assessment results are re-used consistent with the Reuse Policy established by the organization and are supplemented with additional assessments as needed.

The reuse of assessment results in achieving a cost-effective security program capable of producing the evidence necessary to determine the security posture of information systems and the organization.

The use of automation to support control assessments facilitates a greater frequency, volume, and coverage of assessments.

Task M-2 Potential Inputs

Potential Inputs for Task M-2 include

- Organizational continuous monitoring strategy and system level continuous monitoring strategy, if applicable
- Security and privacy plans
- Security and privacy assessment plans
- Security and privacy assessment reports
- Plans of action and milestones;
- Information from automated and manual monitoring tools
- Organization- and System-level risk assessment results
- External assessment or audit results, if applicable

Task M-2 Expected Outputs

Expected Outputs for Task M-2 include:

Updated security and privacy assessment reports.

Task M-2 Primary Responsibilities

The Primary Responsibilities for Task M-2 belong to the Security Control Assessor

The SCA assess the controls implemented within, and inherited by, the system in accordance with the continuous monitoring strategy.

SCAs provide an assessment of the severity of the deficiencies discovered in the system, environment of operation, and common controls. Can recommend corrective actions to address the identified vulnerabilities.

SCAs prepare security and privacy assessment reports containing the results and findings from the assessment.

Task M-2 Supporting Roles

Supporting Roles for Task M-2 include:

- Authorizing Official or Authorizing Official Designated Representative
- System Owner or Common Control Provider
- Information Owner or Steward
- System Security Officer
- System Privacy Officer
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Review Activity

Knowledge Check 3

True or False: Ongoing assessment of the control effectiveness is part of the continuous monitoring activities of the organization.

○ a) True
○ b) False

Task M-3: Ongoing Risk Response

Task M-3 description is to Respond to risk, based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.

Assessment information produced by a Security Control Assessor during continuous monitoring is provided to the

- System Owner
- Common Control Provider.

Reports are provided via updated assessments; automated security/privacy management and reporting tools.

The authorizing official determines the appropriate risk response to the assessment findings.

The Authorizing Official approves responses proposed by the System Owner and Common Control Provider.

The System Owner and Common Control Provider subsequently implement the appropriate risk response.

When the risk response is “acceptance”, the findings remain documented in the security and privacy assessment reports and the findings are monitored for changes to risk factors.

When the risk response is “mitigation”, the planned mitigation actions are included and tracked using the plans of action and milestones.

If requested by the Authorizing Official, Security Control Assessors may provide recommendations for remediation actions.

Recommendations for remediation actions may also be provided by an automated security/privacy management and reporting tool.

An organizational assessment of risk and system-level risk assessment results ***guide and inform the decisions*** regarding ongoing risk response.

Addition references to review; the Organizational Assessment of Risk can be located in the Risk Management Framework - Prepare Step – Task P-3 and the System Level Risk Assessment results can be found in the RMF Prepare Step, Task P-14.

Controls that are modified, enhanced, or added as part of ongoing risk response are reassessed by the Security Control Assessors.

The controls are reassessed to ensure that the new, modified, or enhanced controls have been implemented correctly; are operating as intended; and producing the desired outcome with respect to meeting the security and privacy requirements of the system.

Task M-3 Potential Inputs

Potential Inputs for Task M-3 include:

- Security and privacy assessment reports
- Organization- and System-level risk assessment results
- Security and privacy plans
- Plans of action and milestones

Task M-3 Expected Output

Expected Outputs for Task M-3 include:

- Mitigation actions or risk acceptance decisions
- Updated security and privacy assessment reports

Task M-3 Primary Responsibilities

Primary Responsibilities for Task M- is carried out by:

- Authorizing Official
- System Owner
- Common Control Provider

These three roles work closely together. Select the roles to review.

The Authorizing Official determines the appropriate risk response to the assessment that was proposed by the System Owner and Common Control Provider.

The AO determines the appropriate risk response to the assessment findings; approves responses proposed by the System Owner and Common Control Provider and is responsible and accountable for ensuring that authorization activities and functions that are delegated to Authorizing Official Designated Representatives are carried out as specified.

The System Owner receives the security and privacy assessment results from the Security Control Assessors.

After taking appropriate steps to reduce or eliminate vulnerabilities or security and privacy risks, the System Owner assembles the authorization package and submits the package to the Authorizing Official or the Authorizing Official Designated Representative for adjudication.

Common Control Providers are responsible for:

- Ensuring the documentation of organization-defined common controls in security and privacy plans
- Ensuring that required assessments of the common controls are conducted by qualified assessors with an appropriate level of independence
- Documenting assessment findings in control assessment reports
- Producing plans of action and milestones for controls having deficiencies.

Task M-3 Supporting Roles

The Supporting Roles for Task M-3 include:

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

Review Activity

Knowledge Check

Try answering this question.

Task M-3 is to respond to risk based on the results of ongoing monitoring activities. Select the expected outputs for this task.

- a) Risk acceptance decisions
- b) Updated security and privacy assessment reports
- c) Plans of action and milestones
- d) Control implementation

Task M-4: Authorization Package Updates

The description of Task M4- is to update plans, Assessment Reports, and Plans of Action and Milestones based on the results of the continuous monitoring process.

To achieve near real-time risk management, the Organization updates

- Security and Privacy Plans
- Security and Privacy Assessment Reports
- Plans of Action and Milestones on an ongoing basis.

Updates to the plans reflect modifications to controls based on risk mitigation activities carried out by System Owners or Common Control Providers.

Updates to Control Assessment Reports reflect additional assessment activities carried out to determine control effectiveness based on implementation details in the plans.

Plans of Action and Milestones are updated based on progress made on the current outstanding items.

The Plans of Action and Milestones address security and privacy risks discovered as part of control effectiveness monitoring and describe how the System Owner or Common Control Provider intends to address those risks.

The updated Plan of Action and Milestones:

-Raises awareness of the security and privacy posture of the system
-Common controls inherited by the system.

This update supports near real-time risk management and the ongoing authorization process.

The frequency of updates to risk management information is at the discretion of the System Owner, Common Control Provider, and Authorizing Officials; these updates are in accordance with federal and organizational policies and are consistent with the organizational and system-level continuous monitoring strategies.

The updates to information regarding the security and privacy posture of the system and the common controls inherited by the system are ***accurate and timely*** since the information provided influences ***ongoing actions*** and ***decisions*** by authorizing officials and other senior leaders within the organization.

The use of automated support tools and organization-wide security and privacy program management practices ensure that authorizing officials can readily access the current security and privacy posture of the system.

Ready access to the current security and privacy posture supports continuous monitoring and ongoing authorization and promotes the near real-time management of risk to organizational operations and assets, individuals, other organizations, and the Nation.

Organizations ensure that information needed for oversight, management, and auditing purposes is not modified or destroyed when updating security and privacy plans, assessment reports, and plans of action and milestones.

An effective method to track changes to systems through configuration management procedures is necessary.

The method used will achieve transparency and traceability in the security and privacy activities of the organization.

The method will obtain individual accountability for any security or privacy actions; as well as the method to understand emerging trends in the security and privacy programs of the organization.

Task M-4 Potential Inputs

Task M-4 Potential Inputs for include:

- Security and privacy assessment reports
- Organization-and system-level risk assessment results
- Security and privacy plans
- Plans of action and milestones

Task M-4 Expected Outputs

Expected Outputs for Task M-4 include

- Updated Security and Privacy Assessment Reports
- Updated Plans of action and Milestones
- Updated risk assessment results
- Updated Security and Privacy Plans

Task M-4 Primary Responsibilities

Primary Responsibilities for Task M-4 is shared with the ***System Owner and the Common Control Provider.***

The System Owner ensures that system users and support personnel receive the requisite security and privacy training. Based on guidance from the Authorizing Official, the System Owner informs organizational officials of the need to conduct the authorization, ensures that resources are available for the effort, and provides the required system access, information, and documentation to control assessors. The System Owner receives the security and privacy assessment results from the control assessors. After taking appropriate steps to reduce or eliminate vulnerabilities or security and privacy risks, the System Owner assembles the authorization package and submits the package to the Authorizing Official or the Authorizing Official Designated Representative for adjudication.

The Common Control Providers are responsible for ensuring the documentation of organization-defined common controls in security and privacy plans; ensuring that required assessments of the common controls are conducted by qualified assessors with an appropriate level of independence; documenting assessment findings in control assessment reports; and producing Plans of Action and Milestones for controls having deficiencies. Privacy plans and privacy control assessment reports are made available to Systems Owners whose systems inherit privacy controls that are designated as common controls.

Task M-4 Supporting Roles

The supporting roles for Task M-4 include the:

- Information Owner or Steward
- System Security Officer
- System Privacy Officer
- Senior Agency Official for Privacy and the
- Senior Agency Information Security Officer

Review Activity

Knowledge Check

Try answering this question.

What is the frequency of updates to risk management information?

- ○ a) Discretion of the Control Provider
- ○ b) In accordance with federal and organizational policies
- ○ c) Annually or Semi-Annually
- ○ d) At the request of the Organization

Task M-5: Security and Privacy Reporting

The description of Task M-5 is to report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.

The results of monitoring activities are documented and reported to the AO and other selected organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.

Other organizational officials who may receive security and privacy posture reports include, for example, chief information officer, senior agency information security officer, senior agency official for privacy, senior accountable official for risk management or risk executive (function), information owner or steward.

Also included are incident response roles, and contingency planning roles.

Security and privacy posture reporting can be event-driven, time-driven, or event- and time-driven.

The reports provide the AO and other organizational officials with information regarding the security and privacy posture of the systems including the effectiveness of implemented controls.

Security and privacy posture reports describe the ongoing monitoring activities employed by System Owners or Common Control Providers.

The reports also include information about security and privacy risks in the systems and environments of operation discovered during control assessments, auditing, and continuous monitoring and how System Owners or Common Control Providers plan to address those risks.

Organizations have flexibility in the

- Breadth
- Depth
- Formality
- Form
- Format of security and privacy posture reports.

The goal is efficient ongoing communication with the Authorizing Official and other organizational officials as necessary, conveying the current security and privacy posture of systems and environments of operation and how the current posture affects individuals, organizational missions, and business functions.

At a minimum, security and privacy posture reports summarize changes to the security and privacy plans, security and privacy assessment reports, and plans of action and milestones that have occurred since the last report.

The use of automated security and privacy management and reporting tools by the organization facilitates the effectiveness and timeliness of security and privacy posture reporting.

The frequency of security and privacy posture reports is at the discretion of the organization and in compliance with federal and organizational policies.

Reports occur at appropriate intervals to transmit security and privacy information about systems or common controls but not so frequently as to generate unnecessary work or expense.

To determine if re-authorization action is necessary, Authorizing Officials use the security and privacy posture reports and consult with the Senior Accountable Official for Risk Management or Risk Executive, Senior Agency Information Security Officer, and Senior Agency Official for Privacy.

Security and privacy posture reports are:

- Marked
- Protected
- Handled in accordance with federal and organizational policies.

Security and privacy posture reports are marked, protected, and handled in accordance with federal and organizational policies.

Reporting on security and privacy posture is intended to be ongoing and should not be interpreted as requiring the time, expense, and formality associated with the information provided for the initial authorization.

Rather, reporting is conducted in a cost-effective manner consistent with achieving the reporting objectives.

Task M-5 Potential Inputs

Potential Inputs for Task M-5 include

- Security and privacy assessment reports
- Plans of action and milestones
- Organization and system-level risk assessment results
- Organization- and system-level continuous monitoring strategy
- Security and privacy plans
- Cybersecurity Framework Profile

Task M-5 Expected Outputs

Expected Outputs for Task M-5 include the Security and privacy posture reports.

Task M-5 Roles and Responsibility

Primary Responsibilities for Task M-5 are shared by:

- The System Owner
- The Common Control Provider
- The Senior Agency Information Security Officer and the
- Senior Agency Official for Privacy

The System Owner

- Ensures that system users and support personnel receive the requisite security and privacy training
- Informs organizational officials of the need to conduct the authorization
- Ensures that resources are available
- Provides the required system access, information, and documentation to Security Control Assessors
- Receives the security and privacy assessment results

- Assembles the authorization package and submits the package to the authorizing official or the authorizing official designated representative for adjudication.

The Common Control Provider is responsible for:

- Ensuring the documentation of organization-defined common controls in security and privacy plans
- Ensuring that required assessments of the common controls are conducted by qualified assessors with an appropriate level of independence
- Documenting assessment findings in control assessment reports
- Producing plans of action and milestones for controls having deficiencies.
- Privacy plans and privacy control assessment reports are made available to Systems Owners whose systems inherit privacy controls that are designated as common controls

The Senior Agency Information Security Officer (SAISO) is responsible for

coordinating with the Senior Agency Official for Privacy to ensure coordination between privacy and information security programs.

SAISO maintains security duties as a primary responsibility; and heads an office with the specific mission and resources to assist the organization in achieving trustworthy, secure information and systems in accordance with the requirements in FISMA.

The Senior Agency Information Security Officer may serve as Authorizing Official Designated Representative or as a Security Control Assessor.

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 Agency Official for Privacy is responsible for:

- Coordinating with the Senior Agency Information Security Officer to ensure coordination of privacy and information security activities
- Reviewing and approving the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information
- Designating which privacy controls will be treated as program management, common, system-specific, and hybrid privacy controls

Task M-5 Supporting Roles

The Supporting Roles that support Task M5- are:

System Security Officer and System Privacy Officer

Review Activity

Knowledge Check

Try answering this question.

Task M-5 is to report the security and privacy posture of the system. What format should be used when preparing the report?

- ○ a) Organization have flexibility in the formality and format
- ○ b) Organization must use an outline to summarize the report
- ○ c) Organizations must employ automated tools only and use the pre-formatted output
- ○ d) Organizations use an outlined format and add checkmarks

Task M-6: Ongoing Authorization

The description of Task M-6 is to review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.
To employ an ongoing authorization approach, organizations have an organization-level and system-level continuous monitoring process in place to assess implemented controls on an ongoing basis.

The findings or results from the continuous monitoring process provides ***useful information to authorizing officials to support near-real time risk-based decision making.***

In accordance with the guidance in the RMF Authorize Step - Task R-4, the Authorizing Official or Designated Representative reviews the security and privacy posture of the system (including the effectiveness of the implemented controls) on an ongoing basis to determine the current risk to organizational operations and assets, individuals, other organizations, and the Nation.

The Authorizing Official or (AO) determines the status of the current risk.

If the risk remains at an acceptable level for continued operation, the AO provides appropriate direction to the System Owner or Common Control Provider.

If the AO determines that the risk is no longer at an acceptable level for continued operation, then the AO may issue:

- Denial of authorization to operate

- Denial of authorization to use
- Denial of common control authorization.

A denial of authorization means that the information system is not authorized to operate and not placed into operation; common controls are not authorized to be provided to systems; or that the provider's system is not authorized for use by the customer organization.

The risks may change based on the information provided in the security and privacy posture reports because the reports may indicate changes to the security or privacy risk factors.

Determining how changing conditions affect organizational and individual risk is essential for managing privacy risk and maintaining adequate security.

By carrying out ongoing risk determination and risk acceptance, AOs can maintain system and common control authorizations over time, and transition to ongoing authorization.

By carrying out ongoing risk determination and risk acceptance, AOs can maintain system and common control authorizations over time and transition to ongoing authorization.

Reauthorization actions occur only in accordance with federal or organizational policies.

The AO conveys updated risk determination and acceptance results to the senior accountable official for risk management or the risk executive function.

When possible, organizations look for automated solutions to lower costs, enhance efficiency, and improve the reliability of monitoring security related information.

The use of automated support tools to capture, organize, quantify, visually display, and maintain security and privacy posture information promotes near real-time risk management regarding the risk posture of the organization.

The use of metrics and dashboards increases an organization's capability to make risk based decisions by consolidating data in an automated fashion and providing the data to decision makers at different levels within the organization in an easy-to-understand format

Task M-6 Potential Inputs

Potential Inputs for Task M-6 include:

Risk tolerance; Security and privacy posture reports; plans of action and milestones; organization-and system-level risk assessment results; and the security and privacy plans.

Task M-6 Expected Inputs

Expected Outputs for Task M-6 include:

- A Determination of Risk
- Ongoing authorization to operate
- Ongoing authorization to use
- Ongoing common control authorization
- Denial of ongoing authorization to operate
- Denial of ongoing authorization to use
- Denial of ongoing common control authorization

Task M-6 Primary Responsibility

Primary Responsibilities for Task M-6 is delegated to ***the Authorizing Official or (AO).***

The AO is a senior official or executive with the authority to formally assume responsibility and accountability for operating a system. The AO provides common controls inherited by organizational systems or use of an application from an external provider.

The AO is the ***only*** organizational official who can accept the security and privacy risk to organizational operations, organizational assets, and individuals.

The AO approves plans, plans of action and milestones, and determines whether significant changes in the information systems or environments of operation require reauthorization.

The AO is responsible and accountable for ensuring that authorization activities and functions that are delegated to Authorizing Official Designated Representative are carried out as specified.

Task M-6 Supporting Roles

Supporting Roles for Task M-6 include

- Senior Accountable Official for Risk Management or Risk Executive Function
- Chief Information Officer
- Senior Agency Information Security Officer (SAISO)
- Senior Agency Official for Privacy
- Authorized official Designated Representative (AODR)

Review Activity

Knowledge Check

Try answering this question.

Task M-6 is to review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.

If the current risk is no longer at an acceptable level for continued operation, choose the appropriate decision options. (Select all that apply)

- ○ a) Denial of Authorization to operate
- ○ b) Authorization to Use
- ○ c) Common Control authorization
- ○ d) Disable the Controls

Task M-7 System Disposal

The goal of Task M-7 is to Implement a system disposal strategy and execute required actions when a system is removed from operation.

When a system is removed from operation, several risk management actions are required.

Organizations ensure that controls addressing system disposal are implemented.

Examples include media sanitization; configuration management and control; component authenticity; and record retention.

Organizational tracking and management systems, including inventory systems, are updated to indicate the system that is being removed from service.

Security and privacy posture reports reflect the security and privacy status of the system.

Users and application owners hosted on the disposed system are notified as appropriate, and any control inheritance relationships are reviewed and assessed for impact.

This task also applies to system elements that are removed from operation

Organizations removing a system from operation update the inventory of information systems to reflect the removal.

SOs and security personnel ensure that disposed systems comply with relevant federal laws, regulations, directives, policies, and standards.

Task M-7 Potential Inputs

Potential Inputs for Task M-7 include:

Security and privacy plans; organization- and system-level risk assessment results; and the system component inventory

Task M-7 Expected Outputs

Disposal strategy; updated system component inventory; updated security and privacy plans.

Task M-7 Primary Responsibility

Primary Responsibilities for Task M-7 include the System Owner or the (SO).

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

In coordination with the system security and privacy officers, the system owner is responsible for the development and maintenance of the security and privacy plans and ensures that the system is operated in accordance with the selected and implemented controls. The SO takes appropriate steps to reduce or eliminate vulnerabilities or security and privacy risks. The SO also assembles the authorization package and submits it to the AO or the AODR for adjudication.

Task M-7 Supporting Roles

Supporting Roles for Task M-7 include:

- Authorizing Official or Authorizing Official Designated Representative
- Information Owner or Steward
- System Security Officer
- System Privacy Officer
- Senior Accountable Official for Risk Management or Risk Executive (Function)
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Review Activity

Knowledge Check

Try answering this question.

Task M-7 is to Implement a system disposal strategy and execute required actions when a system is removed from operation.

A system has been removed from operation. What risk management actions are required?

- a) Media sanitization
- b) Replace the removed component
- c) Record retention
- d) Component authenticity
- e) Notify application owners

Course Conclusion

Conclusion

Congratulations on completing Risk Management Framework (RMF) Monitor Step course.

You should now be able to perform all the listed activities:

Policies and guidelines for the Monitor step in the RMF and seven tasks and associated inputs, outputs, roles and responsibilities in the Monitor Step

For more information on the RMF Monitor Step, please visit the Resources link

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

Appendix A: Answer Key

Lesson 1: Review Activity

Knowledge Check – Policies and Guidelines

Which guide assists organizations in the development and the implementation of an ISCM program that provides awareness of threats of the deployed security controls?

.

☐ a) NIST SP 800-37, R2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.
☐ b) NIST SP 800-53A: Assessing Security and Privacy Controls in Information Systems and Organizations
☒ c) NIST SP 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations
☐ d) NIST SP 800 – 128: Guide for Security-Focused Configuration Management of Information Systems

Feedback: *The correct response is NIST SP 800-137*

Lesson 2: Review Activity

Knowledge Check

Task M-1

Common activities within organizations can cause changes to systems or the environments of operation. Changes can have a significant impact on the security and privacy posture of systems. Select all activities that can cause a change to the systems or the environment.

☒ a) Installing hardware
☒ b) Disposing of hardware
☐ c) Opening a Spreadsheet
☐ d) Viewing Presentation

Feedback: Installing hardware; Disposing of hardware.

Knowledge Check

Task M-2

True or False: Ongoing assessment of the control effectiveness is part of the continuous monitoring activities of the organization.

☒ a) True
☐ b) False

Feedback: *True*

Knowledge Check

Task M-3

Task M-3 is to respond to risk based on the results of ongoing monitoring activities. Select the expected outputs for this task.

● a) Risk acceptance decisions
● b) Updated security and privacy assessment reports
○ c) Plans of action and milestones
○ d) Control implementation

Feedback: Risk acceptance decisions and Updated security and privacy assessment reports.

Knowledge Check

Task M-4

What is the frequency of updates to risk management information?

☐ a) Discretion of the Control Provider

☒ b) In accordance with federal and organizational policies
☐ c) Annually or Semi-Annually
☐ d) At the request of the Organization

Feedback*: In accordance with federal and organizational policies*

Knowledge Check

Task M-5

Task M-5 is to report the security and privacy posture of the system. What format should be used when preparing the report?

☒ a) Organization have flexibility in the formality and format
☐ b) Organization must use an outline to summarize the report
☐ c) Organizations must employ automated tools only and use the pre-formatted output
☐ d) Organizations use an outlined format and add checkmarks

Feedback*: Organization have flexibility in the formality and format*

Knowledge Check

Task M-6

Task M-6 is to review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.

If the current risk is no longer at an acceptable level for continued operation, choose the appropriate decision options. (Select all that apply)

☒ a) Risk Management
☐ b) Approval
☐ c) Security
☐ d) Implementation

Feedback: *Denial of Authorization to operate*

Authorization to Use

Common Control Authorization

Knowledge Check

Task M-7

Try answering this question.

Task M-7 is to Implement a system disposal strategy and execute required actions when a system is removed from operation.

A system has been removed from operation. What risk management actions are required?

☒ a) Media sanitization
☒ b) Replace the removed component
☒ c) Record retention
☒ d) Component authenticity
☒e) Notify application owners

***Feedback**: Media sanitization*

Replace the removed component

Record retention

Component authenticity

Notify application owners