RMF Assess Step

Student Guide

May 2023

Center for Development of Security Excellence

Table of Contents

Course Introduction

Introduction

Welcome to Risk Management Framework, or RMF, Assess Step.

This course focuses on the Assess Step, and by the end of the course, you will be able to define the Assess Step in the RMF and identify the six tasks and associated inputs, outputs, roles and responsibilities in the Assess Step.

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.

Objectives

Before you begin, consider the following course learning objectives.

- Identify Policies and guidelines for the Assess Step in the RMF.
- Identify the six tasks and associated inputs, outputs, roles and responsibilities in the Assess Step.

Lessons:

The course is divided into two lessons:

Lesson 1: Policies and Guidelines

Lesson 2: Tasks, Potential Inputs and 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 CNSS.

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

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

OMB Circular A-130: Managing Information as a Strategic resource establishes general policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, I-T resources and supporting infrastructure and services.

The appendices to this Circular also include responsibilities for protecting federal information resources and managing Personally Identifiable Information, or PII.

FIPS 199 Standards for Security Categorization of Federal Information and Information Systems establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments. The purpose of this document is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication eight hundred-thirty nine.

Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process providing senior leaders and executives with the information needed to determine appropriate courses of action in response to identified risks. In particular, this document provides guidance for carrying out each of the steps in the risk assessment process; for example, preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment, and how risk assessments and other organizational risk management processes complement and inform each other.

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

NIST SP 800-55 Revision.1: Performance Measurement Guide for Information Security, document expands upon NIST's previous work in the field of information security measures to provide additional program-level guidelines for quantifying information security performance in support of organizational strategic goals.

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 promulgating 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

NIST SP 800-161 Revision 1- Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations provides a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures.

It also provides guidance to enterprises on how to identify, assess, select, and implement risk management processes and mitigating controls across the enterprise to help manage cybersecurity risks throughout the supply chain. The content in this guidance is the shared responsibility of different disciplines with different Supply Chain Risk Management, or SCRM, perspectives, authorities, and legal considerations

Review Activity

Knowledge Check 1

Which document provides guidance on assessing controls in information security program plans, privacy program plans, system security plans, and privacy plans? True

- ○ (a) NIST SP 800-53A - Assessing Security and Privacy Controls in Information Systems and Organizations
- ○ (b) NIST SP 800-160 v1 - Systems Security Engineering – Considerations for a Multidisciplinary approach in the Engineering of Trustworthy Secure Systems
- ○ (c) NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- ○ (d) NIST SP 800-55 Revision 1, Performance Measurement Guide for Information Security

Lesson 1 Conclusion

Lesson Conclusion

You have completed this lesson. You should now be able to define to define Policy and Guidelines associated with the Assess 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 Assess Step. The Assess Step includes six Tasks that have an alpha designator of **"A"** preceding the task number.

- Task A-1: Assessor Selection
- Task A-2: Assessment Plan
- Task A-3: Control Assessments
- Task A-4: Assessment Reports
- Task A-5: Remediation Actions
- Task A-6: Plan of Action and Milestones

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

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

Task A-1: Assessor Selection

The description is to select the appropriate assessor or assessment team for the type of control assessment to be conducted.

Organizations ensure that Security Control Assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of program management, system-specific, hybrid, and common controls, as appropriate.

This includes general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware components that are implemented.

In organizations where the assessment capability is centrally managed, the senior agency information security officer may have the responsibility of selecting and managing the Security Control Assessors or Assessment Teams for organizational systems.

As controls may be implemented to achieve security and privacy objectives, organizations consider the degree of collaboration necessary between security control and privacy control assessors.

Organizations can conduct self-assessments of controls or obtain the services of an independent Security Control Assessor.

An independent assessor is an individual or group that can conduct an impartial assessment.

Impartiality implies that assessors are free from perceived or actual conflicts of interest with respect to the determination of control effectiveness or the development, operation, or management of the system, common controls, or program management controls.

Task A-1 Potential Inputs

Task S-1 Inputs include:

- Security, privacy, and SCRM plans
- Program management control information
- Common control documentation
- Organizational security and privacy program plans
- SCRM strategy
- System design documentation
- Enterprise, security, and privacy architecture information
- Security, Privacy, and SCRM policies and procedures applicable to the system

Task A-1 Expected Outputs

Task A-1 Expected Outputs contain the selection of the assessor or assessment team responsible for conducting the control assessment.

Task A-1 Roles and Responsibilities

The primary responsibility for Task A-1 rests with the ***Authorizing Official*** or the *Authorizing Official Designated Representative*.

The Authorizing Official determines the level of assessor independence based on applicable laws, executive orders, directives, regulations, policies, or standards.

The Authorizing Official consults with all of the supporting roles to help guide and inform decisions regarding Assessor Independence.

The Authorizing Official determines the level of assessor independence based on applicable laws, executive orders, directives, regulations, policies, or standards.

The Authorizing Official consults with all of the supporting roles to help guide and inform decisions regarding Assessor Independence.

The supporting roles associated with Task A-1 include the:

- Chief Information Officer
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Review Activity

Knowledge Check - Task A-1

Try answering this question.

Control Assessments is a task associated with the Assess Step.

○ a) True

○ b) False

Task A-2: Assessment Plan

The task description is to develop, review, and approve plans to assess implemented controls. Security and privacy assessment plans are developed by Security Control Assessors.

The plans are based on:

- Implementation information contained in Security and Privacy Plans
- Program Management Control Documentation
- Common Control Documentation

Organizations may choose to develop a single, integrated security and privacy assessment plan for the system or the organization.

When developing an integrated assessment plan, the plan delineates or defines roles and responsibilities for the control assessment.

The Assessment Plans provide the objectives for control assessments and specific assessment procedures for each control.

Assessment plans also reflect the type of assessment the organization is conducting, including:

- Developmental testing and evaluation
- Independent verification and validation
- Audits, including supply chain
- Assessments supporting system and common control authorization or reauthorization

- Program management control assessments
- Continuous monitoring
- Assessments conducted after remediation actions

After the Assessment Plans are developed, they are reviewed and approved by the *authorizing official* or *the designated representative of the authorizing official.*

The Authorizing Officials are reviewing for:

- Consistency with the Security and Privacy Objectives for the organization.
- The developed plan employs procedures, methods, techniques, tools, and automation to support continuous monitoring
- Near real-time risk management
- To ensure the Plans are cost-effective.

Approved assessment plans establish expectations for the control assessments and the level of effort for the assessment. Approved assessment plans help to ensure that appropriate resources are applied toward determining control effectiveness while providing the necessary level of assurance in making such determinations.

When controls are provided by an external provider through contracts, interagency agreements, lines of business arrangements, licensing agreements, or supply chain arrangements, the *organization* can request

- Security and privacy assessment plans and assessments results
- Evidence from the provider.

Task A-2 Potential Inputs

Potential Inputs for Task A-2 include:

- Security, privacy, and SCRM plans
- Program management control information
- Common control documentation
- Organizational security and privacy program plans
- SCRM strategy
- System design documentation
- Supply chain information Enterprise, Security and Privacy Architecture Information
- Security, privacy, and SCRM policies and procedures applicable to the system

Task A-2 Expected Outputs

The Expected Outputs from Task-2 include:

The Security and privacy assessment plans approved by the authorizing official

Task A-2 Roles and Responsibilities

The Primary Responsibility for Task A dash 2 includes the ***Security Control Assessor, the Authorizing Official***, or ***the Authorizing Official Designated Representative.***

The Security Control Assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of implemented controls and control enhancements to determine the effectiveness of the controls.

Security Control Assessors provide:

An assessment of the severity of the deficiencies discovered in the system, environment of operation, and common controls. The SCA can recommend corrective actions to address the identified vulnerabilities.

For system-level control assessments, Security Control Assessors do not assess inherited controls, and only assess the system-implemented portions of hybrid controls. The SCA prepare security and privacy assessment reports containing the results and findings from the assessment.

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

The Authorizing Official determines the level of assessor independence based on applicable laws, executive orders, directives, regulations, policies, or standards.

Authorizing officials consult with all of the supporting roles to help guide and inform decisions regarding Assessor Independence.

The supporting Responsibility for Task A-2 include the:

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

Review Activity

Knowledge Check Task A-2

Assessment plans provide the objectives for Control Assessments and specific Assessment procedures for each Control.

- a) True
- b) False

Task A-3: Control Assessments

The task description is to assess the controls in accordance with the assessment procedures described in assessment plans.

Control assessments determine the extent to which the selected controls are:

- Implemented correctly
- Operating as intended
- Producing the desired outcome with respect to meeting Security and Privacy requirements for the System and the Organization.

Task A-3 Assessment Findings

The system owner, common control provider, and/or organization rely on the technical skills and expertise of **assessors** to ***assess implemented controls*** using the assessment procedures specified in assessment plans and ***provide recommendations*** on how to respond to control deficiencies ***to reduce or eliminate identified vulnerabilities or unacceptable risks.***

The senior agency official for privacy serves as the Security Control Assessor for the **privacy controls** and is responsible for;

Conducting an initial assessment of the privacy controls prior to system operation, for **assessing the controls periodically** thereafter at a frequency sufficient to ensure compliance with privacy requirements and to manage privacy risks.

Controls implemented to achieve both security and privacy objectives may require a degree of collaboration between Security and Privacy Control Assessors.

The Security Control Assessor findings are a factual reporting of whether the controls are operating as intended and whether any deficiencies in the controls are discovered during the assessment.

Task A-3 Assessment Types

Control assessments occur as early as possible in the System Development Life Cycle, or SDLC, preferably during the development phase.

Examples of Developmental Testing and Evaluation activities include:

- Design and Code Reviews

- Regression Testing
- Application Scanning

These types of assessments are referred to as:

- Developmental testing and Evaluation

They validate that the Controls are implemented correctly and are consistent with the established information Security and Privacy Architectures.

Deficiencies identified early in the SDLC can be resolved in a more cost-effective manner.

Assessments may be needed prior to source selection during the procurement process to assess potential suppliers or providers before the organization enters into agreements or contracts to begin the development phase.

Task A-3 Results of Control Assessments

The results of control assessments conducted during the SDLC can also be used during the authorization process to avoid unnecessary delays or costly repetition of assessments.

This process is consistent with ***reuse criteria*** established by the Organization.

Organizations can maximize the use of automation to conduct control assessments to

- Increase the speed, effectiveness
- Effectiveness of assessments
- Efficiency of the assessments
- Support continuous monitoring of the security and privacy posture of organizational systems.

Task A-3 Applying and Assessing Controls

Applying and assessing controls throughout the development process may be appropriate for iterative development processes.

When iterative development processes such as agile development are employed, an iterative assessment may be conducted as each cycle is completed.

A similar process is employed for assessing controls in commercial IT products that are used in the system.

Organizations may choose to begin assessing controls prior to the complete implementation of all controls in the security and privacy plans.

This type of incremental assessment is appropriate if it is more efficient or cost-effective to do so.

Task A-3 Common Controls

Common controls, which are controls that are inherited by the system, are assessed separately by Assessors chosen by the Common Control Providers or the Organization and need not be assessed as part of a system level assessment.

Organizations ensure that Assessors have access to the information system and environment of operation where the controls are implemented and to the documentation, records, artifacts, test results, and other materials needed to assess the controls. The Chief Information Officer.

This includes the **controls implemented** by external providers through **contracts, interagency agreements**, and **lines of business arrangements**, **licensing agreements, or supply chain arrangements.**

Task A-3 Reuse Assessment Results

To make the risk management process more efficient and cost-effective, organizations may choose to establish reasonable and appropriate criteria for re-using assessment results as part of organization-wide assessment policy or in the security and privacy program plans.

Think about this example for **a reuse**:

A recent audit of a system may have produced information about the effectiveness of selected controls.

Another opportunity to reuse previous assessment results may come from external programs that test and evaluate security and privacy features of commercial information technology products such as:

- Common Criteria Evaluation and Validation Program
- NIST Cryptographic Module Validation Program

If prior assessment results from the system developer or vendor are available, the Security Control Assessor, under appropriate circumstances, may incorporate those results into the assessment.

In addition, if a control implementation was assessed during other forms of assessment at previous stages of the SDLC, such as unit testing, functional testing, acceptance testing, organizations may consider potential reuse of those results to reduce duplication of efforts.

And finally, assessment results can be reused to support reciprocity, for example, assessment results supporting an authorization to use.

Task A-3 Reuse Assessment Resource

NIST SP 800-53A Revision 5 - Assessing Security and Privacy Controls in Information Systems and Organizations; addresses and Provides guidance for the*:*

- Assess and Monitor steps of the Risk Management Framework (RMF)
- Security and Privacy Control Assessment Processes
- How to build effective assessment plans
- How to Analyze and Manage Assessment Results,
- How to Tailor Assessment Procedures.

Task A-3 Potential Inputs

The Potential Inputs for Task A-3 include:

- Security and privacy assessment plans
- Security and privacy plans
- External assessment
- Audit results—if applicable.

Task A-3 Expected Outputs

The Expected Outputs for Task A-3 include;

Completed control assessments and associated assessment evidence.

Task A-3 Roles and Responsibilities

The Primary Responsibility for Task A-3 belong to the Security Control Assessor.

The Security Control Assessors provides an assessment of the severity of the deficiencies discovered in the system, environment of operation, and common controls, and can recommend corrective actions to address the identified vulnerabilities.

For system-level control assessments, Security Control Assessors **do not** assess inherited controls, and only assess the system-implemented portions of hybrid controls.

Security Control Assessors prepare security and privacy assessment reports containing the results and findings from the assessment.

Security Control Assessors can:

- Provide an assessment of the severity of the deficiencies discovered in the system, environment of operation, and common controls

- Recommend corrective actions to address the identified vulnerabilities

For system-level control assessments, Security Control Assessors:

- **Do not** assess inherited controls, and **only assess** the system-implemented portions of hybrid controls
- Prepare security and privacy assessment reports containing the results and findings from the assessment

The Supporting Roles for Task A-3 include the:

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

Review Activity

Knowledge Check Task A-3

True or False. The Security Control Assessor findings are factual reporting of whether the controls are operating as intended and whether any deficiencies in the controls are discovered.

○ a) True
○ b) False

Task A-4: Assessment Reports

The description for Task A-4 is to prepare the assessment reports documenting the findings and recommendations from the control assessments.

The results of the security and privacy control assessments, including:

- Recommendations for correcting deficiencies in the implemented controls are documented in the assessment reports by Security Control Assessors.
- Organizations may develop a single, integrated security and privacy assessment report.

Task A-4 Assessment reports are:

- Key documents in the system or the common control authorization package that is developed for the authorizing officials.

The Assessment reports include:

- Information based on assessor findings necessary to determine the effectiveness of the controls implemented within, or inherited-by, the information system

Task A-4 Level of Detail

Assessment reports are an important factor in a determining risk to organizational operations and assets, individuals, other organizations, and the Nation by the authorizing official.

The format and the level of detail provided in assessment reports are appropriate for the type of control assessment conducted, for example,

- Developmental testing and evaluation
- Independent verification and validation
- Independent assessments supporting information system or the common control authorizations or reauthorizations
- Self-assessments
- Assessments after remediation actions
- Independent evaluations or audits
- Assessments during continuous monitoring.

The reporting format may also be prescribed by the organization.

Task A-4 Interim Reports

Control assessment results obtained during the SDLC are

- Documented in an interim report and
- Included in the final Security and Privacy assessment reports.

Development of interim reports that document assessment results from relevant phases of the SDLC reinforces the concept that **assessment reports are evolving documents.**

Interim reports are used, as appropriate, to inform the final assessment report.

Task A-4 Executive Summary

Organizations may choose to develop an executive summary from the control assessment findings

The Executive Summary provides authorizing officials and other interested individuals in the organization with an abbreviated version of the Assessment Reports that includes;

- A synopsis of the assessment
- Findings,
- Recommendations for addressing deficiencies in the controls.

Task A-4 Potential Inputs

The Potential Inputs for Task A-4 include completed control assessments and associated assessment evidence.

Task A-4 Expected Outputs

The Expected Outputs for Task A-4 include the completed security and privacy assessment reports detailing the assessor findings and recommendations.

Task A-4 Roles and Responsibilities

The Primary Responsibility for Task A-4 belong to the Security Control Assessor.

The Security Control Assessor is an individual, group, or organization

- Responsible for conducting a comprehensive assessment of implemented controls
- Control enhancements to determine the effectiveness of the controls.
- Provide an assessment of the severity of the deficiencies discovered in the system, environment of operation, and Common Controls
- Recommend corrective actions to address the identified vulnerabilities

For system-level control assessments, Security Control Assessors **do not** assess inherited controls, and only assess the system-implemented portions of hybrid controls

Supporting Roles for Task A-4 include the

- System Owner

- Common Control Provider
- System Security Officer and
- System Privacy Officer

Review Activity

Knowledge Check Task A-4

Try answering this question.

True or False. The results of the security and privacy control Assessments are documented in the Assessment Report

- ○ a) True
- ○ b) False

Task A-5: Remediation Actions

Task A-5, the Task description is to conduct initial remediation actions on the controls and reassess remediated controls.

The security and privacy assessment reports:

Describe deficiencies in the controls that could not be resolved during the development of the system or that are discovered post-development. Such control deficiencies may result in security and privacy risks -including supply chain risks.

The findings generated during control assessments **provide information that facilitates risk responses based on organizational risk tolerance and priorities**

The authorizing official, in consultation and coordination with the **system owners** and other organizational officials, may decide that certain findings represent significant, unacceptable risk and require immediate remediation actions.

Additionally, it may be possible and practical to conduct initial **remediation actions** for assessment findings that can be quickly and easily remediated with existing resources.

If initial remediation actions are taken, assessors will reassess the controls.

Task A-5 Control Reassessments

Control Reassessments determine the extent to which remediated **controls 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.

The Security Control Assessors will update the assessment reports with the findings from the reassessment, but will not change the original assessment results.

Task A-5 Updated Plans

The security and privacy plans are updated based on the findings of the control assessments and any remediation actions taken.

The updated plans reflect:

- State of the controls after the initial assessment
- Any modifications by the system owner or common control provider in addressing recommendations for corrective actions.

At the completion of the control assessments, security and privacy plans contain an accurate description of implemented controls, including compensating controls.

Task A-5 Addendum

Organizations can prepare an addendum to the security and privacy assessment reports that provides an opportunity for system owners and common control providers to respond to **initial assessment findings.**

The addendum may include, for example, information regarding initial remediation actions taken by system owners or common control providers in response to assessor findings.

The addendum can also provide the system owner or common control provider perspective on the findings. This may include providing additional explanatory material, rebutting certain findings, and correcting the record.

The addendum does not change or influence the initial assessor findings provided in the reports.

Information provided in the addendum is considered by authorizing officials when making risk-based authorization decisions.

Organizations implement a process to determine ***the initial actions*** to take regarding the control deficiencies identified during the assessment.

This process can address:

- Vulnerabilities and risks
- False positives
- Other factors
- Security and privacy posture of the system and organization
- Effectiveness of system-specific, hybrid, and common controls

The issue resolution process can also ensure that only substantive items are identified and transferred to the plan of actions and milestones.

Findings from a system-level control assessment may necessitate an update to the system risk assessment and the organizational risk assessment.

The updated Risk Assessments and any inputs from the Senior Accountable Official for Risk Management or Risk Executive function determines the:

- Initial Remediation Actions
- Prioritization of those actions.

System Owners and Common Control Providers may decide, based on a System or Organizational risk assessment, that certain findings are inconsequential and present no significant security or privacy risk.

Such findings are retained in the security and privacy assessment reports and monitored during the monitoring step.

Task A-5 Review Findings

The authorizing official is responsible for:

The authorizing official is responsible for **reviewing and understanding the assessor findings** and for **accepting the security and privacy risks, including any supply chain risks that result from the operation of the system or the use of common controls.**

In all cases, Organizations:

- Review assessor findings to determine the significance of the findings
- Determine whether the findings warrant any further investigation or remediation.

Senior leadership involvement in the mitigation process is necessary to

- Ensure that the Organization's resources are effectively allocated in accordance with organizational priorities
- Providing resources to the systems that are supporting the most critical missions and business functions
- Correcting the deficiencies that pose the greatest risk

Task A-5 Potential Inputs

The Potential Inputs for Task A -5 include

- Completed security and privacy assessment reports with findings and recommendations
- Security and privacy plans
- Security and privacy assessment plans
- Organization- and system-level risk assessment results

Task A-5 Expected Outputs

The Expected Outputs for Task A-5 include

- Completed initial remediation actions based on the security and privacy assessment reports
- Changes to implementations reassessed by the assessment team
- Updated security and privacy assessment reports
- Updated security and privacy plans including changes to the control implementations

Task A-5 Roles and Responsibilities

The Primary Responsibility for Task A-5 belongs to ***the System Owner*, *the Common Control Provider, and the Security Control Assessor.***

Based on Task A-5, you will find that the System Owner, the Common Control Provider, and Security Control Assessor collaborate on this Task.

The System Owner is responsible for

- The development and maintenance of the security and privacy plans
- Ensuring that the system is operated in accordance with the selected and implemented controls.
- Deciding who has access to the system.
- Assembling the authorization package
- Submitting the package to the Authorizing Official or the Authorizing Official Designated Representative for adjudication

The Common Control provider, along with System Owners are responsible for deciding that certain findings are inconsequential and present no significant security or privacy risk.

The Security Control Assessor receives documentation informing them that resources are available for the effort, and that the required system access, information, and documentation are available.

The Security Control Assessors also receive the Security and Privacy Assessment results from the System Owner.

The supporting roles include:

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

- Privacy Engineer
- System Security Officer
- System Privacy Officer

Review Activity

Knowledge Check A-5

Try answering this question.

Identify the Task that requires Remediation Actions.

- ○ a) Task A-2
- ○ b) Task A-3
- ○ c) Task A-4
- ○ d) Task A-5

Task A-6: Plan of Action and Milestones

The task description is to prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.

The plan of action and milestones are included as part of the authorization package.

The plan of action and milestones;

Describes the actions that are planned to correct deficiencies in the controls identified during the assessment of the controls and during continuous monitoring.

The plan of action and milestones includes tasks to be accomplished with a recommendation for completion before or after system authorization, as well as resources required to accomplish the tasks

The milestones are established to meet the tasks; and the scheduled completion dates are set for the milestones and tasks.

The plan of action and milestones is reviewed by the authorizing official to ensure there is agreement with the remediation actions planned to correct the identified deficiencies.

These Remediation Actions are used to monitor progress in completing the actions

Task A-6 Residual Risk

Deficiencies are accepted by the authorizing official as:

- Residual Risk
- Remediated during the Assessment
- Prior to submission of the Authorization Package to the authorizing official

Plan of action and milestones entries are **not** necessary when deficiencies are accepted by the authorizing official as residual risk.

Task A-6 Deficiencies

Deficiencies identified during assessment and monitoring are:

- Documented in the assessment reports, which can be retained within an automated security/privacy management and reporting tool to maintain an effective audit trail.

Task A-6 Action Plan

Organizations develop Plans of Action and Milestones based on assessment results obtained from:

- Control Assessments
- Audits
- Continuous monitoring
- Executive Orders
- Directives
- Policies
- Regulations
- Standards
- Guidance

Task A-6 Process

Organizations implement a consistent process for developing plans of action and milestones that:

- Use a prioritized approach to risk mitigation that is uniform across the organization.
- Risk Assessment guides the prioritization process for items included in the plan of actions and milestones.

Task A-6 Prioritization Process

The Prioritization Process ensures that plans of action and milestones are identified and prioritized by:

- Specific deficiencies in the controls
- Criticality of the identified Control deficiencies
- Proposed risk mitigation approach to address the identified deficiencies in the controls

Risk mitigation resources include, for example, personnel, new hardware or software, and tools.

Task A-6 Potential Inputs

The Potential Inputs for Task A-6 includes

- Updated security and privacy assessment reports
- Updated security and privacy plans
- Organization- and system-level risk assessment results
- Organizational Risk Management Strategy and Risk Tolerance

Task A-6 Expected Outputs

The Expected Outputs for Task A-6 includes

A plan of action and milestones detailing the findings from the security and privacy assessment reports that are to be remediated.

Task A-6 Roles and Responsibilities

The Primary Responsibility belong to the System Owner and the Common Control Provider

The System Owner is responsible for:

- The development and maintenance of the security and privacy plans
- Ensures that the system is operated in accordance with the selected and implemented controls.
- Decides who has access to the system.
- Assembles the authorization package
- Submits the package to the Authorizing Official or the Authorizing Official Designated Representative for adjudication

The Common Control Provider, along with the System Owner, may decide that certain findings are inconsequential and present no significant security or privacy risk.

The Supporting Roles associated with Task A-6 include

- Information Owner or Steward
- System Security Officer
- System Privacy Officer
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy
- Security Control Assessor
- Chief Acquisition Officer

Review Activity

Knowledge Check A-6

Try answering this question.

Deficiencies accepted by the authorized official as residual risk are not entered in the Plan of Action.

○ a) True
○ b) False

You have completed this lesson. You should now be able to define:

You should now be able to define:

○ Assess Step Tasks
○ Potential Inputs and Expected Outputs
○ Roles and Responsibilities associated with each Task

Course Conclusion

Conclusion

Congratulations on completing the RMF Assess Step Course.

You should now be able to identify:

- Identify Policies and guidelines for the Assess Step in the RMF.
- Identify the six tasks and associated inputs, outputs, roles and responsibilities in the Assess Step.

For more information on the RMF Assess Step, please visit the Course Resources link.

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

Appendix A: Answer Key

Lesson 1: Review Activity

Knowledge Check 1 – Policies and Guidelines

Which document provides guidance on assessing controls in information security program plans, privacy program plans, system security plans, and privacy plans?

☒ a) NIST SP 800-53A - Assessing Security and Privacy Controls in Information Systems and Organizations

☐ b) NIST SP 800-160 v1 - Systems Security Engineering – Considerations for a Multidisciplinary approach in the Engineering of Trustworthy Secure Systems

☐ c) NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

☐ d) NIST SP 800-55 Revision 1, Performance Measurement Guide for Information Security

Feedback: *The correct response is a) SP 800-53A*

Lesson 2: Review Activity

Knowledge Check Task A-1

True or False. Control Assessments is a task associated with the Assess Step.

☒ (a) True

☐ (b) False

Feedback: *The correct response Is, False*

Knowledge Check Task A-2

Assessment plans provide the objectives for Control Assessments and specific Assessment procedures for each Control.

☒ a) True

☐ b) False

Feedback: *The correct response is, True.*

Knowledge Check Task A-3

True or False. The Security Control Assessor findings are factual reporting of whether the controls are operating as intended and whether any deficiencies in the controls are discovered.

☒ a) True
☐ b) False

Feedback: *The correct response Is, True.*

Knowledge Check Task A-4

True or False. The results of the security and privacy control Assessments are documented in the Assessment Report

☒ a) True
☐ b) False

Feedback*: Correct response Is, True*

Knowledge Check Task A-5

Select the correct response. Identify the Task that requires Remediation Actions.

☐ a) Task A-2
☐ b) Task A-3
☐ c) Task A-4
☒ d) Task A-5

Feedback*: The correct response is D)*

Knowledge Check *Task* A-6

True or False. Deficiencies accepted by the authorized official as residual risk are not entered in the Plan of Action.

☒ a) True
☐ b) False

Feedback*: The correct response is A).*