Applying Assessment and Authorization in the NISP

Student Guide

November 2021

Center for Development of Security Excellence

Table of Contents

Lesson 1: Course Introduction

Introduction

Welcome

[Jack] “Hey, there. I’m Jack. It’s good to meet you. It’s pretty busy around here right now. We won a big classified contract recently and are getting set up to work on that. Our Facility Security Officer appointed me as our Information System Security Manager. At the moment, that means I’m working toward getting our Information Systems authorized to process, store, and access the classified information our contract requires. I’ll be relying on the 32 CFR Part 117 National Industrial Security Program Operating Manual and the DCSA Assessment and Authorization Process Manual, or DAAPM, to guide me through the process and tell me the requirements.”

[Narrator] Welcome to the Applying Assessment and Authorization in the NISP course! This course walks you through each step of the Assessment and Authorization, or A&A, process. The course is based on the 32 CFR Part 117 NISPOM Rule (NISPOM) and the DCSA Assessment and Authorization Process Manual, or DAAPM. These two documents, which are available through the course resources, detail how DCSA implements the Risk Management Framework, or RMF, for cleared contractor Information Systems under DCSA oversight.

Objectives

Here is the course objective.

- Describe the Assessment and Authorization (A&A) process in accordance with the guidance as outlined in the DCSA Assessment and Authorization Process Manual (DAAPM) and the 32 CFR Part 117 National Industrial Security Program Operating Manual (32 CFR Part 117 NISPOM)

Lesson 2: Getting Started with the A&A Process

Introduction

Objectives

[Jack] “Before I start the A&A process, I need to make sure I’m prepared for what’s coming up. DCSA has a website with Risk Management Framework resources for contractors that I need to review, and I need to read the DAAPM as well. Lastly, I need to make sure I have our sponsorship documentation, so I don’t get delayed later.”

This lesson reviews the steps you should take to prepare for the Assessment and Authorization, or A&A, process.

Here are the lesson objectives.

- Identify the purpose of the Assessment and Authorization (A&A) process
- Identify the prerequisites of the A&A process

A&A Process

Overview

The A&A process consists of seven steps: Prepare Step, Categorize Step, Select Step, Implement Step, Assess Step, Authorize Step, and Monitor Step. Each of the steps involves specific tasks that result in specific outputs.

Purpose

The A&A process is based on the Risk Management Framework, or RMF. All federal government agencies use the RMF to facilitate reciprocity. DCSA uses the A&A process to authorize cleared contractors’ new Information Systems to process, store, and access classified information. DCSA also uses the A&A process to re-authorize a cleared contractor’s existing Information System when it undergoes security- relevant changes or it approaches the expiration date of its Authorization to Operate, or ATO.

Terms and Definitions

Reciprocity: From Committee on National Security Systems Instruction (CNSSI) 4009: Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse Information System resources and/or to accept each other's assessed security posture in order to share information.

Security-relevant changes: Any changes/actions affecting the availability, integrity, authentication, confidentiality, or non- repudiation of an Information System or its environment. Examples include changes to the identification and authentication, auditing, malicious code detection, sanitization, operating system, firewall, router tables and intrusion detection systems (IDS) of a system, or any changes to its location or operating environment.

RMF: Risk Management Framework

A&A: Assessment and Authorization

DCSA: Defense Counterintelligence and Security Agency

ATO: Authorization to Operate

A&A Prerequisites

Overview

As the Information System Security Manager, or ISSM, for a cleared contractor, there are several tasks you should perform before beginning the A&A process. First, make sure that you possess and understand the sponsorship and security documentation associated with your contract. Next, review the materials available on the DCSA RMF website. As you get started in the A&A process, contact your local Information System Security Professional, or ISSP, with any questions or concerns.

Terms and Definitions

RMF: Risk Management Framework

DCSA: Defense Counterintelligence and Security Agency

ISSP: Information System Security Professional

Documentation

The sponsorship and security documentation associated with your contract summarize the security requirements that apply. First, you must have sponsorship documentation. Typically, this is a properly completed DD Form 254, Contract Security Classification Specification. Block 11c indicates the necessity to receive and generate classified material and must be marked "Yes." The 32 CFR Part 117 National Industrial Security Program

Operating Manual, or 32 CFR Part 117 NISPOM, defines other sponsorship documentation that may be used instead, such as a framework agreement or request for proposal.

You must also possess a Security Classification Guide, or SCG. The SCG is a collection of precise, comprehensive guidance that states which elements of information are classified, their classification levels, the reasons for classification, and when the information can be downgraded or declassified. The Information Owner, or IO, provides the SCG.

DCSA RMF Resources

The DCSA website provides cleared contractors with information and resources about the RMF. The website includes the current version of the DCSA Assessment and Authorization Process Manual, or DAAPM, job aids and templates, training resources and toolkits, and other policies and resources. Make sure that you take the time to read the DAAPM, as it provides detailed guidance on every step of the process.

The DCSA RMF website is available through the course resources.

NISP eMass Account

During the Prepare Step, you will register the system in the NISP eMASS instance. NISP eMASS is the government-owned, web-based application that manages the A&A process. The NISP eMass has replaced OBMS as the system of record.

Throughout the process, the ISSM uses NISP eMASS to populate information and upload artifacts, including the generating of a Security Plan, and any supporting artifacts for the Information System. When you create an account, NISP eMASS generates a System Record.

Terms and Definitions

NISP eMASS: National Industrial Security Program (NISP) Enterprise Mission Assurance Support Service (eMASS). NISP eMASS is the portal to manage the A&A process.

A&A: Assessment and Authorization

The NISP Industry eMASS Operation Guide is available through the course resources.

Review Activities

Review Activity 1

What is the purpose of the Assessment and Authorization (A&A) process?

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

□ Facilitate reciprocity

□ Authorize cleared contractors' new Information Systems for classified processing

□ Re-authorize cleared contractors' existing Information Systems when they undergo security-relevant changes

Review Activity 2

Before you begin the Assessment and Authorization (A&A) process, which of these tasks should you perform?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

□ Purchase hardware and software

□ Review your sponsorship documentation and security classification guidance

□ Review the materials on the DCSA Risk Management Framework (RMF) website

□ Assign qualified personnel

Conclusion

Summary

You have completed the Getting Started with the A&A Process lesson.

Lesson 3: Prepare Step

Introduction

Lesson Objective

[Jack] "Now I am going to focus on my organization's security and privacy risks using the Risk Management Framework, or RMF. I will follow the Prepare step of the RMF process to focus on executing the organization's essential activities, mission and business processes, and system levels to help the organization manage its security and privacy risks using the RMF."

This lesson reviews the Prepare step of the Assessment and Authorization, or A&A, process.

Here is the lesson objective. Take a moment to review it.

- Describe the tasks and outputs associated with the Prepare Step

Roles

The major role players associated with the Prepare step are the organization requesting the authorization, key management personnel, the ISSM/ISSO, the ISO, and the FSO.

Prepare Step Tasks

Organization Level Tasks

- The Prepare step tasks are divided into the following two categories: Organization Level Tasks and System Level Tasks. All Prepare Step Tasks shall have an alpha designator of "P" preceding the task number. To illustrate, let's begin by reviewing the Organization Level Prepare Tasks.
- The first Organization Level Prepare Step Task will be Task P-1:
- Identifying and assigning individuals to key roles in the execution of the RMF.

The next task is Task P-2:

- Establishing a risk management strategy for the organization that includes a determination and expression of organizational risk tolerance.

The next organization level task, Task P-3, involves:

- Completing an organization-wide risk assessment or updating an existing risk assessment.

This task is optional:

Task P-4 is establishing and making available organizationally tailored control baselines and/or cybersecurity framework profiles.

Task P-5 is identifying, documenting, and publishing common controls available for inheritance. Task P-6 is also optional and involves prioritizing organizational systems with the same impact level. Task P-7: Developing and implementing an organization-wide strategy for monitoring control effectiveness. This is the final task of the Organization Level tasks.

Next are the System Level Prepare step tasks.

System Level Tasks

The ISSM (also known as ISSM/ISSO), with assistance from the ISSO and Key Management Personnel (KMP), is responsible for the following tasks:

- Task P-8 is identifying business functions and mission/business processes that the system is intended to support.
- Task P-9 is identifying system stakeholders.
- Task P-10 is identifying and prioritizing stakeholder assets.
- Task P-11 is determining authorization boundaries.
- Task P-12 is identifying the types of information processed, stored, and transmitted by the system.
- Task P-13 is identifying and understanding all stages of the information life cycle for each information type processed, stored, or transmitted by the system.
- Task P-14: Performing a system level risk assessment or updating an existing risk assessment. The purpose of the risk assessment is to inform decision makers and support risk responses by identifying:
    a. Relevant threats.
    b. Vulnerabilities, both internal and external, to the organization.
    c. Impacts to the organization that may occur given the potential for threats exploiting vulnerabilities.
    d. Likelihood that harm will occur.

Risk assessment outcomes should be reviewed to examine the facility’s threat picture and to determine if tailoring controls are required. The results are documented in the Risk Assessment Report (RAR). The ISSM will review applicable SCGs and verify the classification level of RAR results.

- Task P-15: Defining and prioritizing security requirements.
- Task P-16: Determining the placement of the system within the enterprise architecture.

- Task P-17: Allocating security requirements to the system and to the environment in which the system operates.
- Task P-18: Registering the system in the NISP eMASS instance. During new system registration, the following details will be documented:
    a. System Information.
    b. Authorization Information.
    c. Roles.

  Follow instructions in the NISP eMASS Industry Operation Guide and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage. This was the final system level task.

The NISP eMASS has replaced OBMS as the system of record. The following applies:

a. All security plans must be submitted via the NISP eMASS instance located at:
b. https://nisp.emass.apps.mil/.
c. Industry must have a DCSA sponsor and take the DISA eMASS training to establish a NISP eMASS account. Reference the NISP eMASS Training Access and Procedures for Cleared Industry.
d. Industry eMASS users will be assigned to the CAC – 1 role.

Prepare Step Outputs

Task Outputs

We have finished reviewing all the tasks that make up the Prepare Step. Various outputs are produced at the Organization Level such as roles being assigned, and Risk Assessment Reports being developed.

Various outputs are produced at the System Level such as Mission/Business Process, Business Functions, and NISP eMASS System Record.

To validate the completion of Organization Level and System Level Tasks, you should now have completed the following: Role Assignments and Risk Assessment Report.

While at the System Level, your final output is a NISP eMASS System of Record.

Organization Level – Task Outputs

- RMF Role Assignments
- Risk Management Strategy
- Risk Assessment Report
- Baselines and/or Profiles established and made available
- List of Common Providers (Common Controls Available for Inheritance)
- Prioritization (of a same impact level) Conducted
- Continuous Monitoring Strategy

System Level – Task Outputs

- Mission/Business Process; Business Functions
- System Stakeholder List
- Asset List
- Documented Authorization Boundary
- System Information Types Identified
- System Information Types
- Risk Assessment Report (RAR)
- Security Requirements
- Security Architecture
- NISP eMASS System Record

Review Activities

Review Activity 1

Prepare Step Tasks are divided into two categories, which are _______ and ________.

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

- □ Operational Level Tasks
- □ Organization Level Tasks
- □ System Level Tasks
- □ Mission Level Tasks

Review Activity 2

Question 1 of 4. The results of this action are used to determine if tailored security controls are required.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Assign qualified personnel to RMF roles
- □ Register System in NISP eMASS
- □ Risk Assessment
- □ Continuous Monitoring Strategy

Question 2 of 4. This is not an output of the Prepare Step.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Assign qualified personnel to RMF roles
- □ Register System in NISP eMASS
- □ Risk Assessment
- □ Continuous Monitoring Strategy

Question 3 of 4. This is the final System Level Prepare Step task.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Assign qualified personnel to RMF roles
- ☐ Register System in NISP eMASS
- ☐ Risk Assessment
- ☐ Continuous Monitoring Strategy

Question 4 of 4. The first Organization Level Prepare Step task is:

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Assign qualified personnel to RMF roles
- ☐ Register System in NISP eMASS
- ☐ Risk Assessment
- ☐ Continuous Monitoring Strategy

Review Activity 3

Question 1 of 3. Which of the following documents the results of the risk and threat assessment?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Initial Security Plan
- ☐ Risk Assessment Report (RAR)
- ☐ Supporting artifacts

Question 2 of 3. Which of the following is responsible for the System Level tasks?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Information System Security Manager/Officer (ISSM/ISSO)
- ☐ Industrial Security Representative (IS Rep)
- ☐ Organization Requesting Authorization (ORA)

Question 3 of 3. What is the purpose of reviewing risk assessment outcomes?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ To examine the facility's threat picture and to determine if tailoring controls are required
- □ To document common controls available for inheritance
- □ To determine the placement of the system within the enterprise architecture

Conclusion

Summary

You have completed the Prepare Step lesson.

Lesson 4: Categorize Step

Introduction

Lesson Objective

[Jack] “Now I am going to categorize the Information System based on the impact due to a loss of confidentiality, integrity, and availability of the system and the information it will process.”

This lesson reviews the Categorize Step of the Assessment and Authorization, or A&A, process.

Here is the lesson objective. Take a moment to review it.

- Describe the tasks and outputs associated with the Categorize Step

Roles

The major role players associated with the Categorize Step are the ISSM/ISSO and the ISO.

Categorize Step Tasks

Tasks

Just as in the previous step, the Categorize step will be preceded by an Alpha designator “C”. For example, the first task of the Categorize step will be Task C-1: Describing and documenting the characteristics of the system. Task C-2 is Categorizing the system. Task C-3 is Reviewing security categorization results. Task C-4 is Populating information not entered during new system registration and documenting categorization results in eMASS.

Let’s examine these in greater detail. The Categorize step focuses on categorizing the system. Security impact levels are defined as Low, Moderate, or High for each of the three system security objectives: C-I-A. Systems will be categorized based on the impact due to a loss of C-I-A of the information or system.

Impact Level	**Confidentiality (unauthorized disclosure of information)**	**Integrity (unauthorized modification or destruction of information)**	**Availability (disruption of access to or use of information)**
Low	N/A* *limited* adverse effect on organizational operations , assets, or individuals	N/A* *limited* adverse effect on organizational operations , assets, or individuals	N/A* *limited* adverse effect on organizational operations , assets, or individuals
Moderate	*serious* adverse effect on organizational operations, assets, or individuals	*serious* adverse effect on organizational operations, assets, or individuals	*serious* adverse effect on organizational operations, assets, or individuals
High	*severe or catastrophic* adverse effect on organizational operations, assets, or individuals	*severe or catastrophic* adverse effect on organizational operations, assets, or individuals	*severe or catastrophic* adverse effect on organizational operations, assets, or individuals

**By definition, the impact of loss of Confidentiality must be either moderate or high.*

Once you have assessed the risk and established the system boundaries, you must categorize the Information System by taking into account the impact that organizational operations, assets, or individuals would experience if a loss of confidentiality, integrity, or availability of the information or the system were to take place.

The DCSA baseline categorization is a Moderate impact due to loss of confidentiality and a Low impact due to loss of integrity or availability. All Information Systems seeking DCSA authorization must meet or exceed this baseline.

The categorization of the information is determined using the contractual requirements established by the IO in DD Form 254 or other approved sponsorship documentation, the type of system or network, and the results of the risk and threat assessment.

Task C-3: Reviewing security categorization results. The categorization of the data and system must be coordinated with the IO. The IO is the authority for determining categorization and must be involved in the process.

Task C-4: Populating information not entered during new system registration and documenting categorization results in eMASS.

During the Categorize step, Industry eMASS users will begin building the security plan.

Follow instructions in the NISP eMASS Industry Operation Guide and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

Outputs

Categorize Step results in the creation of three main items: a System Description, an updated NISP eMASS System Record, and the System Categorization.

Review Activities

Review Activity 1

Who are the major role players associated with the Categorize step?

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

- □ ISSO
- □ ISSM
- □ ISO

Review Activity 2

Question 1 of 3. This will occur based on the impact of documenting the characteristics of the system.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Building the security plan in NISP eMASS
- □ Categorization of the Information System
- □ The System Description

Question 2 of 3. During the Categorize step, Industry eMASS users will begin this action.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Building the security plan in NISP eMASS
- □ Categorization of the Information System
- □ The System Description

Question 3 of 3. This considers the impact on the organization due to a loss of confidentiality, integrity, or availability of the information or the system.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Building the security plan in NISP eMASS
- □ Categorization of the Information System
- □ The System Description

Review Activity 3

What are the process outputs of the Categorize step?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- □ System Description
- □ Updated eMASS System Record
- □ Risk Assessment Report
- □ Security Categorization

Conclusion

Summary

You have completed the Categorize Step lesson.

Lesson 5: Select Step

Introduction

Objectives

[Jack] "Now that I've categorized the Information System, I'll select security controls based on that categorization to reduce the amount of risk associated with the system."

This lesson reviews the Select Step of the Assessment and Authorization, or A&A, process.

Here is the lesson objective. Take a moment to review it.

- Describe the tasks and outputs associated with the Select Step

Roles

The major role players associated with the Select Step are the ISSM/ISSO. The ISO assists the ISSM/ISSO with this task.

Select Step Tasks

Overview

There are five primary tasks to complete in this step, and each task will have an alpha designator of "S" preceding the task number. First, the ISSM/ISSO selects the security controls necessary to protect the system commensurate with the risk. Next, the ISSM tailors the controls as needed. Then, the ISSM designates controls as system-specific, hybrid, or common controls and allocates the specific system elements.

Next, the ISSM designates a strategy to continuously monitor the effectiveness of the security controls. Finally, the ISSM documents security controls to include tailoring actions.

To complete the Select step of the A&A process, the Information System Security Manager, or ISSM, needs the Risk Assessment Report, or RAR, created in the Prepare Step. Recall that the RAR documents the results of the risk and threat assessment. These results influence the selection of security controls used to mitigate the risk associated with the Information System.

Let's examine Select Step Tasks S-1 through S-5 in greater detail.

Task S-1

In Task S-1, the ISSM selects the security controls necessary to protect the system commensurate with the risk. The baseline controls depend on the categorization of the Information System determined in the Categorize Step.

Recall that DCSA establishes a minimum baseline of Moderate-Low-Low. There are three types of security controls: system specific, common, and hybrid.

Task S-2

In Task S-2, the ISSM tailors the baseline security controls as needed. As the ISSM, you may tailor in additional controls to supplement the baseline or tailor out controls that either do not apply or are satisfied by mitigating factors. Tailoring out controls depends on the program and the system requirements. If you choose to tailor controls out, you must provide a justification in the security plan.

Task S-3

System specific security controls apply to a particular Information System, while common controls apply to multiple Information Systems. As the name suggests, hybrid controls blend system-specific and common controls. Refer to the DCSA Assessment and Authorization Process Manual, or DAAPM, for a complete list of baseline security controls. In addition, the ISSM may also choose to implement the DCSA-approved overlay.

An overlay is a fully specified set of controls, control enhancements, and supplemental guidance employed by organizations to provide a disciplined and structured approach to tailoring applied to specific mission or business functions, environments of operation, and technologies.

The DAAPM contains the DCSA-approved overlay.

Some users are general users. They are able only to process data. Other users are privileged users. They have elevated system access and may control the actions that general users can or cannot take.

The DAAPM is available through the course resources.

Common

Common controls are inheritable by one or more organizational Information Systems. This means that the controls applied to a parent system can also be applied to a child system. Common controls are typically provided by the organization or the infrastructure and have several benefits.

They may support multiple Information Systems efficiently and effectively as a common capability. This promotes more cost-effective and consistent security across the organization, may simplify risk management activities, and reduce the number of controls to document and test.

Hybrid

Hybrid controls are implemented in part as a common control and in part as a system-specific control. Be sure to take them into account as they may serve as a template for further control refinement.

Task S-4

In Task S-4, the ISSM develops a strategy to continuously monitor the effectiveness of the security controls. Continuous monitoring is a critical part of risk management and is used to determine whether the planned security control implementation is acceptable.

It includes configuration management and control, security impact analyses on proposed changes, assessment of selected security controls, and security status reporting.

Refer to the *Continuous Monitoring* course available through the Center for Development of Security Excellence, or CDSE, to learn more.

Task S-5

In Task S-5, the industry eMASS users will update the security plan in order to reflect the selection of security controls. To do this, update in NISP eMASS:

- Security Plan with
    - Security Controls Set with Supporting Rationale
    - Implementation Status
    - Responsible Entities
    - Estimated Completion

Be sure to follow instructions in the NISP eMASS Industry Operation Guide and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

Task Outputs

We have just discussed all the tasks that make up the Select Step. Completion of the step should result in the following process outputs: Security Control Selection, List of Tailored Controls, Overlay Selection, Updated System Details, Continuous Monitoring Strategy.

Review Activities

Review Activity 1

Which of the following must you have before beginning the Select Step of the Assessment and Authorization (A&A) process?

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

□ Certification Statement

□ Plan of Action and Milestone (POA&M)

□ Risk Assessment Report (RAR)

□ Continuous Monitoring Plan

Review Activity 2

Select the task that best fits each description. Then check your answers in the Answer Key at the end of this Student Guide.

This task is based on the results of the categorization of the categorization.

□ Develop a continuous monitoring strategy

□ Tailor the controls

□ Submit the security plan and supporting artifacts

□ Security Control Selection

Review Activity 3

Which of the following are process outputs from the Select Step?

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

□ Risk Assessment Report (RAR)

□ Security Control Selection

□ List of Tailored Controls

□ Overlay Selection

□ Plan of Action and Milestone (POA&M)

Conclusion

Summary

You have completed the Select Step lesson.

Lesson 6: Implement Step

Introduction

Objectives

[Jack] “Next, I will work on implementing the security controls for my system. I’ll document the implementation and look for any weaknesses as I go.”

This lesson reviews the Implement Step of the Assessment and Authorization, or A&A, process. All Implement tasks will have an alpha designator of “I” preceding the task number.

Here is the lesson objective. Take a moment to review it.

- Describe the tasks and outputs associated with the Implement Step

Roles

The major role players associated with the Implement Step are the ISSM and ISSO.

Implement Step Tasks

Tasks

In this step, the ISSM implements the security controls identified in the Security Control Selection. The controls should be implemented in accordance with NIST SP 800-53 and will include any additional information necessary to describe how the security capability is achieved such as planned inputs, expected behavior, and expected outputs.

Industry eMASS users will continue completing the security plan. If using an artifact to support the implementation of a control, you will need to provide artifact name, description, type, evidence, expiration date, and other information as applicable.

Outputs

We have just discussed all the tasks that make up the Implement Step. Completion of this step should result in the following process outputs:

- Implementation Plan
- System Level Continuous Monitoring (SLCM) Strategy
- Supporting Artifacts

Review Activities

Review Activity 1

The implementation plan will include additional information such as:

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

- □ Planned Inputs
- □ Risk Assessment Report (RAR)
- □ Expected Behavior
- □ Expected Outputs

Review Activity 2

During the Implement Step, Industry eMASS users will continue completing the _____?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Security Assessment Report (SAR)
- □ Contingency Plan
- □ Risk Assessment Report (RAR)
- □ Security Plan

Conclusion

Summary

You have completed the Implement Step lesson.

Lesson 7: Assess Step

Introduction

Objectives

[Jack] “Okay, the security controls are in place. Now to make sure they are implemented correctly, operating as intended, and meet the security requirements.”

This lesson reviews the Assess Step of the Assessment and Authorization, or A&A, process.

Here is the lesson objective. Take a moment to review it.

- Assess the security controls applicable to the system and determine if the controls are implemented correctly, operating as intended, and producing the desired outcome.

Roles

The major role players associated with the Assess step are: the ISSM/ISSO, ISSP, and the ISO.

Assess Step Tasks

Controls and Procedures

Before the Information System Security Manager, or ISSM, begins the Assess Step of the A&A process, the security controls must be implemented. Once they are implemented, the ISSM uses the security procedures defined in the security plan to assess the controls.

Assess Step Tasks – Part 1

Assess Step Tasks are divided into three parts:

- Part I – Industry (Tasks A-1 through A-8),
- Part II – ISSP (Tasks A-9 through A-11), and
- Part III – Industry (Task A-12).

All Assess Step Tasks shall have an alpha designator of “A” preceding the task number.

Assess Step Tasks – Part I

The ISSM/ISSO is responsible for the Part I Assess Step Tasks. The ISSM/ISSO will conduct the security controls self-assessment utilizing the DISA Security Content Automation Protocol (aka “SCAP”) SCAP Compliance Checker (aka “SCC”) for automated checks and all appropriate baseline/benchmark Security Technical Implementation Guides (aka “STIGs”). The self-assessment process is to ensure the security controls are implemented as organizationally intended to meet the security requirements for the system.

Note: If not contractually mandated, systems are not required to be configured for compliance to STIG requirements. However, Industry is still required to harden systems in order to appropriately manage risk.

Assess Step Tasks – Part I

The ISSM/ISSO will conduct remediation actions to address the deficiencies identified during the self-assessment. The ISSM/ISSO will develop a POA&M for unacceptable risks identified during the self-assessment.

The ISSM/ISSO will review applicable SCG and verify classification level of all security plan artifacts. It is important to note that if supporting artifacts are deemed classified, the assigned ISSP should be contacted, for guidance. The ISSM/ISSO will finalize the security plan for review and authorization consideration in eMASS. In order to provide a complete security plan and facilitate the assessment and authorization process, supporting artifacts should be included.

NOTE: If annotating the vulnerability is determined to be classified as per the SCG, indicate in eMASS that details will be maintained on-site.

The ISSM/ISSO will document the self-assessment results and determine if all aspects of the security controls, including the Control Correlation Identifiers (CCIs), are compliant, non-compliant, or not applicable. Industry eMASS users will finalize the security plan.

Assess Step Tasks – Part I

The Industry eMASS users will ensure the following are complete:

- Required system details
- Implementation Plan and SLCM
- Risk Assessment for all non-compliant controls
- Authorization activities artifacts
- All Assessment Procedures (APs)/CCIs tested, and results applied
- POA&M is accurate and addresses all non-compliant controls

Once the ISSM confirms that the security plan reflects actual state of security controls, the ISSM moves the package to the next stage of the CAC (CAC-2 role/ISSP) for validation, using the Bulk Processing feature in eMASS. The ISSP will complete the validation/assessment.

We have completed all tasks associated with Part I. Now let’s take a look at the Part II tasks.

Assess Step Tasks – Part II

The ISSP will review the final security plan and supporting artifacts. It is important to note that, if the security plan is not acceptable and/or has insufficient documentation, it will be documented in the Security Assessment Report (SAR) and may result in the ISSP recommending a Denial of Authorization to Operate (DATO). If acceptable, an on-site assessment will be scheduled, or waived in rare circumstances.

The ISSP will conduct the on-site assessment. The on-site assessment will include the following:

- Assessing the applicable technical security controls, system configuration, manual and not reviewed (NR) checks using the most up-to-date applicable DISA compliance scanning tools (e.g., SCC, STIGs, and associated benchmarks).
- Identifying any necessary remediation/mitigation actions for the POA&M.

Any weaknesses and/or deficiencies will be documented in the SAR and the ISSP will make risk-based recommendations based on the assessment results. The ISSP presents the recommendations to the AO and the AO makes the final decision. The ISSP will validate the controls and record the results in NISP eMASS.

We have completed all tasks associated with Part II. Now let’s take a look at the Part III tasks.

Assess Step Tasks – Part III

The ISSM/ISSO, with assistance from the ISO, is responsible for the following. Developing/ Updating POA&M based on findings and recommendations from the Security Assessment Report (SAR). The ISSM will update the POA&M, to include identifying corrective actions, determining resources required, documenting milestone completion dates, and addressing any residual findings. The POA&M will identify:

- Tasks to be accomplished.
- Resources required to accomplish the tasks.
- Any milestones in meeting the tasks, to include percentage completed.
- Scheduled completion dates for the milestones.
- Mitigating Actions.

Outputs

The process outputs for the Assess Step include:

- Assessment of Security Controls
- Remediation Actions
- Finalized Security Plan
- Review and Validation of Security Controls
- POA&M
- SAR

Note: Only upload unclassified materials to eMASS.

Review Activities

Review Activity 1

Assess Step Tasks are divided into how many parts?

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

□ One

□ Two

□ Three

□ None

Review Activity 2

Question 1 of 4. Assess the security controls.

Select the role responsible for each task or output. Then check your answers in the Answer Key at the end of this Student Guide.

□ ISSM/ISSO

□ SCA/ISSP

□ Both

Question 2 of 4. Verify the classification level of the security plan.

Select the role responsible for each task or output. Then check your answers in the Answer Key at the end of this Student Guide.

□ ISSM/ISSO

□ SCA/ISSP

□ Both

Question 3 of 4. Create the Security Assessment Report (SAR)

Select the role responsible for each task or output. Then check your answers in the Answer Key at the end of this Student Guide.

□ ISSM/ISSO

□ SCA/ISSP

□ Both

Question 4 of 4. Make authorization recommendation.

Select the role responsible for each task or output. Then check your answers in the Answer Key at the end of this Student Guide.

- □ ISSM/ISSO
- □ SCA/ISSP
- □ Both

Conclusion

Summary

You have completed the Assess Step lesson.

Lesson 8: Authorize Step

Introduction

Objectives

[Jack] “The SCA accepted all of the materials for my system, so now I wait for an authorization decision from the AO.”

This lesson reviews the Authorize Step of the Assessment and Authorization, or A&A, process.

Here is the lesson objective. Take a moment to review it.

- Describe the tasks and outputs associated with Authorize Step

Roles

The major role players associated with the Authorize Step are: the ISSP and the AO.

Authorize Step Tasks

Authorize Step Tasks – Part I

Authorize Step Tasks are divided into two parts:

- Part I – ISSP (Tasks R-1 through R-3) and
- Part II – AO (Tasks R-4 through R-6)

All Authorize Step Tasks shall have an alpha designator of “R” preceding the task number.

The ISSP is responsible for the Authorize Step – Part I tasks. Let’s take a look at these.

The ISSP will finalize the security plan by ensuring the information needed by the AO to make risk-based decisions is included in the security authorization package. For systems inheriting common controls for specific security capabilities, the security plan for the common controls must also be included.

The ISSP (CAC-2 role) validates all Security Controls in NISP eMASS, initiates the appropriate workflow, and submits the finalized system security authorization package via the PAC for review and approval.

As a PAC user within NISP eMASS, the ISSP will apply an assessment decision. The ISSP will assess the package and provide a complete SAR containing:

- Security Control Assessor Executive Summary
- Overall System Cybersecurity Risk
- Assessment Date

Additionally, the ISSP will recommend an Authorization Termination Date or ATD, to the AO. When complete, the ISSP will submit the package to the next role in the approval chain.

Authorize Step Tasks – Part II

The Authorizing Official, or AO, is responsible for the Authorize Step – Part II tasks. Let's take a look at these.

The AO will determine whether the identified risks need to be mitigated prior to authorization. Important Note: The explicit acceptance of risk is the responsibility of the AO. The AO will issue an authorization decision to the ISSM, and other organizational officials. The document contains:

- Authorization decision
- Terms and conditions for the authorization
- ATD – Processing beyond this date is unauthorized

The ATD cannot be greater than 1,095 calendar days (3 years). The ATD is determined by the AO.

The AO will apply one of the following authorization decisions within eMASS:

- ATO
- Authorization to Operate with Conditions (ATO-C)
- Interim Authorization to Test (IATT)
- DATO
- Decommissioned

Note: It is important to note that if necessary, the AO can add a residual risk statement as a comment or an artifact. The AO will have up to 30 days after a package has been authorized to update the authorization information.

Warning: An ATO cannot be issued if a non-compliant security control has a HIGH or VERY HIGH residual risk level.

The package is a static snapshot in time once it enters the approval process.

AUTHORIZE STEP SUPPORTING INFORMATION

If the live system data is changed while the package is being reviewed, the package will not be updated. The package information cannot be edited or changed except for the following:

a. All POA&M items contained in the package are completely locked except for “severity” during the review process until approved by the AO when an authorization decision is applied.

b. Changes to the “severity” POA&M items in the package will be reflected in the live system.

c. The risk assessment summary contained in the package can be updated during the review process until it is finalized by the ISSP.

d. Changes to the Risk Assessment Summary in the Risk Assessment package will be reflected in the live system.

e. An assessment and authorization decision applied to the package will be reflected in the live data.

Outputs

We have just discussed all the tasks that make up the Authorize Step. Completion of this step should result in the following process outputs:

- Submission of System Security Authorization Package to the PAC
- SAR Executive Summary
- Application of Approval Status to Security Plan
- Authorization Decision

Review Activities

Review Activity 1

Who issues the authorization decision for the Information System and the common controls inherited by the system?

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

- □ Information System Security Manager (ISSM)
- □ Security Control Assessor (SCA)
- □ Authorizing Official (AO)
- □ Information Owner (IO)

Review Activity 2

The authorization decision document contains which of the following?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Authorization Decision
- □ Decommissioning Document
- □ Terms and conditions for the authorization
- □ ATD – Processing beyond this date is unauthorized

Review Activity 3

All POA&M items contained in the package are completely locked except for ________ during the review process until approved by the AO when an authorization decision is applied.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Completion Date
- □ POC
- □ Severity
- □ Estimated Cost

Review Activity 4

The explicit acceptance of risk is the responsibility of the ________.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Security Control Assessor (SCA)
- □ Authorizing Official (AO)
- □ Information System Security Manager (ISSM)
- □ Information System Owner (ISO)

Review Activity 5

Who determines the ATD?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- □ Security Control Assessor (SCA)
- □ Authorizing Official (AO)
- □ Information System Security Manager (ISSM)
- □ Information System Owner (ISO)

Conclusion

Summary

You have completed the Authorize Step lesson.

Lesson 9: Monitor Step

Introduction

Lesson Objective

[Jack] "Now that the system is up and running, I'm using the continuous monitoring strategy in the security plan to make sure the controls still do what they need to do. This kind of ongoing security and risk assessment supports near real-time risk management that keeps my organization running."

This lesson reviews the Monitor Step of the Assessment and Authorization, or A&A, process.

Here is the lesson objective. Take a moment to review it.

- Describe the tasks and outputs associated with the Monitor Step

Roles

The major role players associated with the Monitor Step are: the ISSM/ISSO, the ISO, the FSO, and the AO.

Overview

This step focuses on maintaining an ongoing situational awareness about the security posture of the system and organization. A continuous monitoring strategy includes:

- Maintaining and executing configuration management processes.
- Determining the security impact of proposed or actual changes to the system and its operating environment.
- Assessing selected security controls (including system-specific, hybrid, and common controls) based on the approved continuous monitoring strategy.
- Ensuring security documentation is updated and maintained based on the results of continuous monitoring activities.
- Providing security status reports on the security posture of the system to appropriate officials in accordance with the continuous monitoring strategy.
- Supporting risk management decisions to help maintain organizational risk tolerance at acceptable levels.

Monitor Step Tasks

Monitor Step Tasks – Part I

Monitor Step Tasks are divided into three parts:

- Part I – Industry (Tasks M-1 through M-7)
- Part II – ISSP (Tasks M-8, M-9) and
- Part III – AO (Tasks M-10, M-12).

All Monitor Step Tasks shall have an alpha designator of “M” preceding the task number.

The ISSM/ISSO, with assistance from the ISO, FSO, and other system stakeholders, is responsible for the Monitor Step – Part I tasks.

Let’s take a look at Part I – Industry.

The ISSM/ISSO will monitor all technical, management, and operational security controls employed within and inherited by systems in accordance with the continuous monitoring strategy. The frequency of monitoring is based on the continuous monitoring strategy developed by the ISO/ISSM.

The ISSM/ISSO will conduct ongoing assessments of control effectiveness in accordance with the continuous monitoring strategy. The ISSM/ISSO will conduct remediation/mitigation based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M. The ISO and CCP initiate remediation actions on outstanding items listed in the POA&M and findings produced during the continuous monitoring of security controls. An assessment of risk (either formal or informal) informs organizational decisions with regard to conducting ongoing remediation/mitigation actions.

The ISSM/ISSO will reflect any modifications to security controls in the updated security plan. Continuous monitoring status reports will reflect additional assessment activities carried out. Additionally, the ISSM/ISSO will update the POA&M to report progress made on outstanding items. Organizations will ensure the original information needed for oversight, management and auditing purposes is not modified or destroyed.

Any anomalies or issues must be reported immediately to the ISSP. The ISSM/ISSO shall maintain a log of continuous monitoring activities on-site. The ISSM/ISSO will use NISP eMASS to submit all appropriate administrative and security-relevant documentation to DCSA. Security status reports will be appropriately marked, protected, and handled in accordance with Federal and organizational policies.

The ISSM/ISSO will implement a decommission plan and update the security plan on the live system in NISP eMASS as required. Follow instructions in the NISP eMASS Industry Operation Guide and reference the NISP eMASS Information and Resource Center.

Task M-5: Any anomalies or issues (e.g., security control deviations, threat environment changes, incidents impacting system risk level, security relevant changes, etc.) must be reported immediately to the ISSP.

The ISSM is required to maintain a log of continuous monitoring activities on-site. Continuous monitoring documentation will be assessed during the SVA and other engagement activities (e.g., Advise & Assist visits, periodic communications, etc.). Actions associated with continuous monitoring activities are a method to meet self-inspection requirements outlined in NISPOM, Chapter 8, Section 101h. The ISSM will be able to demonstrate that all the weekly, quarterly, and annual activities have taken place as part of their self-inspection.

All appropriate administrative and security relevant documentation will be submitted to DCSA using eMASS. Security status reporting can be event driven, time driven, or both. The goal is ongoing communication with DCSA to convey the current security state of the system and its environment of operation. Security status reports will be appropriately marked, protected, and handled in accordance with Federal and organizational policies.

Task M-6: A decommission plan addresses the approach used to securely transition the system and system elements into a decommissioned state.

The results of the risk assessment drive decisions on the appropriate actions taken during decommissioning. Those actions include:

a. Ensuring no classified, sensitive, or privacy information will be exposed during the decommissioning process.
b. Ensuring control inheritance relationships are reviewed and assessed for impact. If the system undergoing decommissioning provides inherited controls, ensure “disinherited” controls are implemented elsewhere if they are still required.
c. Ensuring artifacts and supporting documentation are disposed of according to their sensitivity or classification in accordance with the approved system security authorization package.

When requesting the decommission of an authorized system, the ISSM will initiate a Decommission Workflow in eMASS.

Monitor Step Tasks – Part II

We’ve completed Monitor Step Tasks Part I; now let’s move on to Part II – ISSP.

The ISSP’s review determines whether the operational risk remains acceptable to the organization, assets, individuals, other organizations, and/or to national security. The ISSP may provide recommendations as to appropriate remediation actions. Security controls that have changed during continuous monitoring are reassessed.

The ISSP verifies all decommissioning activities and ensures proper sanitation IAW procedures outlined in the security plan and DAAPM.

Upon completion of Part II activities by the ISSP, the AO will complete Part III.

Monitor Step Tasks – Part III

We’ve completed Monitor Step Tasks Part I and Part II.

Now let’s move on to Part III – AO.

The AO uses the information provided by the ISSP to determine if the authorization decision needs to be changed from an ATO to a DATO or if reauthorization action is necessary.

The AO formally approves the decommissioning systems.

Note: Task M-11 is omitted per the DAAPM.

Outputs

The Monitor Step produces several outputs, depending on the outcome of continuous monitoring or whether decommissioning is required.

During monitoring, the following outputs are produced:

- Decommissioning Plan
- Updated Security Plan
- Updated POA&M
- All security controls approved according to the Continuous Monitoring Strategy

Review Activities

Review Activity 1

When does continuous monitoring begin?

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

- □ Only after full Authorization to Operate (ATO) is issued
- □ As soon as the contract is awarded
- □ When the Security Control Assessor (SCA) indicates
- □ Once the Information System receives ATO or ATO with conditions

Review Activity 2

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

Acronyms:
ISSM – Information System Security Manager

SCA – Security Controls Assessor

AO – Authorizing Official

Question 1 of 6. Select the role responsible for each task and output.

Task 1: Conducts remediation actions.

- □ AO
- □ ISSM
- □ SCA

Question 2 of 6. Select the role responsible for each task and output.

Task 2: Reviews security status reports.

- □ AO
- □ ISSM
- □ SCA

Question 3 of 6. Select the role responsible for each task and output.

Task 3: Updates the security plan.

□ AO
□ ISSM
□ SCA

Question 4 of 6. Select the role responsible for each task and output.

Task 4: Determines when reauthorization is needed.

□ AO
□ ISSM
□ SCA

Question 5 of 6. Select the role responsible for each task and output.

Task 5: Verifies proper sanitation of storage media.

□ AO
□ ISSM
□ SCA

Question 6 of 6. Select the role responsible for each task and output.

Task 6: Formally approves the decommissioning plan.

□ AO
□ ISSM
□ SCA

Conclusion

Summary

You have completed the Monitor Step lesson.

Lesson 10: Course Conclusion

Conclusion

Summary

[Jack] That process was a lot of work, but it’s worth it to protect our national security. As you get started on this process for your own organization, remember that the DCSA Assessment and Authorization Process Manual and the 32 CFR Part 117 National Industrial Security Program Operating Manual Rule are there to provide the requirements and guidance.

[Narrator] This course reviewed each step in the Assessment and Authorization, or A&A, process. Remember to refer to the course resources for additional materials, including the DCSA Assessment and Authorization Process Manual, or DAAPM.

Lesson Review

Here is a list of the lessons in the course.

Lessons:
- Course Introduction
- Getting Started with the A&A Process
- Prepare Step
- Categorize Step
- Select Step
- Implement Step
- Assess Step
- Authorize Step
- Monitor Step
- Course Conclusion

Lesson Summary

Congratulations. You have completed the *Applying Assessment and Authorization in the NISP course.*

You should now be able to describe the Assessment and Authorization (A&A) process in accordance with the guidance as outlined in the DCSA Assessment and Authorization Process Manual (DAAPM) and the 32 CFR Part 117 National Industrial Security Program Operating Manual Rule (NISPOM).

To receive credit for this course, you must take the Applying Assessment and Authorization in the NISP examination. Follow the instructions on screen to access the online exam..

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

What is the purpose of the Assessment and Authorization (A&A) process?

Select all that apply.

- □ Facilitate reciprocity *(correct response)*
- □ Authorize cleared contractors' new Information Systems for classified processing *(correct response)*
- □ Re-authorize cleared contractors' existing Information Systems when they undergo security-relevant changes *(correct response)*

Feedback: *The A&A process facilitates reciprocity and is used by DCSA to both authorize new Information Systems and re-authorize existing systems when necessary.*

Review Activity 2

Before you begin the Assessment and Authorization (A&A) process, which of these tasks should you perform?

Select all that apply.

- □ Purchase hardware and software
- □ Review your sponsorship documentation and security classification guidance *(correct response)*
- □ Review the materials on the DCSA Risk Management Framework (RMF) website *(correct response)*
- □ Assign qualified personnel *(correct response)*

Feedback: *You should possess and understand your sponsorship documentation and security classification guidance, review the materials available on the DCSA RMF website including the DCSA Assessment and Authorization Process Manual (DAAPM), and assign qualified personnel.*

Lesson 3 Review Activities

Review Activity 1

Prepare Step Tasks are divided into two categories, which are _______ and ________.

Select all that apply.

- □ Operational Level Tasks
- □ Organization Level Tasks *(correct response)*
- □ System Level Tasks *(correct response)*
- □ Mission Level Tasks

Feedback: *Prepare Step Tasks are divided into two categories: Organization Level Tasks and System Level Tasks.*

Review Activity 2

Question 1 of 4. The results of this action are used to determine if tailored security controls are required.

Select the best response.

- □ Assign qualified personnel to RMF roles
- □ Register System in NISP eMASS
- □ Risk Assessment *(correct response)*
- □ Continuous Monitoring Strategy

Feedback: *The results of the risk assessment are used to determine if it is necessary to tailor security controls to reduce risk to an acceptable level.*

Question 2 of 4. This is not an output of the Prepare Step.

Select the best response.

- □ Assign qualified personnel to RMF roles
- □ Register System in NISP eMASS
- □ Risk Assessment
- □ Continuous Monitoring Strategy *(correct response)*

Feedback: *Continuous Monitoring Strategy is not an output of the Prepare step.*

Question 3 of 4. This is the final System Level Prepare Step task.

Select the best response.

□ Assign qualified personnel to RMF roles

□ Register System in NISP eMASS *(correct response)*

□ Risk Assessment

□ Continuous Monitoring Strategy

Feedback: *Registering your system in NISP eMASS is the final System Level Prepare Step task.*

Question 4 of 4. The first Organization Level Prepare Step task is:

Select the best response.

□ Assign qualified personnel to RMF roles *(correct response)*

□ Register System in NISP eMASS

□ Risk Assessment

□ Continuous Monitoring Strategy

Feedback: *The first Organization Level Prepare Step task is: Assign risk management roles.*

Lesson 4 Review Activities

Review Activity 1

Who are the major role players associated with the Categorize step?

Select all that apply.

- □ ISSO (correct response)
- □ ISSM (correct response)
- □ ISO (correct response)

Feedback: *The ISSO, ISSM, and ISO are all major role players associated with the Categorize Step.*

Review Activity 2

Question 1 of 3. This will occur based on the impact of documenting the characteristics of the system.

Select the best response.

- □ Building the security plan in NISP eMASS
- □ Categorization of the Information System *(correct response)*
- □ The System Description

Feedback: *The System Description is the result of describing and documenting the characteristics of the system.*

Question 2 of 3. During the Categorize step, Industry eMASS users will begin this action.

Select the best response.

- □ Building the security plan in NISP eMASS *(correct response)*
- □ Categorization of the Information System
- □ The System Description

Feedback: *During the Categorize step, Industry eMASS users will begin building the security plan.*

Question 3 of 3. This considers the impact on the organization due to a loss of confidentiality, integrity, or availability of the information or the system.

Select the best response.

- □ Building the security plan in NISP eMASS
- □ Categorization of the Information System *(correct response)*
- □ The System Description

Feedback: *An Information System's categorization is based on the impact due to a loss of confidentiality, integrity, or availability. The DCSA baseline categorization is Moderate-Low-Low.*

Review Activity 3

What are the process outputs of the Categorize step?

Select all that apply.

- □ System Description *(correct response)*
- □ Updated eMASS System Record *(correct response)*
- □ Risk Assessment Report
- □ Security Categorization *(correct response)*

Feedback: *The process outputs of the Categorize step are the System Description, an Updated eMASS System Record, and the Security Categorization.*

Lesson 5 Review Activities

Review Activity 1

Which of the following must you have before beginning the Select Step of the Assessment and Authorization (A&A) process?

Select the best response.

- □ Certification Statement
- □ Plan of Action and Milestone (POA&M)
- □ Risk Assessment Report (RAR) *(correct response)*
- □ Continuous Monitoring Plan

Feedback: *The RAR contains information needed to select appropriate security controls.*

Review Activity 2

This task is based on the results of the categorization of the categorization.

Select the best response.

- □ Develop a continuous monitoring strategy
- □ Tailor the controls
- □ Submit the security plan and supporting artifacts
- □ Security Control Selection *(correct response)*

Feedback: *The security control selection is based upon the results of the categorization.*

Review Activity 3

Which of the following are process outputs from the Select Step?

Select all that apply.

- □ Risk Assessment Report (RAR)
- □ Security Control Selection *(correct response)*
- □ List of Tailored Controls *(correct response)*
- □ Overlay Selection *(correct response)*
- □ Plan of Action and Milestone (POA&M)

Feedback: *The process outputs of the Select step are Security Control Selection, List of Tailored Controls, and Overlay Selection.*

Lesson 6 Review Activities

Review Activity 1

The implementation plan will include additional information such as:

Select all that apply.

- □ Planned Inputs (correct response)
- □ Risk Assessment Report (RAR)
- □ Expected Behavior (correct response)
- □ Expected Outputs (correct response)

Feedback: *The implementation plan will include any additional information necessary to describe how the security capability is achieved, such as (a) Planned Inputs, (b) Expected Behavior, and (c) Expected Outputs.*

Review Activity 2

During the Implement Step, Industry eMASS users will continue completing the _____?

Select the best response.

- □ Security Assessment Report (SAR)
- □ Contingency Plan
- □ Risk Assessment Report (RAR)
- □ Security Plan *(correct response)*

Feedback: *During the Implement Step, Industry eMASS users will continue completing the security plan.*

Lesson 7 Review Activities

Review Activity 1

Assess Step Tasks are divided into how many parts?

Select the best response.

- □ One
- □ Two
- □ Three *(correct response)*
- □ None

Feedback: *Assess Step Tasks are divided into 3, which are Part I-Industry, Part II-ISSP and Part III-Industry.*

Review Activity 2

Question 1 of 4. Assess the security controls.

Select the role responsible for each task or output.

- □ ISSM/ISSO
- □ SCA/ISSP
- □ Both *(correct response)*

Feedback: *The ISSM/ISSO self-assesses the Information System, and the SCA/ISSP conducts an on-site assessment to validate operation.*

Question 2 of 4. Verify the classification level of the security plan.

Select the role responsible for each task or output.

- □ ISSM/ISSO (correct response)
- □ SCA/ISSP
- □ Both

Feedback: *IAW Task A-4, the ISSM/ISSO will verify the classification level of all security plan artifacts.*

Question 3 of 4. Create the Security Assessment Report (SAR)

Select the role responsible for each task or output.

□ ISSM/ISSO

□ SCA/ISSP *(correct response)*

□ Both

Feedback: *The SCA/ISSP creates a SAR after conducting the on-site assessment.*

Question 4 of 4. Make authorization recommendation.

Select the role responsible for each task or output.

□ ISSM/ISSO

□ SCA/ISSP *(correct response)*

□ Both

Feedback: *The SCA/ISSP makes an authorization recommendation to the Authorizing Official (AO).*

Lesson 8 Review Activities

Review Activity 1

Who issues the authorization decision for the Information System and the common controls inherited by the system?

Select the best response.

- □ Information System Security Manager (ISSM)
- □ Security Control Assessor (SCA)
- □ Authorizing Official (AO) *(correct response)*
- □ Information Owner (IO)

Feedback: The AO issues the authorization decision.

Review Activity 2

The authorization decision document contains which of the following?

Select all that apply.

- □ Authorization Decision *(correct response)*
- □ Decommissioning Document
- □ Terms and conditions for the authorization *(correct response)*
- □ ATD – Processing beyond this date is unauthorized *(correct response)*

Feedback: *The authorization decision document contains the authorization decision, the terms and conditions for the authorization, and ATD.*

Review Activity 3

All POA&M items contained in the package are completely locked except for ________ during the review process until approved by the AO when an authorization decision is applied.

Select the best response.

- □ Completion Date
- □ POC
- □ Severity *(correct response)*
- □ Estimated Cost

Feedback: *All POA&M items contained in the package are completely locked except for Severity during the review process until approved by the AO when an authorization decision is applied.*

Review Activity 4

The explicit acceptance of risk is the responsibility of the ________.

Select the best response.

- □ Security Control Assessor (SCA)
- □ Authorizing Official (AO) *(correct response)*
- □ Information System Security Manager (ISSM)
- □ Information System Owner (ISO)

Feedback: *The explicit acceptance of risk is the responsibility of the Authorizing Official (AO).*

Review Activity 5

Who determines the ATD?

Select the best response.

- □ Security Control Assessor (SCA)
- □ Authorizing Official (AO) *(correct response)*
- □ Information System Security Manager (ISSM)
- □ Information System Owner (ISO)

Feedback: *Authorizing Official (AO) determines the ATD.*

Lesson 9 Review Activities

Review Activity 1

When does continuous monitoring begin?

Select the best response.

- □ Only after full Authorization to Operate (ATO) is issued
- □ As soon as the contract is awarded
- □ When the Security Control Assessor (SCA) indicates
- □ Once the Information System receives ATO or ATO with conditions *(correct response)*

Feedback: *Continuous monitoring begins as soon as the Information System is operational and has been issued ATO or ATO with conditions.*

Review Activity 2

Question 1 of 6. Select the role responsible for each task and output.

Task 1: Conducts remediation actions.

- □ AO
- □ ISSM *(correct response)*
- □ SCA

Feedback: *The ISSM role conducts remediation actions and updates the security plan*

Question 2 of 6. Select the role responsible for each task and output.

Task 2: Reviews security status reports.

- □ AO
- □ ISSM
- □ SCA *(correct response)*

Feedback: *The SCA reviews the reported security status of the Information System and evaluates whether risk remains at an acceptable level.*

Question 3 of 6. Select the role responsible for each task and output.

Task 3: Updates the security plan.

- □ AO
- □ ISSM *(correct response)*
- □ SCA

***Feedback:** The ISSM updates and maintains security documentation associated with the Information System, including the security plan.*

Question 4 of 6. Select the role responsible for each task and output.

Task 4: Determines when reauthorization is needed.

- □ AO (correct response)
- □ ISSM
- □ SCA

***Feedback:** The AO determines whether security-relevant changes require reauthorization.*

Question 5 of 6. Select the role responsible for each task and output.

Task 5: Verifies proper sanitation of storage media.

- □ AO
- □ ISSM
- □ SCA *(correct response)*

***Feedback:** After the ISSM decommissions the system, the SCA verifies that the proper decommissioning steps were taken.*

Question 6 of 6. Select the role responsible for each task and output.

Task 6: Formally approves the decommissioning plan.

- □ AO (correct response)
- □ ISSM
- □ SCA

***Feedback:** The AO formally approves the decommissioning plan.*