Applying Assessment and Authorization in the NISP

Student Guide

September 2017

Center for Development of Security Excellence

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 National Industrial Security Program Operating Manual and the DSS Assessment and Authorization Process Manual to guide me through the process and tell me the requirements.”

Welcome to the Applying Assessment and Authorization in the NISP course! This course walks you through each step of the Assessment and Authorization (A&A) process. It is based on the NISP Operating Manual (NISPOM) and the DSS Assessment and Authorization Process Manual (DAAPM). These two documents, which are available through the course resources, detail how DSS implements the Risk Management Framework (RMF) for cleared contractor Information Systems under DSS oversight.

Objectives

Here is the course objective:

- Describe the Assessment and Authorization (A&A) process in accordance with the guidance as outlined in the DSS Assessment and Authorization Process Manual (DAAPM) and the National Industrial Security Program Operating Manual (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. DSS has a website with Risk Management Framework resources for contractors that I need to review, and I need to read the DAAPM as well. So I don't get delayed later, I also need to make sure that I have our sponsorship documentation and register for an account with DSS's ODAA Business Management System."

This lesson reviews the steps you should take to prepare for the Assessment and Authorization (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

Recall that the A&A process consists of six steps:

- Step 1, Categorize System
- Step 2, Select Security Controls
- Step 3, Implement Security Controls
- Step 4, Assess Security Controls
- Step 5, Authorize System
- Step 6, Monitor Security Controls

Each of these steps requires certain inputs and tasks, and results in specific outputs.

Purpose

The A&A process is based on the Risk Management Framework (RMF). All federal government agencies use the RMF to facilitate reciprocity.

DSS uses the A&A process to authorize cleared contractors' new Information Systems to process, store, and access classified information. DSS 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 (ATO).

Term	Definition
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.

A&A Prerequisites

Overview

As the Information System Security Manager (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 DSS RMF website.
- Finally, register for an account on the Office of the Designated Approving Authority (ODAA) Business Management System, known as OBMS.

Note: ODAA is the previous name of the NISP Authorizing Office (NAO), which manages the A&A process for DSS.

As you get started in the A&A process, contact your local Information System Security Professional (ISSP) with any questions or concerns.

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 National Industrial Security Program Operating Manual (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 (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 (IO) provides the SCG.

DSS RMF Resources

The DSS website provides cleared contractors with information and resources about the RMF. It includes the current version of the DSS Assessment and Authorization Process Manual (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 DSS RMF website is available through the course resources.

OBMS Account

OBMS is a DSS system that manages the A&A process. Throughout the process, the ISSM uses OBMS to upload information to DSS, including the System Security Plan (SSP) and any supporting artifacts for the Information System. When you create an account, OBMS generates a Unique Identifier (UID) that DSS uses to identify the contractor and their materials. Be sure to include this UID on all documentation to prevent rejection or delays.

OBMS job aids are 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. Then check your answers 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 DSS Risk Management Framework (RMF) website
- ☐ Register for an ODAA Business Management System (OBMS) account

Lesson 3: Categorize System

Introduction

Objectives

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 Step 1 of the Assessment and Authorization (A&A) process.

Here is the lesson objective.

- Describe the inputs, tasks, and outputs associated with Step 1, Categorize System

Step 1 Inputs

Inputs

Recall that you will need the sponsorship documentation and security classification guidance associated with your contract before you begin.

In addition, you may find it helpful to begin coordinating with the:

- Information Owner (IO)
- DSS Industrial Security Representative (IS Rep)
- DSS Counterintelligence Special Agent (CISA)
- Information System Security Professional (ISSP) assigned as the Security Controls Assessor (SCA)

Task 1-1

Task 1-1: Categorize the Information System and document the results in the System Security Plan (SSP)

In Step 1, the ISSM performs one primary task, which is to categorize the Information System and document the results in the System Security Plan (SSP). To do this, you first assess the risks and threats to the facility and the program. Next, you establish Information System boundaries, and then categorize the Information System. Finally, you assign qualified personnel to the Risk Management Framework (RMF) team.

Assess Risks and Threats

Recall that risk is a major factor in the A&A process. To begin categorizing the Information System, you must first assess the risks and threats to the facility and the program. You will later use the results of the risk and threat assessment to determine if it is necessary to tailor security controls to reduce risk to an acceptable level.

DSS also considers the results of the risk and threat assessment to validate the system categorization and may change the system categorization with concurrence from the IO. Note that a high threat picture requires IO concurrence on the categorization of the system.

Information System Boundaries

Information System boundaries establish the scope of protection for organizational Information Systems based on the risk assessment for the technologies the facility possesses. They describe what the organization agrees to protect and include people, processes, and information technologies.

The ISSM establishes Information System boundaries in coordination with the security categorization process before developing the SSP. The boundaries you establish affect your ability to successfully manage risk. Expansive boundaries with many system components and unnecessary architectural complexity make the risk management process extremely unwieldy and complex. Conversely, boundaries that are too limited increase the number of systems that the ISSM needs to manage separately and can unnecessarily inflate the information security costs for the organization.

Considerations

When establishing boundaries, consider whether the resources identified as an Information System support the same mission or business objectives or functions. Do they possess essentially the same operating characteristics and information security requirements? Do the resources reside in the same general operating environment or in various locations with similar operating requirements? Do they reside in the same geographic area?

System Categorization

Once you have assessed the risk and established the system boundaries, you must categorize the Information System by taking into account the impact 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 DSS 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 DSS authorization must meet or exceed this baseline.

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	
Moderate	*serious* adverse effect on organizational operations, assets, or individuals		
High	*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.

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.

Assign Personnel

As the ISSM, you may appoint an Information System Security Officer (ISSO) to support your RMF efforts. In addition, you may choose to place additional personnel from your organization, such as the network administrator, on the RMF team.

Step 1 Outputs

Outputs

Step 1 results in the creation of three main items:

- A Risk Assessment Report (RAR)
- An initial draft of the System Security Plan (SSP)
- Initial versions of the supporting artifacts associated with the Information System

Risk Assessment Report

The RAR documents the results of the risk and threat assessment. DSS provides a template for the RAR on their RMF website and recommends using the template to minimize the possible need for additional assessment time. When documenting results in the RAR, be sure to follow the appropriate security classification guidance.

The DSS RMF website is available through the course resources.

Initial System Security Plan

The SSP identifies the protection measures to safeguard classified information and should include as much detail as possible to explain and define the Information System and its

characteristics. DSS provides a template for the SSP on their RMF website and recommends using the template to minimize the possible need for additional assessment time.

The DSS RMF website is available through the course resources.

There are two types of security plans: the SSP and the Master Systems Security Plan (MSSP). This is also referred to as a Type Authorization. The SSP seeks authorization for a single Information System. The MSSP or Type Authorization is used to authorize multiple Information Systems that operate in the same environment at the same classification level, are of the same system type, and run an approved operating system, under the same security plan. The same template is used for both types of security plans. This course refers to both types as the SSP.

The ISSM builds the SSP gradually throughout the A&A process. At this step, document the following in the SSP:

- Boundaries
- Categorization
- Personnel

Supporting Artifacts

The SSP may include supporting artifacts such as a hardware baseline, configuration diagram, or software baseline. Refer to the DSS Assessment and Authorization Process Manual (DAAPM) to determine the artifacts required for the Information System.

The DAAPM is available through the course resources.

Review Activities

Review Activity 1

Before beginning Step 1, you should coordinate with which of the following roles?

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

- ☐ Information Owner (IO)
- ☐ DSS Industrial Security Representative (IS Rep)
- ☐ DSS Counterintelligence Special Agent (CISA)
- ☐ Information System Security Professional (ISSP)

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.

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

- ○ Assign qualified personnel to RMF roles
- ○ Categorize the Information System
- ○ Assess risks and threats
- ○ Establish Information System boundaries

2 of 4. This describes what the organization agrees to protect and includes people, processes, and technology.

- ○ Assign qualified personnel to RMF roles
- ○ Categorize the Information System
- ○ Assess risks and threats
- ○ Establish Information System boundaries

3 of 4. This considers the impact on the organization due to a loss of confidentiality, integrity, or availability of the information or the system.

- ○ Assign qualified personnel to RMF roles
- ○ Categorize the Information System
- ○ Assess risks and threats
- ○ Establish Information System boundaries

4 of 4. This may add an ISSO to the contractor team.

- ○ Assign qualified personnel to RMF roles
- ○ Categorize the Information System
- ○ Assess risks and threats
- ○ Establish Information System boundaries

Review Activity 3

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

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

- ○ Initial System Security Plan (SSP)
- ○ Risk Assessment Report (RAR)
- ○ Supporting artifacts

Question 2 of 3. Which of the following documents the Information System boundary, the system categorization, and the personnel assigned to the process?

- ○ Initial System Security Plan (SSP)
- ○ Risk Assessment Report (RAR)
- ○ Supporting artifacts

Question 3 of 3. A configuration diagram is an example of which of the following?

- ○ Initial System Security Plan (SSP)
- ○ Risk Assessment Report (RAR)
- ○ Supporting artifacts

Lesson 4: Select Security Controls

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 Step 2 of the Assessment and Authorization (A&A) process.

Here is the lesson objective.

- Describe the inputs, tasks, and outputs associated with Step 2, Select Security Controls

Step 2 Inputs

Risk Assessment Report (RAR)

To complete this step in the A&A process, the Information System Security Manager (ISSM) needs the Risk Assessment Report (RAR) created in Step 1. 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.

Step 2 Tasks

Overview

Task 2-1: Identify and document the applicable baseline security controls

Task 2-2: Tailor the controls as needed

Task 2-3: Develop a continuous monitoring strategy

Task 2-4: Submit the System Security Plan (SSP) and supporting artifacts to DSS (if needed)

There are four primary tasks to complete in this step. First, the ISSM identifies and documents the baseline security controls applicable to the Information System. Next, the ISSM tailors the controls as needed. Then, the ISSM develops a strategy to continuously monitor the effectiveness of the security controls. Finally, the ISSM submits the System Security Plan (SSP) and supporting artifacts to DSS if concurrence is necessary.

Task 2-1

Task 2-1: Identify and document the applicable baseline security controls

In task 2-1, the ISSM identifies and documents the baseline security controls that apply to the Information System. The baseline controls depend on the categorization of the Information System determined in Step 1. Recall that DSS establishes a minimum baseline of Moderate-Low-Low.

There are three types of security controls:

- System specific
- Common
- Hybrid

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 DSS Assessment and Authorization Process Manual (DAAPM) (Appendix A) for a complete list of baseline security controls.

In addition, the ISSM may also choose to implement the DSS-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 (Appendix D) contains the DSS-approved overlay.

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 2-2

Task 2-2: Tailor the controls as needed

In task 2-2, 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 SSP, and the Information Owner (IO) or government customer may need to provide a Risk Acknowledgement Letter (RAL).

Task 2-3

Task 2-3: Develop a continuous monitoring strategy

In task 2-3, 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
- Security status reporting

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

Task 2-4

Task 2-4: Submit the System Security Plan (SSP) and supporting artifacts to DSS (if needed)

In task 2-4, the ISSM seeks DSS concurrence with the Information System categorization and security control selection if the system does not meet or exceed the DSS baseline of Moderate-Low-Low.

If this is the case, seek approval from the Security Controls Assessor (SCA) before continuing to the next step in the process. To do this, upload the following materials to the ODAA Business Management System, (OBMS):

- A current, in-progress SSP that describes the security control selections and justifications for modifications to the baseline
- The RAR
- Any other supporting artifacts

To upload the RAR, add a Profile extension in OBMS. OBMS validation also requires a Certification Statement that the ISSM will create later in this process. To pass validation in this step, upload a blank Certification Statement.

This task is not required when the Information System meets or exceeds the baseline and the baseline controls and overlays are not modified.

Step 2 Outputs

Updated SSP

Step 2 results in an updated SSP that describes the security control selection and the continuous monitoring strategy. When describing the security controls, be sure to include the baseline security controls, any overlays selected, and tailoring of the controls and to explain why these controls were selected, tailored, or determined to not be applicable.

Review Activities

Review Activity 1

Which of the following must you have before beginning Step 2 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
- ○ Risk Acknowledgement Letter (RAL)
- ○ 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.

Question 1 of 4. This task requires categorization of the Information System as its direct input.

- ○ Develop a continuous monitoring strategy
- ○ Tailor the controls
- ○ Submit the System Security Plan (SSP) and supporting artifacts
- ○ Identify and document baseline security controls

Question 2 of 4. Details of how you will perform configuration management are included in this task.

- ○ Develop a continuous monitoring strategy
- ○ Tailor the controls
- ○ Submit the System Security Plan (SSP) and supporting artifacts
- ○ Identify and document baseline security controls

Question 3 of 4. This task is necessary if the Information System does not meet or exceed the DSS baseline.

- ○ Develop a continuous monitoring strategy
- ○ Tailor the controls
- ○ Submit the System Security Plan (SSP) and supporting artifacts
- ○ Identify and document baseline security controls

Question 4 of 4. This task may include supplementation of the selected security controls.

- ○ Develop a continuous monitoring strategy
- ○ Tailor the controls
- ○ Submit the System Security Plan (SSP) and supporting artifacts
- ○ Identify and document baseline security controls

Review Activity 3

Which of the following will you update with the security control selection and continuous monitoring strategy?

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

- ○ Risk Assessment Report (RAR)
- ○ System Security Plan (SSP)
- ○ Sponsorship documentation
- ○ Risk Acknowledgement Letter (RAL)

Lesson 5: Implement Security Controls

Introduction

Objectives

Jack: "This is great—DSS approved the security controls for my system, so now I can work on implementing them. I'll document the implementation and look for any weaknesses as I go."

This lesson reviews Step 3 of the Assessment and Authorization (A&A) process.

Here is the lesson objective.

- Describe the inputs, tasks, and outputs associated with Step 3, Implement Security Controls

Step 3 Inputs

SCA Validation

Recall that the Information System Security Manager (ISSM) must obtain validation from the Security Controls Assessor (SCA) before proceeding with this step if the Information System does not meet or exceed the DSS baseline of Moderate-Low-Low.

Note that reviews performed by DSS are often iterative and require multiple submissions and reviews before approval is granted. For system categorization and controls selection concurrence, DSS aims to provide a response within 5 business days.

Step 3 Tasks

Tasks 3-1 and 3-2

Task 3-1: Implement the security controls specified in the SSP

Task 3-2: Document security control implementation in the SSP

In this step, the ISSM implements the security controls as described in the System Security Plan (SSP) and documents the implementation in the SSP. The documentation should provide a functional description of the control implementation, including planned inputs, expected behavior, and expected outputs. It also describes how the security control achieves the required security capability.

Step 3 Outputs

Update SSP

Step 3 results in an updated SSP that describes:

- The implementation of the security controls
  - Planned inputs
  - Expected behavior
  - Expected outputs
- The achievement of the required security capability

Review Activities

Review Activity 1

Your Information System does not meet the baseline. What must you obtain before implementing the security controls?

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

- ○ A Risk Acknowledgement Letter (RAL) from DSS
- ○ Approval of the System Security Plan (SSP) from the Information Owner (IO)
- ○ Concurrence from DSS on the system categorization and controls selection

Review Activity 2

How is the System Security Plan (SSP) used during the implementation of the security controls?

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

- ☐ It outlines the security controls to implement.
- ☐ It includes a functional description of the control implementation.
- ☐ It describes how the security capability required by each security control is achieved.

Lesson 6: Assess Security Controls

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 Step 4 of the Assessment and Authorization (A&A) process.

Here is the lesson objective.

- Describe the inputs, tasks, and outputs associated with Step 4, Assess Security Controls

Step 4 Inputs

Controls and Procedures

Before the Information System Security Manager (ISSM) begins this step in the A&A process, the security controls must be implemented. Once they are implemented, the ISSM uses the security procedures defined in the System Security Plan (SSP) to assess the controls.

Step 4 Tasks

Overview

Task 4-1: The ISSM assesses the security controls

Task 4-2: The ISSM reviews the applicable security classification guidance and verifies the classification level of all SSP artifacts

Task 4-3: The SCA receives and reviews the SSP and supporting artifacts

Task 4-4: The SCA conducts an on-site assessment

The ISSM works in coordination with the Security Controls Assessor (SCA) to complete the tasks in this step. First, the ISSM assesses the security controls and ensures that all documentation is properly classified. Then, the SCA reviews the SSP and supporting artifacts and conducts an assessment.

Task 4-1

Task 4-1: The ISSM assesses the security controls

In task 4-1, the ISSM assesses the security controls in accordance with the security procedures defined in the SSP. This ensures that the controls are implemented correctly, operating as intended, and meet the security requirements for the Information System. The DSS Risk Management Framework (RMF) website contains several tools you can use to aid the assessment. As you assess the system, be sure to document any issues, vulnerabilities, or weaknesses.

The DSS RMF website is available through the course resources.

Tools

Available tools to assess security controls:

- Security Content Automation Protocol (SCAP) Compliance Checker (SCC)
- DISA's Security Technical Implementation Guidelines (STIGs) Viewer
- DSS Technical Assessment job aids

Note: Information System Security Managers (ISSMs) are not limited to these approved tools and may use any that prove helpful.

Task 4-2

Task 4-2: The ISSM reviews the applicable security classification guidance and verifies the classification level of all SSP artifacts

In task 4-2, the ISSM reviews the applicable security classification guidance and verifies the classification level of all SSP artifacts.

Task 4-3

Task 4-3: The SCA receives and reviews the SSP and supporting artifacts

In task 4-3, the SCA receives and reviews the SSP and supporting artifacts. During the review, the SCA validates the classification level and determines whether the SSP and supporting artifacts fully address all of the system security controls and security configurations.

If the SSP and supporting artifacts are acceptable, the SCA schedules an on-site assessment.

If they are not, the ISSM must revise and resubmit the SSP and supporting artifacts. This is often necessary before an on-site assessment can be scheduled.

Upon receipt of a complete and accurate SSP with all of the required supporting artifacts, DSS aims to complete assessment and authorization actions within 30 days.

Task 4-4

Task 4-4: The SCA conducts an on-site assessment

In task 4-4, the SCA assesses the information provided in the SSP and supporting artifacts and conducts an assessment of the technical security controls and system configuration. The assessment validates that the Information System operates as documented and that the controls are in place and operating as intended.

Step 4 Outputs

Overview

Both you, as the ISSM, and the SCA are responsible for outputs in this step. The ISSM submits the SSP and supporting artifacts to DSS via the ODAA Business Management System (OBMS). The SCA creates a Security Assessment Report (SAR), completes OBMS inputs, and makes an authorization recommendation to the Authorizing Official (AO).

ISSM

As the ISSM, you use OBMS to upload the SSP and supporting artifacts created throughout this process. These artifacts include:

- A Certification Statement
- The Risk Assessment Report (RAR)
- A Plan of Action and Milestones (POA&M)
- The supporting contractual requirement
- Any other supporting documentation required for the system

Ensure that you only upload unclassified attachments to OBMS. Seek guidance from the SCA on how to handle any classified artifacts.

System Security Plan (SSP)

The SSP should reflect the actual state of the security controls based on the vulnerabilities of the security control assessment, reassessment, and completion of any remediation actions taken.

When uploading the SSP to OBMS, use the document type “SSP”. Note that the SSP is required for OBMS validation.

Certification Statement

The Certification Statement is verification from the ISSM that the Information System has undergone a comprehensive evaluation of all of the technical and non-technical security features and safeguards and that all of the required security features are functioning as outlined in the SSP. The Certification Statement details the inspection and test procedures used.

When uploading the Certification Statement to OBMS, use the document type "Certification Statement". Note that the Certification Statement is required for OBMS validation.

Risk Assessment Report (RAR)

The RAR, which documents the results of the risk and threat assessment, is also required for OBMS validation. When uploading the RAR to OBMS, use the document type "Profile".

Plan of Action and Milestones (POA&M)

The POA&M is an agreement between the contractor and DSS that states which baseline technical security configurations cannot immediately be met and why. As the ISSM, you use the POA&M to document the approach and timeline to bring the Information System into compliance. The POA&M is a living document that stays with the system throughout its lifecycle and outlines non-compliance issues, mitigation plans, and adjustments necessary to demonstrate implementation of assigned security controls. It also outlines the timeline to accomplish the plan, including the anticipated completion date and the risk level of each non-compliance issue.

Depending on the severity of the issues, an Information System with a POA&M in place may still receive conditional Authorization to Operate, known as ATO with conditions, while the issues are resolved. Where there is an unacceptable level of risk, the AO issues Denial of Authorization to Operate (DATO).

When uploading a POA&M to OBMS, use the document type "Other".

Supporting Contractual Requirement

Upload the sponsorship documentation associated with the Information System to OBMS. Usually, this is a properly completed DD Form 254, Contract Security Classification Specification, but the National Industrial Security Program Operating Manual (NISPOM) defines other sponsorship documentation that may be used instead.

When uploading sponsorship documentation to OBMS, use the document type "Other".

Other Supporting Documentation

To determine any other supporting documentation that may be required by an Information System, refer to the DSS Assessment and Authorization Process Manual (DAAPM).

The DAAPM is available through the course resources.

Some examples of other artifacts include:

- Risk Acknowledgement Letter (RAL)
  - A letter from the Information Owner (IO) acknowledging the level of risk when an Information System cannot be configured to meet the requirements of the National Industrial Security Program Operating Manual (NISPOM) due to customer-defined requirements
- Interconnection Security Agreement (ISA)
  - A document that regulates security-relevant aspects of an intended connection between an agency and an external system
- Memorandum of Agreement (MOA)
  - An agreement between two or more parties that includes specific terms that are agreed to and a commitment by at least one party to engage in action
- Memorandum of Understanding (MOU)
  - An agreement between two or more parties that includes only general understandings between the parties

When uploading other supporting documentation to OBMS, use the document type "Other".

SCA

Recall that the SCA creates the SAR, completes OBMS inputs, and makes an authorization recommendation to the AO. The SCA may recommend:

- Conditional Authorization to Operate, known as ATO with conditions
- Full Authorization to Operate (ATO)
- Denial of Authorization to Operate (DATO)

Common Reasons to Recommend DATO

These include:

- Missing ISSM signature on the security package submission and certification statement
- Missing or inaccurate hardware list, software list, and/or configuration diagram
- Physical security inadequately explained
- Identification and authentication inadequately explained
- Missing MOA, MOU, or ISA when one is required
- Missing a letter from the IO when variances are needed
- Missing a signed DSS Form 147, Record of Controlled Area when the system is in a closed area
- Vulnerabilities results at an unacceptable level
- Unacceptable level of risk

Review Activities

Review Activity 1

You have finished implementing the security controls for your Information System. Do you need anything else before proceeding to assess the security controls?

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

- ○ Yes
- ○ No

Review Activity 2

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

1 of 4. Assess the security controls

- ○ ISSM
- ○ SCA
- ○ Both

2 of 4. Verify the classification level of the System Security Plan (SSP)

- ○ ISSM
- ○ SCA
- ○ Both

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

- ○ ISSM
- ○ SCA
- ○ Both

4 of 4. Make authorization recommendation

- ○ ISSM
- ○ SCA
- ○ Both

Lesson 7: Authorize System

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 Step 5 of the Assessment and Authorization (A&A) process.

Here is the lesson objective.

- Describe the inputs, tasks, and outputs associated with Step 5, Authorize System

Step 5 Inputs

Security Authorization Package

Before the system can be authorized, the Authorizing Official (AO) needs the security authorization package. It includes the final System Security Plan (SSP) and the supporting artifacts, the Security Assessment Report (SAR), and an authorization recommendation from the Security Controls Assessor (SCA).

Step 5 Tasks

Authorization Decision

Task 5-1: AO issues an authorization decision

In this step, the AO issues an authorization decision for the Information System and the common controls inherited by the system. To begin, the AO reviews the system authorization package, consults with the SCA, and evaluates the level of risk associated with the Information System. The authorization decision is based on whether risk is at an acceptable level.

Authorization Decision

The authorization decision may be to issue:

- Authorization to Operate (ATO)
- ATO with conditions
- Denial of Authorization to Operate (DATO)

When the AO issues either ATO or ATO with terms and conditions, the contractor may begin processing classified information. Continuous monitoring must begin as soon as operation begins. When the AO grants ATO with conditions, the Information System Security Manager (ISSM) must also respond to corrective actions and recommendations.

When the AO issues DATO, the contractor must cease operation of the Information System immediately, as continued operation is considered a violation of DoD policy and NISPOM requirements. The ISSM responds to corrective actions and updates the SSP. The AO will reconsider the authorization decision on receipt of a revised security authorization package.

Step 5 Outputs

Authorization Decision Document

The authorization decision document includes the authorization decision, terms and conditions, and the authorization termination date (ATD). Note that processing beyond the ATD is unauthorized and considered a violation of DoD policy and NISPOM requirements.

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 Controls Assessor (SCA)
- ○ Authorizing Official (AO)
- ○ Information Owner (IO)

Review Activity 2

Which of the following are parts of the security authorization package?

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

- ☐ System Security Plan (SSP)
- ☐ Supporting artifacts
- ☐ Security Assessment Report (SAR)
- ☐ Authorization recommendation

Review Activity 3

Select the all of the authorization decisions that apply to each description. Then check your answers in the Answer Key at the end of this Student Guide.

Description 1 of 3. The contractor may begin processing classified information.

- ☐ ATO
- ☐ ATO with terms and conditions
- ☐ DATO

Description 2 of 3. The contractor must respond to corrective actions.

- ☐ ATO
- ☐ ATO with terms and conditions
- ☐ DATO

Description 3 of 3. The contractor must cease operation of the Information System immediately.

- ☐ ATO
- ☐ ATO with terms and conditions
- ☐ DATO

Lesson 8: Monitor System

Introduction

Objectives

Jack: "Now that the system is up and running, I'm using the continuous monitoring strategy in the System 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 Step 6 of the Assessment and Authorization (A&A) process.

Here is the lesson objective.

- Describe the inputs, tasks, and outputs associated with Step 6, Monitor System

Step 6 Inputs

Authorization to Operate

Continuous monitoring begins as soon as the Information System receives Authorization to Operate (ATO), even with conditions, from the Authorizing Official (AO).

Step 6 Tasks

Overview

Task 6-1: The ISSM assesses the security controls

Task 6-2: The ISSM conducts remediation actions

Task 6-3: The ISSM updates and maintains security documentation

Task 6-4: The ISSM submits security status reports

Task 6-5: The ISSM implements the decommissioning strategy

Task 6-6: The SCA reviews reported security status

Task 6-7: The SCA reviews the decommissioning request

The Information System Security Manager (ISSM) and the Security Controls Assessor (SCA) both play a role in continuous monitoring.

The ISSM assesses a selected subset of security controls in accordance with the continuous monitoring strategy and conducts remediation actions when necessary. In addition, the ISSM updates and maintains the security documentation associated with the Information System and submits security status reports to the SCA and other appropriate officials when necessary. When the Information System is no longer needed, the ISSM implements the decommissioning strategy.

The SCA reviews security status reports and the decommissioning request when it is received.

Task 6-1

Task 6-1: The ISSM assesses the security controls

In task 6-1, the ISSM assesses a selected subset of security controls in accordance with the continuous monitoring plan. The System Security Plan (SSP) approved by the AO contains the continuous monitoring plan and defines the selection of controls and the frequency of assessment.

When conducting continuous monitoring, the ISSM may leverage commercial tools when they are configured in accordance with the SSP. For example, you may choose to use a tool to provide password change reminders, as long as it issues reminders as often as the SSP requires.

Requirement Satisfaction

Activities that may fill the requirement for continuous monitoring include:

- Security control assessments conducted as part of an Information System:
  - Authorization
  - Ongoing authorization
  - Reauthorization
- Continuous monitoring activities
- Testing and evaluation of the Information System as part of:
  - The system development life cycle process
  - An audit

Task 6-2

Task 6-2: The ISSM conducts remediation actions

In task 6-2, the ISSM conducts remediation actions based on the results of ongoing monitoring activities, risk assessment, and outstanding items in the Plan of Action and

Milestones (POA&M). When remediation actions result in a change to the Information System or configuration management, be sure to conduct an impact analysis.

Task 6-3

Task 6-3: The ISSM updates and maintains security documentation

In task 6-3, the ISSM updates and maintains the security documentation associated with the Information System, including the SSP, status reports, and the POA&M. When updating documentation, be sure not to modify or destroy critical original information required to oversee, manage, or audit the Information System. Updated documentation must be submitted to DSS through the ODAA Business Management System (OBMS).

System Security Plan (SSP)

The SSP must reflect any modifications to the security controls that result from risk mitigation activities and any security-relevant changes that may require reauthorization of the Information System.

Security-relevant changes affect the availability, integrity, authentication, confidentiality, or non-repudiation of an Information System or its environment. Examples include:

- Identification and authentication
- Auditing
- Sanitization
- Operating system
- Firewall
- Router tables
- Information System location
- Operating environment
- Hardware and/or software baseline

Status Reports

Status reports reflect additional assessment activities carried out to determine security control effectiveness based on modifications to the SSP and the deployed controls.

Plan of Action and Milestones (POA&M)

The POA&M reports progress made on current outstanding items listed in the plan, addresses vulnerabilities assessed during the security impact analysis or security control monitoring, and describes how the ISSM intends to address the vulnerabilities.

Task 6-4

Task 6-4: The ISSM submits security status reports

In task 6-4, the ISSM submits security status reports to the SCA and other appropriate officials on an ongoing basis in accordance with the frequency defined in the SSP. These reports convey to DSS the current security state of the Information System and its environment of operation, and may be event-driven, time-driven, or both.

Reports must be appropriately marked, protected, and handled in accordance with federal and organizational policies. The National Institute of Standards and Technology Special Publication (NIST SP) 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, contains additional guidance on marking, protecting, and handling reports.

The NIST SP 800-137 is available through the course resources.

Task 6-5

Task 6-5: The ISSM implements the decommissioning strategy

As the ISSM, task 6-5 requires that you implement the decommissioning strategy detailed in the SSP when the Information System is no longer needed—such as at the end of the contract—or is no longer authorized. As part of decommissioning, the ISSM ensures that all security controls addressing Information System removal and decommissioning are implemented, updates the tracking and management systems, notifies the users and application owners, and reviews and assesses security control inheritance relationships for impact.

Task 6-6

Task 6-6: The SCA reviews reported security status

In task 6-6, the SCA reviews the reported security status of the Information System and determines whether risk to organizational operations and assets, individuals, other organizations, and national security remains acceptable. The SCA reports security-relevant changes to the AO, who determines whether the changes require reauthorization of the system.

Task 6-7

Task 6-7: The SCA reviews the decommissioning request

Task 6-7 addresses DSS's handling of decommissioning requests. When the SCA receives a decommissioning request from the contractor, he or she reviews it and forwards it to the AO. The AO then issues an Information System removal and decommissioning letter.

During the next security assessment, the SCA will verify that all security controls addressing Information System removal and decommissioning were implemented and that storage media and memory associated with the Information System were sanitized in accordance with the procedures outlined in the SSP.

Step 6 Outputs

Monitoring and Decommissioning

Step 6 produces several outputs, depending on the outcome of continuous monitoring or whether decommissioning is required.

During monitoring, the ISSM produces:

- An updated SSP
- An updated POA&M
- Security status reports

During decommissioning, the AO produces the Information System removal and decommissioning letter.

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 Controls Assessor (SCA) indicates
- ○ Once the Information System receives ATO or ATO with conditions

Review Activity 2

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

1 of 6. Conducts remediation actions

- ○ ISSM
- ○ SCA
- ○ AO

2 of 6. Reviews security status reports

- ○ ISSM
- ○ SCA
- ○ AO

3 of 6. Updates the System Security Plan (SSP)

- ○ ISSM
- ○ SCA
- ○ AO

4 of 6. Determines when reauthorization is needed

- ○ ISSM
- ○ SCA
- ○ AO

5 of 6. Verifies proper sanitization of storage media

- ISSM
- SCA
- AO

6 of 6. Issues Information System removal and decommissioning letter

- ISSM
- SCA
- AO

Lesson 9: 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 DSS Assessment and Authorization Process Manual and the National Industrial Security Program Operating Manual are there to provide the requirements and guidance."

This course reviewed each step in the Assessment and Authorization (A&A) process. Remember to refer to the course resources for additional materials, including the DSS Assessment and Authorization Process Manual (DAAPM).

Lesson Summary

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

You should now be able to perform all of the listed activities.

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

To receive course credit, you must take the *Applying Assessment and Authorization in the NISP* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

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

- ☑ 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 DSS 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?

- ☐ Purchase hardware and software
- ☑ Review your sponsorship documentation and security classification guidance *(correct response)*
- ☑ Review the materials on the DSS Risk Management Framework (RMF) website *(correct response)*
- ☑ Register for an ODAA Business Management System (OBMS) account *(correct response)*

Feedback: *You should possess and understand your sponsorship documentation and security classification guidance, review the materials available on the DSS RMF website including the DSS Assessment and Authorization Process Manual (DAAPM), and register for an OBMS account.*

Lesson 3 Review Activities

Review Activity 1

Before beginning Step 1, you should coordinate with which of the following roles?

- ☑ Information Owner (IO) *(correct response)*
- ☑ DSS Industrial Security Representative (IS Rep) *(correct response)*
- ☑ DSS Counterintelligence Special Agent (CISA) *(correct response)*
- ☑ Information System Security Professional (ISSP) *(correct response)*

Feedback: *You may find it helpful to begin coordinating with all of these roles from the beginning of the Assessment and Authorization (A&A) process.*

Review Activity 2

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

- ○ Assign qualified personnel to RMF roles
- ○ Categorize the Information System
- ⊙ Assess risks and threats *(correct response)*
- ○ Establish Information System boundaries

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

2 of 4. This describes what the organization agrees to protect and includes people, processes, and technology.

- ○ Assign qualified personnel to RMF roles
- ○ Categorize the Information System
- ○ Assess risks and threats
- ⊙ Establish Information System boundaries *(correct response)*

Feedback: *Information System boundaries establish the scope of protection for organizational Information Systems and include the people, processes, and information technologies.*

3 of 4. This considers the impact on the organization due to a loss of confidentiality, integrity, or availability of the information or the system.

- ○ Assign qualified personnel to RMF roles
- ⦿ Categorize the Information System *(correct response)*
- ○ Assess risks and threats
- ○ Establish Information System boundaries

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

4 of 4. This may add an ISSO to the contractor team.

- ⦿ Assign qualified personnel to RMF roles *(correct response)*
- ○ Categorize the Information System
- ○ Assess risks and threats
- ○ Establish Information System boundaries

Feedback: *The ISSM may choose to appoint an ISSO to support RMF efforts.*

Review Activity 3

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

- ○ Initial System Security Plan (SSP)
- ⦿ Risk Assessment Report (RAR) *(correct response)*
- ○ Supporting artifacts

Feedback: *The RAR documents the results of the risk and threat assessment.*

Question 2 of 3. Which of the following documents the Information System boundary, the system categorization, and the personnel assigned to the process?

- ⦿ Initial System Security Plan (SSP) *(correct response)*
- ○ Risk Assessment Report (RAR)
- ○ Supporting artifacts

Feedback: *At the end of Step 1, the initial SSP documents boundaries, categorization, and personnel.*

Question 3 of 3. A configuration diagram is an example of which of the following?

- ○ Initial System Security Plan (SSP)
- ○ Risk Assessment Report (RAR)
- ⊙ Supporting artifacts *(correct response)*

Feedback: *Supporting artifacts may include a hardware baseline, configuration baseline, or software baseline.*

Lesson 4 Review Activities

Review Activity 1

Which of the following must you have before beginning Step 2 of the Assessment and Authorization (A&A) process?

- ○ Certification Statement
- ○ Risk Acknowledgement Letter (RAL)
- ⊙ Risk Assessment Report (RAR) *(correct response)*
- ○ Continuous Monitoring Plan

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

Review Activity 2

Question 1 of 4. This task requires categorization of the Information System as its direct input.

- ○ Develop a continuous monitoring strategy
- ○ Tailor the controls
- ○ Submit the System Security Plan (SSP) and supporting artifacts
- ⊙ Identify and document baseline security controls *(correct response)*

Feedback: *An Information System's baseline security controls depend on the categorization of the system. The minimum baseline established by DSS is Moderate-Low-Low.*

Question 2 of 4. Details of how you will perform configuration management are included in this task.

- ⊙ Develop a continuous monitoring strategy *(correct response)*
- ○ Tailor the controls
- ○ Submit the System Security Plan (SSP) and supporting artifacts
- ○ Identify and document baseline security controls

Feedback: *The continuous monitoring strategy includes configuration management and control, security impact analyses, security control assessment, and security status reporting.*

Question 3 of 4. This task is necessary if the Information System does not meet or exceed the DSS baseline.

- ○ Develop a continuous monitoring strategy
- ○ Tailor the controls
- ⦿ Submit the System Security Plan (SSP) and supporting artifacts *(correct response)*
- ○ Identify and document baseline security controls

Feedback: *DSS must concur with the Information System categorization and security control selection if the system does not meet or exceed the baseline of Moderate-Low-Low.*

Question 4 of 4. This task may include supplementation of the selected security controls.

- ○ Develop a continuous monitoring strategy
- ⦿ Tailor the controls *(correct response)*
- ○ Submit the System Security Plan (SSP) and supporting artifacts
- ○ Identify and document baseline security controls

Feedback: *Security controls may be tailored in to supplement the baseline or tailored out when not needed.*

Review Activity 3

Which of the following will you update with the security control selection and continuous monitoring strategy?

- ○ Risk Assessment Report (RAR)
- ⦿ System Security Plan (SSP) *(correct response)*
- ○ Sponsorship documentation
- ○ Risk Acknowledgement Letter (RAL)

Feedback: *The SSP will describe the security control selection and outline the continuous monitoring strategy.*

Lesson 5 Review Activities

Review Activity 1

Your Information System does not meet the baseline. What must you obtain before implementing the security controls?

- ○ A Risk Acknowledgement Letter (RAL) from DSS
- ○ Approval of the System Security Plan (SSP) from the Information Owner (IO)
- ⊙ Concurrence from DSS on the system categorization and controls selection *(correct response)*

Feedback: *If the Information System does not meet or exceed the DSS baseline of Moderate-Low-Low, obtain validation from the Security Controls Assessor (SCA) before proceeding.*

Review Activity 2

How is the System Security Plan (SSP) used during the implementation of the security controls?

- ☑ It outlines the security controls to implement. *(correct response)*
- ☑ It includes a functional description of the control implementation. *(correct response)*
- ☑ It describes how the security capability required by each security control is achieved. *(correct response)*

Feedback: *The SSP is the primary driver of this step. It includes the security controls to implement and is where the ISSM describes the implementation of the controls.*

Lesson 6 Review Activities

Review Activity 1

You have finished implementing the security controls for your Information System. Do you need anything else before proceeding to assess the security controls?

- ⦿ Yes *(correct response)*
- ○ No

Feedback: *You will also need the security procedures outlined in the System Security Plan (SSP).*

Review Activity 2

1 of 4. Assess the security controls

- ○ ISSM
- ○ SCA
- ⦿ Both *(correct response)*

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

2 of 4. Verify the classification level of the System Security Plan (SSP)

- ○ ISSM
- ○ SCA
- ⦿ Both *(correct response)*

Feedback: *The ISSM must review the security classification guidance and verify the classification level of the SSP and all artifacts prior to submission to DSS. The SCA validates the classification level.*

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

- ○ ISSM
- ⦿ SCA *(correct response)*
- ○ Both

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

4 of 4. Make authorization recommendation

- ○ ISSM
- ⦿ SCA *(correct response)*
- ○ Both

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

Lesson 7 Review Activities

Review Activity 1

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

- ○ Information System Security Manager (ISSM)
- ○ Security Controls Assessor (SCA)
- ⊙ Authorizing Official (AO) *(correct response)*
- ○ Information Owner (IO)

Feedback: *The AO issues the authorization decision.*

Review Activity 2

Which of the following are parts of the security authorization package?

- ☑ System Security Plan (SSP) *(correct response)*
- ☑ Supporting artifacts *(correct response)*
- ☑ Security Assessment Report (SAR) *(correct response)*
- ☑ Authorization recommendation *(correct response)*

Feedback: *These are all included in the security authorization package.*

Review Activity 3

Description 1 of 3. The contractor may begin processing classified information.

- ☑ ATO *(correct response)*
- ☑ ATO with terms and conditions *(correct response)*
- ☐ DATO

Feedback: *When ATO is issued, even with terms and conditions, the contractor may begin processing classified information.*

Description 2 of 3. The contractor must respond to corrective actions.

- ☐ ATO
- ☑ ATO with terms and conditions *(correct response)*
- ☑ DATO *(correct response)*

Feedback: *When ATO with terms and conditions or DATO is issued, the contractor must respond to corrective actions.*

Description 3 of 3. The contractor must cease operation of the Information System immediately.

- ☐ ATO
- ☐ ATO with terms and conditions
- ☑ DATO *(correct response)*

Feedback: *When DATO is issued, the contractor must cease operation of the Information System immediately.*

Lesson 8 Review Activities

Review Activity 1

When does continuous monitoring begin?

- ○ Only after full Authorization to Operate (ATO) is issued
- ○ As soon as the contract is awarded
- ○ When the Security Controls 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

1 of 6. Conducts remediation actions

- ⊙ ISSM *(correct response)*
- ○ SCA
- ○ AO

Feedback: *The ISSM conducts remediation actions based on ongoing monitoring activities.*

2 of 6. Reviews security status reports

- ○ ISSM
- ⊙ SCA *(correct response)*
- ○ AO

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

3 of 6. Updates the System Security Plan (SSP)

- ⊙ ISSM *(correct response)*
- ○ SCA
- ○ AO

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

4 of 6. Determines when reauthorization is needed

- ○ ISSM
- ○ SCA
- ⦿ AO *(correct response)*

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

5 of 6. Verifies proper sanitization of storage media

- ○ ISSM
- ⦿ SCA *(correct response)*
- ○ AO

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

6 of 6. Issues Information System removal and decommissioning letter

- ○ ISSM
- ○ SCA
- ⦿ AO *(correct response)*

Feedback: *The AO issues the Information System removal and decommissioning letter.*