Introduction to the NISP RMF A&A Process

Student Guide

January 2022

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Introduction

Welcome

Information system security is an essential element of overall national security and the protection of our warfighters. Authorized information systems used by cleared contractor companies play a vital role in keeping our nation's information secure. These systems must be assessed and authorized using a standard process to ensure that they operate at an acceptable level of risk. In this course, you will learn about the Risk Management Framework, or RMF, process for assessing and authorizing contractor information systems.

Objectives

Here are the course objectives. Take a moment to review them.

- Identify and define the components of the risk management process
- Identify key sources of risk
- Identify and define security objectives and the characteristics of security controls
- Explain how impact levels are assigned to confidentiality, integrity, and availability
- Define Risk Management Framework (RMF) Assessment and Authorization (A&A) process and identify its purpose and timeline
- Identify the legal, regulatory, and contractual requirements that govern the RMF A&A process
- Identify and define Defense Counterintelligence and Security Agency (DCSA) and contractor roles and responsibilities related to the RMF A&A process

Lesson 2: The Risk Management Process

Introduction

Objectives

Risk management is the backbone of the Risk Management Framework, or RMF, Assessment and Authorization, or A&A, process of ensuring contractor classified information systems adequately protect information. In this lesson, you will learn about components of the risk management process and the sources of risk. You will also learn about security objectives, impact levels, and confidentiality, integrity, and availability of information systems.

Here are the lesson objectives. Take a moment to review them.

- Identify and define the components of the risk management process
- Identify key sources of risk
- Identify and define security objectives and characteristics of security controls
- Explain how impact levels are assigned to confidentiality, integrity, and availability

Risk, Vulnerabilities, and Threats

Risk

Risk is a function of the likelihood of a threat exploiting a vulnerability and the resulting consequence of that adverse event on the organization. Risk is a major factor in the RMF A&A process. Information systems that are deemed to operate at an acceptable level of risk are granted Approval to Operate, or ATO, while those that do not are Denied Approval to Operate, or DATO. It is important to understand what threats and vulnerabilities mean in the context of the RMF A&A process. Let’s take a closer look.

Vulnerabilities

Vulnerabilities are weaknesses in design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. Vulnerability points include physical security, information system software and hardware, as well as data and people. In evaluating a system, it is important to consider all aspects of each vulnerability—the ease and potential rewards of its exploitation, its probability of occurrence, related threats, and residual risk.

Threats

Threats are any source or event with the potential to cause harm to an information system. Threats may or may not be controllable. Threats are always present and generally occur when least expected. Threats may be intentional and targeted or unintentional and accidental.

Whether intended or not, threats may come from a variety of sources. Human threats are caused by people and can be caused by unintentional acts such as mistakenly downloading a malicious attachment, or by deliberate actions such as knowingly stealing information. Natural threats include events such as floods, earthquakes, tornadoes, and electrical storms. Environmental threats include long-term power failure, pollution, chemical spills, or liquid leakage.

What is Risk Management?

Components

Risk management is essential to the RMF A&A process. It is the tool organizations use to minimize the overall risk to their information systems. Within the RMF A&A process, the Plan of Action and Milestones, or POA&M, is one tool used to address risk.

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization. We will briefly describe each of the four risk management components FRAME, ASSESS, RESPOND, and MONITOR the process.

The first component of risk management addresses how organizations frame risk or establish a risk context—that is, describing the environment in which risk-based decisions are made.

The second component of risk management addresses how organizations assess risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify threats to organizations, internal and external vulnerabilities, the harm—that is the consequences or impact, to organizations that may occur given the potential for threats exploiting vulnerabilities and the likelihood that harm will occur.

The third component of risk management addresses how organizations respond to risk once that risk is determined based on the results of risk assessments.

The fourth component of risk management addresses how organizations monitor risk over time.

Let’s take a closer look at what each of these steps entails.

FRAME Risk

FRAME risk describes how organizations frame risk or establish a risk context - that is, describes the environment in which risk-based decisions are made to produce a risk management strategy. Additionally, it establishes a realistic and credible risk frame that requires organizations to identify risk assumptions (for example, assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time); Identify risk constraints (that is, constraints on the risk assessment, response, and monitoring alternatives under consideration); Identify risk tolerance (for example, levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and finally, identify priorities and trade-offs (that is, the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses).

The output to FRAME risk is a risk management strategy that addresses how organization intend to assess risk, respond to risk, and monitor risk.

Assess, Monitor, Respond Risk

The purpose of the assessment component is to identify threats to organizations, internal and external vulnerabilities, the harm that may occur, and the likelihood of the harm occurring. How organizations respond is based on the risk assessment.

Risk response identifies, evaluates, decides on, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to organizational operations and assets, individuals, other organizations, and the Nation.

This component of risk management addresses how organizations monitor risk over time. It verifies how planned risk responses are implemented, determines the ongoing effectiveness, and identifies risk-impacting changes.

Risk Respond Options

Options are:

Accept - Risk acceptance is the appropriate risk response when the identified risk is within the organizational risk tolerance.

Avoid - Risk avoidance may be the appropriate risk response when the identified risk exceeds the organizational risk tolerance.

Mitigate - Risk mitigation, or risk reduction, is the appropriate risk response for that portion of risk that cannot be accepted, avoided, shared, or transferred.

Share or Transfer - Risk sharing or risk transfer is the appropriate risk response when organizations desire and have the means to shift risk liability and responsibility to other organizations. Risk transfer shifts the entire risk responsibility or liability from one organization to another organization.

Share - Risk sharing shifts a portion of risk responsibility or liability to other organizations

Transfer - Risk transfer shifts the entire risk responsibility or liability from one organization to another organization

Security Objectives and Controls

Security Objectives

Part of risk management involves examining the ability of information systems to meet their security objectives. The operation of all information technology systems has five main objectives, though the requirements for each objective depend to some extent on the specific environment.

- *Confidentiality* preserves authorized restrictions on information disclosure and includes the ability to protect personal privacy and proprietary information. For example, confidentiality guards against a user without proper clearance accessing classified information.

- *Integrity* guards against improper modification to or destruction of information. For example, integrity prevents a user from improperly or maliciously modifying a database.
- *Availability* ensures timely and reliable access to and use of information. For example, availability ensures that an information system is accessible when an authorized user needs it.
- *Non-repudiation* ensures that a party in an electronic exchange cannot deny their participation or the authenticity of the message. For example, a digital signature in an email message confirms the identity of the sender.
- *Authentication* ensures that the identity of a user has been verified prior to allowing access to an information system. For example, a Common Access Card, or CAC, is one method to provide system identification that authenticates the user.

Rollover Text:

- **Confidentiality**: Assurance that information is not disclosed to unauthorized individuals, processes, or devices
- **Integrity**: Assurance that information is not modified or destroyed via unauthorized means
- **Availability**: Assurance that information is available to users in a timely manner
- **Non-repudiation:** Assurance that electronic messages are authentic
- **Authentication**: Assurance that the identity of users has been verified prior to allowing access to an information system

Impact Levels

Cleared contractor facilities must meet requirements based on the impact levels defined for the information their systems will process. There are three impact levels, and they are defined based on the confidentiality, integrity, and availability of the information.

The risk management process considers the impact level of an information system and uses it to determine the amount of risk associated with operating the system. This information contributes to the overall risk determination that is used to make authorization decisions.

When the loss of integrity or availability of the information would have a limited adverse effect on organizational operations, assets, or individuals, the associated impact level is low. Any loss of confidentiality must be considered either moderate or high impact. When the loss of confidentiality, integrity, or availability of the information would have a serious adverse effect on organizational operations, assets, or individuals, the associated impact level is moderate. When the loss of confidentiality, integrity, or availability of the information would have a severe or catastrophic adverse effect on organizational operations, assets, or individuals, the associated impact level is high.

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* *By definition, the impact of loss of Confidentiality must be either moderate or high.	limited adverse effect on organizational operations, assets, or individuals	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

Security Controls

An information system’s baseline security controls depend on the security requirements of the system based on the impact level of the information it will process. Security controls are organized into families by the National Institute of Standards and Technology Special Publication, or NIST SP, 800-53, Security and Privacy Controls for Information Systems and Organizations.

The security controls in each of these families must have certain characteristics. A security control must be something that can be tested. For example, you can validate if there are backup copies of all critical software stored in an appropriate location. Also, compliance with the control must be measurable. To continue our previous example, you can determine if there is compliance or non-compliance with the requirement to safely store backup copies of critical software. Additionally, implementation of security controls must be actions or activities that can be assigned to an individual. One person can be assigned responsibility for making backup copies of software and storing it in the correct location. Finally, because security controls are assignable, there is accountability for keeping information systems secure.

Examples of Security Control Families:

- Access Control
- Implementation
- Awareness and Training
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Physical and Environmental Protection

Review Activity

Overview

You are overseeing the risk management process for the implementation of an information system with a small user base at your organization. As you step through the risk management process review activity, questions will appear for you to answer. When you answer a question correctly, the risk level associated with your information system lowers. Answer carefully, though—when you answer a question incorrectly, the risk level associated with the information system rises! How much can you reduce the risk associated with the system?

Part 1

This component describes an environment in which risk-based decision are made:

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

○ MONITOR

○ FRAME

○ ASSESS

○ RESPOND

Part 2

True or false? To determine the risk associated with the information system, you must assess the likelihood of a threat exploiting a vulnerability and the impact that would have on your organization.

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

○ True

○ False

Part 3

As you consider possible threats to the information system, you spot the following in your facility. Are any of these potential sources of threat?

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

□ An untrained user who unknowingly shares sensitive information

□ A leaking pipe in the server room

□ A hacker targeting the local area network

□ A weather report of severe thunderstorms in the area

Part 4

Now that you have assessed the risk, what would be the next step?

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

○ MONITOR

○ FRAME

○ ASSESS

○ RESPOND

Part 5

How well do you know the security objectives of information systems?

Match each objective and its description. Check your answer in the Answer Key at the end of this Student Guide.

Descriptions:

A. Assurance that information is not disclosed to unauthorized individuals, processes, or devices

B. Assurance that information is not modified or destroyed via unauthorized means

C. Assurance that information is available to users in a timely manner

D. Assurance that electronic messages are authentic

E. Assurance that the identity of users has been verified prior to allowing access to an information system

Objectives:	**Responses:**
Authentication	
Availability	
Confidentiality	
Integrity	
Non-repudiation	

Part 6

You have determined that the impact of a loss of availability to the information would result in a serious adverse effect on your organization's operations, assets, or individuals. What is the associated impact level?

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

○ Low

○ Moderate

○ High

Part 7

What characteristics must all security controls possess?

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

□ Testable

□ Measurable

□ Assignable

□ Accountable

Part 8

What are the three impact levels?

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

○ Low, Medium, High

○ Low, Moderate, High

○ Small, medium, Large

○ Moderate, High, Very High

Debrief

You have completed the risk management review activity.

Summary

You have completed the Risk Management Process lesson.

Lesson 3: RMF Assessment and Authorization Overview

Introduction

Objectives

To ensure that contractor information systems are able to properly safeguard the critical information they contain, each system must be assessed and authorized to meet established standards and fulfill the security requirements of the 32 CFR Part 117 National Industrial Security Program Operating Manual, or NISPOM. In this lesson, you will learn about the Risk Management Framework, or RMF, Assessment and Authorization, or A&A, process. You will also learn about its purpose, the requirements that govern it, and the steps it entails.

Here are the lesson objectives. Take a moment to review them.

- Define Risk Management Framework (RMF) Assessment and Authorization (A&A) process and identify its purpose and timeline
- Identify the legal, regulatory, and contractual requirements that govern the RMF A&A process

Background

DCSA Role in RMF A&A

The Defense Counterintelligence and Security Agency, or DCSA, plays an integral role in providing guidance and procedures for RMF A&A compliance for contractors operating under the National Industrial Security Program, or NISP. DCSA has the responsibility of assessing risks, vulnerabilities, and threats to cleared contractor information systems. The RMF A&A process requires organizations to implement countermeasures, security controls, and other protection measures to minimize risks to information systems as much as possible.

A&A Purpose

The RMF A&A process is crucial to information system security as it protects against:

- Threats from both outside users and authorized, inside users
- Vulnerabilities in information technology systems
- Information leaks
- Malicious software and virus attacks
- Hackers

When a system is assessed and authorized under the DCSA RMF A&A process, it means the system has adequate countermeasures in place to protect against these threats and vulnerabilities. Let’s take a closer look at what this means.

Definitions

What is assessment and authorization?

Assessment refers to testing and evaluating the security controls applied to an information system. This ensures the controls are correctly implemented, operating as intended, and meet the security requirements for the system. Assessment first validates that an information system has adequate protection measures in place and then verifies that those measures are actually implemented on the system and are functioning properly.

Authorization is the official decision by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations, including mission, functions, image, or reputation; organizational assets; individuals; other organizations; and the nation. The implementation of the agreed upon set of security controls and prescribed set of safeguards form the basis for the authorization decision. For cleared contractors, this means that DCSA, as the designated Cognizant Security Agency, or CSA, approves the contractor information system to process classified information and acknowledges that the information system has an acceptable level of risk to adequately protect classified information.

Let’s take a closer look at the steps involved in the RMF A&A process.

RMF A&A Process

The RMF A&A process is a continuous process designed to validate that information systems processing classified information meet the requirements for authorization and maintain the authorized security posture from system inception through termination. The NISP Authorization Office, or NAO, oversees this process for cleared contractor information systems.

The process begins when a cleared contractor receives a DD Form 254, DOD Contract Security Classification Specification. First, the contractor prepares to execute the RMF from both the organization and system level perspectives. Next, the contractor categorizes the information system and the information processed, stored, and transmitted by the system based on an analysis of the impact due to a loss of confidentiality, integrity, and availability. Next, the contractor selects an initial set of baseline security controls for the information system based on the security categorization of the system and tailors them as needed. Then, the contractor implements the security controls and describes how they are employed within the information system and its environment of operation. The contractor then performs a self-assessment of the information system to ensure it meets security requirements before requesting that DCSA perform an on-site assessment and grant Approval to Operate, or ATO.

The Authorizing Official, or AO, at DCSA grants or denies approval based on a risk determination. If the AO grants ATO, the information system undergoes continuous monitoring to ensure the controls remain effective and that the impacts of any changes are assessed. If, at any point, the information system is no longer needed, the AO withdraws the system’s authorization and the contractor implements the decommissioning strategy.

Prepare Step

The Prepare Step focuses 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. It is divided into two categories: Organization Tasks, and System Tasks.

Organization Level Tasks

- Task P-1: Identifying and assigning individuals to key roles in the execution of the RMF
- Task P-2: Establishing a risk management strategy for the organization that includes a determination and expression of organizational risk tolerance
- Task P-3: Completing an organization-wide risk assessment or updating an existing risk assessment
- Task P-4: Establishing and making available organizationally-tailored control baselines and/or cybersecurity framework profiles (optional)
- Task P-5: Identifying, documenting, and publishing common controls available for inheritance
- Task P-6: Prioritizing organizational systems with the same impact level (optional).
- Task P-7: Developing and implementing an organization-wide strategy for monitoring control effectiveness

System Level Tasks

- Task P-8: Identifying business functions and mission/business processes that the system is intended to support
- Task P-9: Identifying system stakeholders
- Task P-10: Identifying and prioritizing stakeholder assets
- Task P-11: Determining authorization boundaries
- Task P-12: Identifying the types of information processed, stored, and transmitted by the system
- Task P-13: 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 relevant threats, vulnerabilities, impacts, and likelihood that harm will occur
- 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 system information, authorization information, and roles will be documented

Rollover text

- eMASS: Enterprise Mission Assurance Support Service

Outputs:

- RMF Role Assignments
- Business Functions
- Risk Management Strategy
- Mission/Business Processes
- Statement of Risk Tolerance
- System Information Type(s)
- RAR (Risk Assessment Report)
- System Stakeholder List
- List of CCPs
- Asset List
- Common Controls Available via Inheritance
- Documented Authorization Boundary
- Organizational Continuous Monitoring Strategy
- Security Requirements
- Security Architecture
- Supported Missions
- NISP eMASS System Record
- Documentation of the stages through which information passes in the system such as:
  - Data Flow Diagrams
  - Database Schemas
  - Data Dictionaries
  - Other Designated Deliverables

Categorize Step

In this step, the contractor categorizes the system in accordance with the DCSA Assessment and Authorization Process Manual (DAAPM). In addition, the contractor initiates the Security Plan to document the categorization of the system and finally, they document the categorization results in eMASS.

Contractor:

- C-1: Describe and document the characteristics of the system
- C-2: Categorize the system
- C-3: Review security categorization results
- C-4: Populate information not entered during new system registration and document results in eMASS

Outputs:

- System Description
- Updated eMASS System Record
- Security Categorization

Select Step

In this step, the contractor identifies and selects the security controls, tailors the initial controls designates controls as system-specific, hybrid, or common controls, and develops a system-level continuous monitoring strategy.

The outputs of this step are the security control selection, list of tailored controls, overlay selection, updated system details, and a continuous monitoring strategy.

Contractor:

- S-1: Select Security Controls
- S-2: Tailor Initial Controls
- S-3: Designate Controls as Hybrid, System Specific, or Common
- S-4: Develops system-level continuous monitoring strategy
- S-5: Document to include tailoring actions

Outputs:

- Security Control Selection
- List of Tailored Controls
- Overlay Selection
- Updated System Details
- Continuous Monitoring Strategy

Implement Step

In this step, the contractor implements the selected security controls, documents the security control implementation and updates the Security Plan in eMASS.

This step results in an Implementation Plan, System Level Continuous Monitoring Strategy, and Supporting Artifacts.

Contractor:

- I-1: Implements control solutions consistent with regulations
- I-2: Documents security control implementation in the Security Plan
- I-3: Update Security Plan in eMASS

Outputs:

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

Assess Step

In this step, the contractor completes all tasks in the Assess step to include conducting an initial self-assessment, applying any initial remediation actions required based on the findings of the assessment and developing POA&Ms. The Security Plan is finalized and then moved to next stage of the CAC Validation.

The ISSP will then review the final Security Plan and supporting artifacts, conduct an on-site assessment to validate the controls and conclude with reporting the result in eMASS.

Lastly, the contractor will develop/update POA&M based on findings and recommendation from the SAR.

This step produces a finalized Security Plan, Assessment, Review, and Validation of Security Controls, POA&M, and SAR.

Contractor: (Part I)

- A-1: Conducts self-assessment
- A-2: Conducts Remediation Actions
- A-3: Develops POA&M
- A-4: Reviews SCGs, verify classification level of artifacts
- A-5: Finalizes the Security Plan and authorization consideration in eMASS
- A-6: Documents results and compliance status
- A-7: Verifies in eMASS and moves Security Plan to CAC validation
- A-8: Moving the security plan to the next stage of the CAC for validation

ISSP: (Part II)

- A-9: Reviews the Security Plan and artifacts
- A-10: Conducts on-site assessment
- A-11: Validates Controls

Contractor: (Part III)

- A-12: Develops/Update POA&M

Outputs:

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

Authorize Step

In this step, a Security Controls Assessor, or SCA, also known as an Information System Security Professional, or ISSP, verifies the finalized security plan, submits the system security authorization package via the PAC, and applies an assessment decision. The AO provides risk responses for determined risk. The AO may then issue and apply an Authorization to Operate with Conditions, or ATO-C, full Approval to Operate, or ATO, Interim Authorization to Test, or IATT, Denial of Approval to Operate, or DATO, or Decommission.

This step produces a submission of System Security Authorization Package to the PAC, SAR Executive Summary, Application of Approval Status to Security Plan, and Authorization Decision.

All of the documentation developed throughout the RMF is part of the security authorization package, which is maintained throughout the system's lifecycle.

Security Controls Assessor (SCA) / Information System Security Professional (ISSP):

- R-1: Verifies the finalized Security Plan
- R-2: Submits system security authorization package via the PAC
- R-3: Applies an assessment decision

AO:

- R-4: Provides risk responses for determined risk
- R-5: Issues an authorization decision document to include common controls inherited
- R-6: Applies an authorization decision
    - Authorization to Operate with Conditions (ATO-C)
    - Approval to Operate (ATO)
    - Interim Authorization to Test (IATT)
    - Denial of Approval to Operate (DATO)
    - Decommission

Outputs:

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

Rollover Text

Approval to Operate (ATO)

- Granted after the information system is determined to be in compliance by a successful onsite validation to ensure the system is properly configured and protected
- Represents the AO's acceptance of the information technology system and confirmation that the information system is operating at an acceptable level of risk

Denial of Approval to Operate (DATO)

- Represents the AO's determination that a contractor information system cannot operate due to inadequate design, failure to adequately implement assigned controls, or other lack of adequate security
- Halts operation of the system if it is already operational

Authorization to Operate with Conditions (ATO-C)

- Temporary authorization to connect granted under the conditions or constraints

Interim Authorization to Test (IATT)

- Temporary authority to connect granted for a defined period of time to test
- Test data must not be classified or contain program information

Decommission

- A release outcome following the decision that media does not contain sensitive data.
- NOTE: IAW DAAPM: Has the same context as the NIST Term

Monitor Step

After a system is authorized, it must continue to operate at an acceptable level of risk to maintain its authorization. As part of continuous monitoring, the contractor conducts periodic self-assessments of the system, ensure documentation is maintained and reports results to ISSP. Additionally, the contractor implements a decommission plan and make live updates to the system. DCSA also performs periodic system assessments during facility reviews and formally decommissions the system.

In addition, security relevant changes trigger a full reassessment of the system and the AO must reauthorize the system. Even if a security relevant change does not occur, the system undergoes reassessment and reauthorization upon expiration of its ATO, which is typically 3 years from the date of issuance.

Outputs from the Monitor step are the, decommission plan, an updated security plan, updated POA&M remediation or mitigation items, and updated technical, management, and operational security controls. Updated technical, management, and operational security controls are submitted for approval according to the continuous monitoring strategy.

Contractor: (Part I)

- M-1: Monitor all controls IAW the continuous monitoring strategy
- M-2: Conduct ongoing assessments
- M-3: Analyze and respond to continuous monitoring activities
- M-4: Ensure documentation is updated and maintained
- M-5: Report results to ISSP
- M-6: Implement a Decommission Plan
- M-7: Make updates to live system

ISSP: (Part II)

- M-8: Review reported security status
- M-9: Review and submit decommission requests

AO: (Part III)

- M-11: Conduct ongoing authorizations
- M-12: Formally decommission systems

* Security-relevant changes trigger reassessment and reauthorization.

Outputs:

- Decommission Plan
- Updated Security Plan
- Updated POA&M remediation/mitigation items
- Updated Technical, Management, and Operational Security Controls

Rollover Text

- 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

Decommissioning

When the contractor no longer needs the information system, such as at the end of a contractor program, the AO withdraws the system's ATO. The contractor decommissions the information system according to the planned strategy, which determines approaches, schedules, and resources to decommission, specific considerations of decommission, and effectiveness and completeness of decommission actions.

Decommission is the same as the NIST term "disposal." A decommission plan addresses the approach used to securely remove the system and its elements from operation.

A decommission plan determines:

- Approaches of decommission
- Schedules of decommission
- Resources of decommission
- Specific considerations of decommission
- Effectiveness and completeness of decommission actions

Regulatory Basis

Principal Regulations

To be granted ATO, cleared contractor information systems must meet DCSA requirements of key cybersecurity procedures and guidance. The NISPOM Rule establishes the standard procedures and requirements for all government contractors with regard to classified information. 32 CFR Part 117.18 contains the requirements for information system security and specifically addresses Assessment and Authorization.

As the CSA, DCSA is responsible for issuing Industrial Security Letters, or ISLs, that provide further guidance on selected NISPOM changes and issue updated processes and procedures, technical standards, and templates.

The DOD Instruction, or DODI 8510.01, Risk Management Framework for DOD Information Technology, establishes the RMF as the vehicle for assessment and authorization, while the National Institute of Standards and Technology, or NIST, Special Publication 800-137, Information Security Continuous Monitoring, or ISCM, for Federal Information Systems and Organizations establishes requirements and processes for continuous monitoring.

Contractors should refer to the DCSA Assessment and Authorization Process Manual, or DAAPM, for detailed guidance on the RMF A&A process as it applies to contractors. Adherence to the standards in this process manual is required for DCSA to be able to issue an ATO. Keep in mind that the DAAPM is a living document updated regularly by the NISP Authorization Office, or NAO, to reflect changing technologies and the security controls necessary in this changing environment. DCSA strives to issue this document twice a year. It is available to cleared industry personnel; please refer to the NAO section of the DCSA website (https://www.dcsa.mil/mc/ctp/nao/).

Rollover Text

NISPOM Rule: National Industrial Security Program Operating Manual

- Establishes procedures and requirements for government contractors

ISLs: Industrial Security Letters

- Provide guidance, clarification, and implementation of NISPOM changes

DODI 8510.01: Risk Management Framework for DOD Information Technology

- Establishes the RMF as the vehicle for assessment and authorization

NIST SP 800-137: Information Systems Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

- Establishes requirements and processes for continuous monitoring.

DAAPM: DCSA Assessment and Authorization Process Manual provides RMF A&A process:

- Guidance
- Standards
- Templates

Other Regulations

There are a variety of other policies that govern the RMF A&A process. As part of DCSA responsibilities under the NISP, the RMF A&A process must stay consistent with federal and intelligence community general policies.

One of these is the Director of National Intelligence, or DNI, Committee of National Security System Instruction, or CNSSI, 1253, Security Categorization and Control Selection for National Security Systems. This instruction provides the baseline set of controls, as well as tailoring guidance, to ensure that organizations select a robust set of security controls to secure their national security systems, based on assessed risk.

The NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, provides guidelines for the security authorization of federal information systems.

The NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, contains recommended security controls for federal information systems and organizations. This instruction provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

The Federal Information Process Standards, or FIPS, Publication 200, Minimum Security Requirements for Federal Information and Information Systems, identifies the minimum security requirements for information and information systems.

Finally, although not currently applicable under the NISP, the Federal Information Security Modernization Act, or FISMA, requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

The concepts and general security concerns and requirements are applicable to DOD and NISP system security controls.

Rollover Text
CNSSI 1253: Security Categorization and Control Selection for National Security Systems
Provides:

- Baseline controls
- Tailoring guidance

NIST SP 800-37: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

- Provides guidelines for the security authorization of federal information systems

NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations

- Provides guidelines for selecting and specifying security controls

FIPS Pub 200: Minimum Security Requirements for Federal Information and Information Systems

- Identifies the minimum security requirements for information and information systems

FISMA: Federal Information Security Modernization Act

- Requires information security for systems that support the operations and assets of the agency

Review Activity

Part 1

What does the RMF A&A process protect against?

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

☐ Threats from outside users

☐ Threats from insider or authorized users

☐ Vulnerabilities in information systems

☐ Information leaks

☐ Malicious software and virus attacks

☐ Hackers

Part 2

In which Step of RMF are the roles and responsibilities selected?

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

- ○ Categorize Step
- ○ Implement Step
- ○ Prepare Step
- ○ Assess Step

Part 3

In which step of the RMF A&A process does the contractor develop a system-level continuous monitoring strategy?

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

- ○ Categorize Step
- ○ Select Step
- ○ Authorize Step
- ○ Monitor Step

Part 4

In which step of the RMF A&A process does the contractor document security control implementation in the Security Plan?

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

- ○ Categorize Step
- ○ Select Step
- ○ Implement Step
- ○ Assess Step

Part 5

In which step of the RMF A&A process does the contractor evaluate the implementation of the security controls?

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

- ○ Implement Step
- ○ Assess Step
- ○ Authorize Step
- ○ Monitor Step

Part 6

Which document establishes procedures and requirements for all government contractors with regard to classified information?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ National Industrial Security Program Operating Manual Rule (NISPOM)
- ○ Industrial Security Letter (ISL)
- ○ DCSA Assessment and Authorization Process Manual (DAAPM)
- ○ Federal Information Security Modernization Act (FISMA)

Part 7

Which document provides RMF A&A process guidance, standards, and templates for government contractors?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ National Industrial Security Program Operating Manual Rule (NISPOM)
- ○ Industrial Security Letter (ISL)
- ○ DCSA Assessment and Authorization Process Manual (DAAPM)
- ○ Federal Information Security Modernization Act (FISMA)

Debrief

You have completed this review activity.

Summary

You have completed the RMF Assessment and Authorization Overview lesson.

Lesson 4: Roles and Responsibilities

Introduction

Objectives

The Risk Management Framework, or RMF, Assessment and Authorization, or A&A, process relies upon a large team of professionals to ensure that information systems processing classified information operate at an acceptable level of risk. This lesson will introduce you to both the Defense Counterintelligence and Security Agency, or DCSA, and cleared contractor roles and responsibilities related to the RMF A&A process.

Here is the lesson objective.

- Identify and define the Defense Counterintelligence and Security Agency, or DCSA, and contractor roles and responsibilities related to the Risk Management Framework, or RMF, Assessment and Authorization, or A&A, process

Background

Introduction to Contractor and DCSA Roles

The RMF A&A process relies on the actions of cleared contractor personnel and DCSA. Cleared contractor personnel work to ensure their systems are developed, operated, and maintained following the requirements of the RMF A&A process. There are DCSA A&A professionals available to support the cleared contractors' A&A efforts and those who make the ultimate authorization decision.

Let's take a closer look by first examining the roles and responsibilities of cleared contractor personnel.

Rollover Text
Contractor Roles:

- FSO: Facility Security Officer
- ISSM: Information System Security Manager
- ISSO: Information System Security Officer

DCSA Roles:

- AO/AODR: Authorizing Official/Authorizing Official's Designated Representative
- SCA: Security Control Assessor
- IS Rep: Industrial Security Representative

Contractor Roles

FSO

The FSO is responsible for ensuring that his or her facility complies with DCSA requirements. As part of the responsibilities, the FSO supervises and directs all security measures for implementation of regulatory requirements at the facility. The FSO also supports the ISSM with the management of information systems at the facility.

Rollover Text

- FSO: Facility Security Officer
- ISSM: Information System Security Manager

ISSM

As the cleared contractor employee with overall responsibility for the information systems security program and for implementing NISP requirements, the ISSM oversees the daily supervision of the cleared contractor's information system security program.

Depending on the size of the contractor's facility, a cleared contractor facility may have one ISSM and one or more alternate ISSMs. In cleared contractor facilities with multiple ISSMs, there is a primary ISSM that assumes responsibility for the facility's overall information systems security program. In addition, the FSO may also serve as the ISSM.

Regardless of whether the ISSM is the sole ISSM for their facility, one of the alternate ISSMs, or the FSO serving as the ISSM, the ISSM certifies to DCSA that all security requirements are in place and the information system is properly configured and protected. The ISSM must be able to effectively and quickly respond to security instances that impact the facility's information system.

The ISSM must be trained to a level commensurate with the level of complexity of the facility's information system. If the ISSM does not have the technical knowledge to securely configure the systems at their facility, he or she may appoint an ISSO to do so. If the ISSM does not meet the requirements, the authorization of the facility's information system may be in jeopardy.

Rollover Text

- ISSM: Information System Security Manager
- ISSO: Information System Security Officer

ISSO

Not all cleared contractor facilities have an ISSO. The ISSO is appointed, when needed, by the ISSM. Like the ISSM, a cleared contractor facility may have one or more ISSOs, depending on the facility's size, number of systems and their complexity. The ISSO is appointed by the ISSM under certain circumstances, such as when the cleared contractor has multiple authorized information systems or when the technical complexity of the cleared contractor's information system security program warrants the appointment.

The ISSM determines the responsibilities for the ISSO. These responsibilities may include ensuring the implementation of security measures in accordance with facility procedures, identifying and documenting any unique threats and performing risk assessments as required, and certifying to DCSA that the assigned security controls have been correctly implemented.

Rollover Text

- ISSM: Information System Security Manager
- ISSO: Information System Security Officer

Users

The users of cleared contractor information systems are vital to the successful operation of those systems. All users must:

- Comply with the information system security program requirements
- Be aware of and knowledgeable about their responsibilities in regard to information system security
- Be accountable for their actions on an information system
- Ensure that any authentication mechanisms, including passwords, are not shared and are protected at the highest classification level and most restrictive classification category of the information to which the system is accredited to process
- Acknowledge, in writing, their responsibilities for protecting the information system and classified information

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.

DCSA Roles

Overview

The NISP Authorization Office, or NAO, is the entity within DCSA responsible for authorizing cleared contractor information systems and providing A&A oversight. Within the NAO, there are several A&A officials responsible for ensuring that cleared contractor facilities meet the RMF A&A process requirements. The Authorizing Official, or AO, has ultimate approving responsibility and authority. However, the AO delegates this responsibility regionally to the Authorizing Official's Designated Representative, or AODR. The Security Control Assessor, or SCA, and Industrial Security Representative, or IS Rep, evaluate, certify, and inspect all information system technical features and safeguards. Each reviews and inspects systems within their level of competence. In addition, the IS Rep is the primary point of contact between DCSA and a cleared contractor facility. Finally, there are a number of other DCSA personnel who support the RMF A&A process.

Let's take a closer look at the responsibilities of each of these roles.

AO/AODR

The AO is the authorizing authority for cleared contractor classified systems, and oversees and manages the A&A of cleared contractor classified information systems to ensure consistency with federal cybersecurity policy. When the system security plan is reviewed and determined to be in compliance and acceptable, it is the AO or AODR that issues the authorization decision.

Rollover Text

- AO/AODR: Authorizing Official/Authorizing Official's Designated Representative
- A&A: Assessment and Authorization

SCA

An SCA is an Information System Security Professional, or ISSP, appointed by the AO to oversee contractor classified information systems. The primary role of the SCA is technical in nature. SCAs are experts in how classified information systems must operate and are usually the primary point of contact to contractors for A&A guidance, support, and advice. SCAs evaluate, certify, and inspect the technical features and safeguards for all types of information systems within their level of competence. Additionally, SCAs ensure physical, operational, and technical controls are implemented and are adequate to protect the classified information resident on the information system. The SCA's assessment enables the AO or AODR to grant the authorization determination.

Rollover Text

- SCA: Security Control Assessor
- ISSP: Information System Security Professional
- AO: Authorizing Official/Authorizing Official's Designated Representative
- A&A: Assessment and Authorization
- AODR: Authorizing Official's Designated Representative

IS Rep

IS Reps are the primary points of contact between DCSA and cleared contractor facilities. IS Reps serve as important resources for cleared contractor facilities. They provide advice and assistance to cleared contractors on the RMF A&A process for certain information systems and other security related matters. Finally, IS Reps keep the SCA and AO or AODR updated on the status of the cleared contractor's overall security compliance posture.

Rollover Text

- IS Rep: Industrial Security Representative
- RMF A&A: Risk Management Framework Assessment and Authorization
- SCA: Security Control Assessor
- AO/AODR: Authorizing Official/Authorizing Official's Designated Representative

Other Agency Personnel

Other agency personnel may be involved in the RMF A&A process, depending on the agency relationship the particular contractor facility holds.

Cognizant Security Agency (CSA):

- Establishes security requirements and ensures cleared contractors processing classified information meet those requirements.
- DOD is the largest of the five designated CSAs.

Information Owner (IO):

- Issues DD Form 254, DOD Contract Security Classification Specification to allow classified processing
- Approves special procedures:
- Clean-up procedures for data spills
- Alternate trusted download procedures
- Specific security requirements

RMF Risk Executive Function:

- Ensures consistency across an organization regarding information systems:
- Risk considerations align with overall strategic goals and objectives
- Security risks and risk tolerance are managed consistently

Information System Security Officer (ISSO): An ISSO is an individual responsible for ensuring the appropriate operational security posture is maintained for a system. The ISSO will be assigned by the ISSM and appointed in writing. The ISSO must be a U.S. citizen and employed by the cleared contractor or its subcontractor. The ISSO assists the ISSM in meeting their duties and responsibilities.

Common Control Provider (CCP): A CCP is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (e.g., security controls inherited by systems). The CCP may be an entity in the organization other than the assigned ISSO/ISSM for a system that maintains these controls under a larger umbrella.

Review Activity

Who Am I? Round 1

Can you figure out who the mystery person is using the process of elimination? Use the hints to determine who the mystery person is.

Hint 1: I work for a cleared contractor.

Hint 2: My facility also employs others in my role.

Hint 3: I oversee the security of information systems at my facility.

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

○ Facility Security Officer (FSO)

○ Authorizing Official (AO)

○ Information System Security Manager (ISSM)

○ Security Control Assessor (SCA)

○ Information System Security Officer (ISSO)

○ Industrial Security Representative (IS Rep)

Rollover Text:

- FSO: Facility Security Officer
- AO: Authorizing Official
- ISSM: Information System Security Manager
- SCA: Security Control Assessor
- ISSO: Information System Security Officer
- IS Rep: Industrial Security Representative

Who Am I? Round 2

Can you figure out who the mystery person is using the process of elimination? Use the hints to determine who the mystery person is.

Hint 1: I work for DCSA.

Hint 2: I provide advice and assistance to cleared contractors on the A&A process.

Hint 3: I assess the implementation of security controls to ensure the protection of classified information.

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

○ Facility Security Officer (FSO)

○ Authorizing Official (AO)

○ Information System Security Manager (ISSM)

○ Security Control Assessor (SCA)

○ Information System Security Officer (ISSO)

○ Industrial Security Representative (IS Rep)

Rollover Text

- FSO: Facility Security Officer
- AO: Authorizing Official
- ISSM: Information System Security Manager
- SCA: Security Control Assessor
- ISSO: Information System Security Officer
- IS Rep: Industrial Security Representative

Summary

You have completed the Roles and Responsibilities lesson. Open the Student Guide to review.

Lesson 5: Course Conclusion

Conclusion

Course Summary

To ensure that contractor information systems are able to properly safeguard the critical information they contain, each system must be assessed to ensure it meets established standards and may be authorized to operate. The Defense Counterintelligence and Security Agency, or DCSA, uses the Risk Management Framework, or RMF, Assessment and Authorization, or A&A, process to approve the operation of information systems processing classified information. Ensuring that cleared contractors have strong information system security programs is essential to keeping information secure and protects both national security and the lives of warfighters.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- The Risk Management Process
- RMF Assessment and Authorization Overview
- Roles and Responsibilities

Lesson Summary

Congratulations. You have completed the *Introduction to the NISP RMF A&A Process* course.

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

- Identify and define the components of the risk management process
- Identify key sources of risk
- Identify and define security objectives and the characteristics of security controls
- Explain how impact levels are assigned to confidentiality, integrity, and availability
- Identify the legal, regulatory, and contractual requirements that govern the RMF A&A process
- Identify and define Defense Counterintelligence and Security Agency (DCSA) and contractor roles and responsibilities related to the RMF A&A process

To receive course credit, you must take the Introduction to the NISP RMF A&A Process examination. Select Exit to return to the course page; then, select Launch Exam to begin the online exam.

Appendix A: Answer Key

Lesson 2 Review Activity

Part 1

This component describes an environment in which risk-based decision are made:

○ MONITOR

○ FRAME *(correct response)*

○ ASSESS

○ RESPOND

Feedback: The first component, FRAME, describes the environment in which risk-based decisions are made.

Part 2

True or false? To determine the risk associated with the information system, you must assess the likelihood of a threat exploiting a vulnerability and the impact that would have on your organization.

○ True *(correct response)*

○ False

Feedback: *Risk is comprised of vulnerabilities that threats may exploit and the consequences of that adverse event occurring.*

Part 3

As you consider possible threats to the information system, you spot the following in your facility. Are any of these potential sources of threat?

□ An untrained user who unknowingly shares sensitive information *(correct response)*

□ A leaking pipe in the server room *(correct response)*

□ A hacker targeting the local area network *(correct response)*

□ A weather report of severe thunderstorms in the area *(correct response)*

Feedback: *All of these things are sources of threat. Threats can be intentional or unintentional and may come from human, natural, or environmental sources.*

Part 4

Now that you have assessed the risk, what would be the next step?

- ○ MONITOR
- ○ FRAME
- ○ ASSESS
- ○ RESPOND *(correct response)*

Feedback: *The third component of risk management addresses how organizations respond to risk once that risk is determined based on the results of risk assessment.*

Part 5

How well do you know the security objectives of information systems?

Descriptions:

A. Assurance that information is not disclosed to unauthorized individuals, processes, or devices

B. Assurance that information is not modified or destroyed via unauthorized means

C. Assurance that information is available to users in a timely manner

D. Assurance that electronic messages are authentic

E. Assurance that the identity of users has been verified prior to allowing access to an information system

Objectives:	**Responses:**
Authentication	E
Availability	C
Confidentiality	A
Integrity	B
Non-repudiation	D

Part 6

You have determined that the impact of a loss of availability to the information would result in a serious adverse effect on your organization's operations, assets, or individuals. What is the impact level of the information the system will process?

○ Low

○ Moderate *(correct response)*

○ High

Feedback: *The impact level is Moderate when the unauthorized disclosure, modification, or destruction of the information or the disruption of the ability to access the information would have a serious adverse effect on organizational operations, assets, or individuals.*

Part 7

What characteristics must all security controls possess?

❒ Testable *(correct response)*

❒ Measurable *(correct response)*

❒ Assignable *(correct response)*

❒ Accountable *(correct response)*

Feedback: *Security controls must possess all of these characteristics.*

Part 8

What are the three impact levels?

○ Low, Medium, High

○ Low, Moderate, High *(correct response)*

○ Small, Medium, Large

○ Moderate, High, Very High

Feedback: *There are three impact level which are Low, Moderate, and High.*

Lesson 3 Review Activity

Part 1

What does the RMF A&A process protect against?

- ❐ Threats from outside users *(correct response)*
- ❐ Threats from insider or authorized users *(correct response)*
- ❐ Vulnerabilities in information systems *(correct response)*
- ❐ Information leaks *(correct response)*
- ❐ Malicious software and virus attacks *(correct response)*
- ❐ Hackers *(correct response)*

Feedback: *The RMF A&A process helps guard against both threats and vulnerabilities, which includes all of these things.*

Part 2

In which Step of the RMF are the roles and responsibilities selected?

- ○ Categorize Step
- ○ Implement Step
- ○ Prepare Step *(correct response)*
- ○ Assess Step

Feedback: *The roles and responsibilities are selected during the Prepare Step.*

Part 3

In which step of the RMF A&A process does the contractor develop a system-level continuous monitoring strategy?

- ○ Categorize Step
- ○ Select Step *(correct response)*
- ○ Authorize Step
- ○ Monitor Step

Feedback: *The contractor develops a system-level continuous monitoring strategy during the Select Step.*

Part 4

In which step of the RMF A&A process does the contractor document security control implementation in the Security Plan?

- ○ Categorize System
- ○ Select Step
- ○ Implement Step *(correct response)*
- ○ Assess Step

Feedback: *The contractor documents security control implementation in the Security Plan during the Implement Step.*

Part 5

In which step of the RMF A&A process does the contractor evaluate the implementation of the security controls?

- ○ Implement Step
- ○ Assess Step *(correct response)*
- ○ Authorize Step
- ○ Monitor Step

Feedback: *The contractor conducts a self-assessment of the security controls and conducts initial remediation actions in the Assess Step.*

Part 6

Which document establishes procedures and requirements for all government contractors with regard to classified information?

- ○ National Industrial Security Program Operating Manual Rule (NISPOM) *(correct response)*
- ○ Industrial Security Letter (ISL)
- ○ DCSA Assessment and Authorization Process Manual (DAAPM)
- ○ Federal Information Security Management Act (FISMA)

Feedback: *The NISPOM establishes procedures and requirements for all government contractors handling classified information.*

Part 7

Which document provides RMF A&A process guidance, standards, and templates for government contractors?

- ○ National Industrial Security Program Operating Manual Rule (NISPOM)
- ○ Industrial Security Letter (ISL)
- ○ DCSA Assessment and Authorization Process Manual (DAAPM) *(correct response)*
- ○ Federal Information Security Management Act (FISMA)

Feedback: *The DAAPM provides government contractors guidance, standards, and templates for the RMF A&A process.*

Lesson 4 Review Activity

Who Am I? Round 1

Can you figure out who the mystery person is using the process of elimination?

Hint 1: I work for a cleared contractor.

Hint 2: My facility also employs others in my role.

Hint 3: I oversee the security of information systems at my facility.

- ○ Facility Security Officer (FSO)
- ○ Authorizing Official (AO)
- ○ Information System Security Manager (ISSM) *(correct response)*
- ○ Security Control Assessor (SCA)
- ○ Information System Security Officer (ISSO)
- ○ Industrial Security Representative (IS Rep)

Feedback: *The ISSM oversees information system security at cleared contractor facilities. Large facilities may have multiple ISSMs.*

Who Am I? Round 2

Can you figure out who the mystery person is using the process of elimination?

Hint 1: I work for DCSA.

Hint 2: I provide advice and assistance to cleared contractors on the A&A process.

Hint 3: I assess the implementation of security controls to ensure the protection of classified information.

○ Facility Security Officer (FSO)

○ Authorizing Official (AO)

○ Information System Security Manager (ISSM)

○ Security Control Assessor (SCA) *(correct response)*

○ Information System Security Officer (ISSO)

○ Industrial Security Representative (IS Rep)

Feedback: *The SCA serves as the contractor's primary point of contact for help with the RMF A&A process and ensures adequate and correctly implemented controls.*