Introduction to the NISP RMF A&A Process

Student Guide

July 2017

Center for Development of Security Excellence

Lesson 1: 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 (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 Security Service (DSS) 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 (RMF) Assessment and Authorization (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 (ATO) while those that do not are Denied Approval to Operate (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 (POA&M) is one tool used to address risk. The components of risk management include:

- Risk assessment
- Risk mitigation
- Evaluation of the process

Risk assessment involves identifying and evaluating risks and risk impacts and recommending countermeasures to reduce risk. Risk mitigation takes the countermeasures recommended as part of the risk assessment and prioritizes, implements, and maintains them. Finally, evaluation of the process is continual and is essential for implementing a successful risk management program. Let's take a closer look at what each of these steps entails.

Risk Assessment

Risk assessment is used to determine the extent of the potential threat to an information system and the risk associated with it. To determine the likelihood of a future adverse event, threats to an information system must be analyzed together with the system's potential vulnerabilities and countermeasures - which are also referred to as controls. The output of risk assessment helps identify the appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk Mitigation

Risk mitigation takes the countermeasures recommended as part of the risk assessment and prioritizes, implements, and maintains them. Because it's not possible to eliminate all risk, it is important to implement the most appropriate controls to decrease risk to an acceptable level, with minimal adverse impact on the organization's resources and mission.

Risk Mitigation Options

Approaches to Risk Mitigation

- Risk Planning: To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.
- Research and Acknowledgment: To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.

Risk Mitigation Options

- Risk Acceptance: To accept the potential risk and continue operating the information system or to implement controls to lower the risk to an acceptable level.
- Risk Avoidance: To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).
- Risk Limitation: To limit the risk by implementing controls to minimize the adverse impact of a threat exploiting a vulnerability (e.g., use of supporting, preventive, detective controls).

Evaluation

Evaluation is a continual process and is vital for implementing a successful risk management program. While there should be a specific schedule for assessing and mitigating mission risks, the process should be flexible enough to allow changes when warranted. An example would be when major changes to an information system are made due to changes resulting from new policies or new technologies. Cleared contractor information systems may need to be re-authorized when security-relevant changes occur or three years from the issuance date of the ATO, whichever comes first. However, the Authorizing Official (AO) may concur with continuation of the ATO without re-authorization when an effective continuous monitoring strategy is in place. It is recommended that contractors evaluate risk management functions on a continual basis in addition to the required annual self-assessment.

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.

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.

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.

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 (NIST SP) 800-53A, Assessing Security and Privacy Controls in Federal 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

First you must determine the extent of the risk associated with the information system. In which component of the risk management process is this task completed?

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

- ○ Evaluation
- ○ Risk Assessment
- ○ Risk Mitigation

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 associated with the information system, you must implement controls to decrease the risk to an acceptable level. In which component of the risk management process is this task performed?

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

- ○ Evaluation
- ○ Risk Mitigation

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 impact level of the information the system will process?

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

Once all of the controls are implemented and Approval to Operate (ATO) is granted, when should you evaluate the system?

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

- ○ Continuously assess and mitigate risks throughout the life cycle of the system
- ○ Wait until the next required evaluation to reassess the system
- ○ Operate the system without continuous evaluation until the ATO expires

Debrief

You have completed the risk management review activity.

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 National Industrial Security Program Operating Manual (NISPOM). In this lesson, you will learn about the Risk Management Framework (RMF) Assessment and Authorization (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 RMF A&A process and identify its purpose and timeline
- Identify the legal, regulatory, and contractual requirements that govern the RMF A&A process

Background

DSS Role in RMF A&A

The Defense Security Service (DSS) plays an integral role in providing guidance and procedures for RMF A&A compliance for contractors operating under the National Industrial Security Program (NISP). DSS 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 DSS 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 DSS, as the designated Cognizant Security Agency (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 (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 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 DSS validate the self-assessment and grant Approval to Operate (ATO). The Authorizing Official (AO) at DSS 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.

Categorize System

In this step, the contractor categorizes the system in accordance with the DSS Assessment and Authorization Process Manual (DAAPM). In addition, the contractor initiates the System Security Plan (SSP) to document the categorization of the system and registers the system with the DoD Component Cybersecurity Program. Finally, the contractor assigns qualified personnel to the RMF A&A process team.

System Security Plan (SSP)

The SSP is the formal document used by the government contractor to identify the protection measures to safeguard information being processed in a classified environment.

Select Security Controls

In this step, the contractor identifies common controls, selects security controls, applies overlays and tailors the controls as needed, develops a system-level continuous monitoring strategy, and internally reviews and approves the SSP and monitoring strategy. The outputs of this step are the SSP and monitoring strategy.

Implement Security Controls

In this step, the contractor implements the control solutions consistent with DoD Component Cybersecurity architectures and documents the security control implementation in the SSP. This step results in an updated SSP.

Assess Security Controls

In this step, the contractor develops and approves a security assessment plan and conducts an initial self-assessment of the security controls. The contractor also conducts any required initial remediation actions based on the findings of the assessment. This step produces a revised SSP.

Authorize System

In this step, DSS begins their review of the system to arrive at an authorization decision. A Security Controls Assessor (SCA), also known as an Information System Security Professional (ISSP), performs a preliminary review of the documentation submitted by the contractor and conducts an onsite assessment to validate the contractor's findings. If vulnerabilities are uncovered, the SCA works with the contractor to document them in a

Plan of Action and Milestones (POA&M) that outlines the severity of the vulnerability and provides a plan and timeline for mitigating the problem.

The SCA prepares a Security Assessment Report (SAR) and makes an authorization recommendation, but the ultimate authorization decision must be issued by the AO. The AO may issue full Approval to Operate (ATO) or Denial of Approval to Operate (DATO).

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

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

Monitor Security Controls

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. DSS also performs periodic system assessments during facility reviews. 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.

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 in the SSP.

Regulatory Basis

Principal Regulations

To be granted ATO, cleared contractor information systems must meet DSS requirements of key cybersecurity procedures and guidance.

The National Industrial Security Program Operating Manual (NISPOM) establishes the standard procedures and requirements for all government contractors with regard to classified information. Chapter 8 contains the requirements for information system security; Section 2 specifically addresses Assessment and Authorization.

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

The DoD Instruction (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 (NIST) Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations establishes requirements and processes for continuous monitoring.

Contractors should refer to the DSS Assessment and Authorization Process Manual (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 DSS to be able to issue an ATO. Keep in mind that the DAAPM is a living document updated regularly by the NISP Authorization Office (NAO) to reflect changing technologies and the security controls necessary in this changing environment. DSS strives to issue this document twice a year. It is available to cleared industry personnel; please refer to the NAO section of the DSS website (www.dss.mil).

Other Regulations

There are a variety of other policies that govern the RMF A&A process. As part of DSS 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 (DNI) Committee of National Security System Instruction (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 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, 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 (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 Management Act (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.

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 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 System
- ○ Select Security Controls
- ○ Authorize System
- ○ Monitor Security Controls

Part 3

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

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

- ○ Categorize System
- ○ Select Security Controls
- ○ Implement Security Controls
- ○ Assess Security Controls

Part 4

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 Security Controls
- ○ Assess Security Controls
- ○ Authorize System
- ○ Monitor Security Controls

Part 5

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 (NISPOM)
- ○ Industrial Security Letter (ISL)
- ○ DSS Assessment and Authorization Process Manual (DAAPM)
- ○ Federal Information Security Management Act (FISMA)

Part 6

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 (NISPOM)
- ○ Industrial Security Letter (ISL)
- ○ DSS Assessment and Authorization Process Manual (DAAPM)
- ○ Federal Information Security Management Act (FISMA)

Debrief

You have completed this review activity.

Lesson 4: Roles and Responsibilities

Introduction

Objectives

The Risk Management Framework (RMF) Assessment and Authorization (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 Security Service (DSS) and cleared contractor roles and responsibilities related to the RMF A&A process.

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

- Identify and define the DSS and contractor roles and responsibilities related to the RMF A&A process

Background

Introduction to Contractor and DSS Roles

The RMF A&A process relies on the actions of cleared contractor personnel and DSS. Cleared contractor personnel work to ensure their systems are developed, operated, and maintained following the requirements of the RMF A&A process. There are DSS 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.

Contractor Roles

Overview

Within cleared contractor facilities, the Facility Security Officer (FSO) supervises and directs all security measures for implementation of regulatory requirements at the facility. The Information System Security Manager (ISSM) is appointed by key management personnel such as the FSO, Vice President, or Director of Security. The ISSM holds ultimate responsibility to implement information system security requirements as mandated by the National Industrial Security Program Operating Manual (NISPOM). The FSO supports the ISSM in implementing these requirements at the cleared contractor's facility. Some cleared contractor facilities also have an Information System Security Officer (ISSO). This role is appointed by the ISSM, when necessary, and supports the ISSM in implementing NISP

requirements. Finally, the users of the cleared contractor's information system must follow information system security procedures.

Let's look more closely at each role and its responsibilities.

FSO

The FSO is responsible for ensuring that his or her facility complies with DSS 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.

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 DSS 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.

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 and number and complexity of information systems. 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 DSS that the assigned security controls have been correctly implemented.

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.

DSS Roles

Overview

The NISP Authorization Office (NAO) is the entity within DSS 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 (AO) has ultimate approving responsibility and authority. However, the AO delegates this responsibility regionally to the Authorizing Official's Designated Representative (AODR). The Security Control Assessor (SCA) and Industrial Security Representative (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 DSS and a cleared contractor facility. Finally, there are a number of other DSS 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.

SCA

An SCA is an Information System Security Professional (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.

IS Rep

IS Reps are the primary points of contact between DSS 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.

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.

Other Agency Roles	Responsibilities
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

Other Agency Roles	Responsibilities
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

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)

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 DSS.

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)

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 Security Service (DSS) uses the Risk Management Framework (RMF) Assessment and Authorization (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 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
- Define RMF 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 DSS 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. 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 Activity

Part 1

First you must determine the extent of the risk associated with the information system. In which component of the risk management process is this task completed?

- ○ Evaluation
- ⊙ Risk Assessment *(correct response)*
- ○ Risk Mitigation

Feedback: *Risk assessment is used to determine the extent of risk associated with an information system.*

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 associated with the information system, you must implement controls to decrease the risk to an acceptable level. In which component of the risk management process is this task performed?

- ○ Evaluation
- ⊙ Risk Mitigation *(correct response)*

Feedback: *Risk mitigation takes countermeasures recommended as part of the risk assessment and prioritizes, implements, and maintains them.*

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 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

Once all of the controls are implemented and Approval to Operate (ATO) is granted, when should you evaluate the system?

- ⊙ Continuously assess and mitigate risks throughout the life cycle of the system *(correct response)*
- ○ Wait until the next required evaluation to reassess the system
- ○ Operate the system without continuous evaluation until the ATO expires

Feedback: *Evaluation occurs on a regular schedule and as needed when security-relevant changes occur.*

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 A&A process does the contractor develop a system-level continuous monitoring strategy?

- ○ Categorize System
- ⊙ Select Security Controls *(correct response)*
- ○ Authorize System
- ○ Monitor Security Controls

Feedback: *The contractor develops a system-level continuous monitoring strategy during Step 2, Select Security Controls.*

Part 3

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

- ○ Categorize System
- ○ Select Security Controls
- ⊙ Implement Security Controls *(correct response)*
- ○ Assess Security Controls

Feedback: *The contractor documents security control implementation in the SSP during Step 3, Implement Security Controls.*

Part 4

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

- ○ Implement Security Controls
- ⦿ Assess Security Controls *(correct response)*
- ○ Authorize System
- ○ Monitor Security Controls

Feedback: *The contractor conducts a self-assessment of the security controls and conducts initial remediation actions in Step 4, Assess Security Controls.*

Part 5

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

- ⦿ National Industrial Security Program Operating Manual (NISPOM) *(correct response)*
- ○ Industrial Security Letter (ISL)
- ○ DSS 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 6

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

- ○ National Industrial Security Program Operating Manual (NISPOM)
- ○ Industrial Security Letter (ISL)
- ⦿ DSS 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

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

Hint 1: I work for DSS.

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.*