Student Guide

Course: Introduction to the NISP Certification and Accreditation Process

Lesson 1: Course Introduction

Course Information

Purpose	Provides training on the policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the Certification and Accreditation (C&A) Process and in support of the DSS Mission. In addition, provides an understanding on the contractor requirements under the NISP.
Audience	Military, DSS civilian and other Government personnel, and contractor professionals who have responsibility for evaluating information systems and certifying to the Government that information systems meet security requirements
Pass/Fail %	75%
Estimated completion time	90 minutes

Course Overview

Information system security is an essential element of overall national security and the protection of our warfighters. Accredited information systems used by cleared contractor companies play a vital role in keeping our nation's information secure, and must be certified and accredited using a standard process to ensure that they operate at an acceptable level of risk.

In this course, you will learn about the process for certifying and accrediting contractor information systems.

Course Objectives

- Define certification and accreditation and identify its purpose, process, and timeline
- Identify the legal, regulatory, and contractual requirements that govern the certification and accreditation process
- Identify and define DSS and contractor roles and responsibilities related to the certification and accreditation process
- Identify and define the components of the risk management process
- Identify key sources of risk
- Identify and define security objectives, protection levels, and the need-to-know basis for confidentiality, integrity and availability

Course Structure

- Course Introduction
- Certification and Accreditation Overview
- Roles and Responsibilities
- The Risk Management Process
- Course Conclusion

Student Guide

Course: Introduction to the NISP Certification and Accreditation Process

Lesson 2: Certification and Accreditation Overview

Introduction

Objectives

To ensure that contractor information systems are able to properly safeguard the critical information they contain, each system must be certified and accredited to meet established standards and fulfill the security requirements of the NISPOM.

In this lesson, you will learn about the certification and accreditation process. You will also learn about its purpose, the requirements that govern it, and the steps it entails.

The lesson objectives are:

- Define certification and accreditation and identify its purpose, process, and timeline
- Identify the legal, regulatory, and contractual requirements that govern the certification and accreditation process

Background

1. C&A and the DSS Mission

The Defense Security Service plays an integral role in providing guidance and procedures for certification and accreditation compliance for contractors operating under the NISP.

The mission of DSS is to support national security and the war fighter, to secure the nation's technological base, issue guidance and procedures, and oversee the protection of U.S. and foreign classified information in the hands of industry. The C&A process supports this mission. It is the method DSS uses to set standards and procedures, provide guidance, approve and disapprove the operation of information systems processing classified information.

Ensuring that contractors have strong information system security programs that are authorized to operate by the C&A process is essential to keeping information secure, and is vital to DSS' ability to execute its mission successfully.

2. C&A Purpose

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

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

When a system is certified and accredited under the DSS C&A process, it means the system has adequate countermeasures in place to protect against these threats and vulnerabilities.

3. Risks, Vulnerabilities, and Threats

DSS has the responsibility of assessing risks, vulnerabilities, and threats to cleared contractor information systems. You'll learn more about risk, vulnerabilities, and threats later in this course. For now, you should know that the C&A process requires organizations to implement countermeasures, security controls, and other protection measures to minimize risks as much as possible. To understand how organizations achieve this, you must understand the relationship between risk, threat, and vulnerability.

Risk is the possibility that a particular *threat* will compromise and exploit a particular *vulnerability*. When we assess risk, we estimate the likelihood of a *particular* threat occurring and exploiting a *particular* vulnerability. When a threat successfully exploits system vulnerability, the *consequence* is the potential impact of the resulting loss of information or capabilities. Reducing either the threat or the vulnerability reduces the risk. While threats are hard to control, you *can* minimize vulnerabilities by applying safeguards, or countermeasures, to protect the system.

Together, threats, vulnerabilities, and countermeasures are considered and used to determine the overall risk to a particular information system. An information system that has an acceptable level of risk is granted approval to operate. By accrediting the cleared contractor's information system, the Designated Approving Authority (DAA) officially declares that the contractor's identified protection measures and environment effectively protect classified information from unauthorized access, disclosure, and modification. Information systems that do *not* have an acceptable level of residual risk or protection measures are not approved to operate.

What is Certification and Accreditation?

1. Definition

You've just learned how the C&A process is an important part of how DSS executes its mission. You've learned about what the C&A process helps guard against and you've also learned how threats, vulnerabilities, and the determination of risk apply to the C&A process. But what *is* certification and accreditation?

The following are the official certification and accreditation definitions, as defined by The Office of the Designated Approving Authority (ODAA) Process Manual.

Certification: Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.

Accreditation: The formal declaration by the Designated Approving Authority (DAA) that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Certification is a comprehensive evaluation of the management, operational, and technical security features of an information system performed by the cleared contractor. The certification process is initiated only after the contractor has signed a contract or sponsorship with DoD authorizing it to process classified information. A valid requirement must exist to process classified on an information system in order to initiate the C&A process. Certification 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.

Accreditation is the formal declaration by the DAA that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. More simply put, accreditation is the approval by the cognizant security agency (CSA) for the system to process classified information.

Certifying and accrediting a cleared contractor information system amounts to an acknowledgement that that particular system has an acceptable level of risk to adequately protect classified information. DSS is delegated as the CSA for cleared contract information systems.

2. Process Overview

The C&A life cycle is a continuous process designed to validate that information systems processing classified information meet the requirements for accreditation, and that the systems continue to maintain the accredited security posture throughout their lifecycle: from system inception to termination. The Office of the Designated Approving Authority (ODAA) is the entity that oversees this process for cleared contractor information systems.

The steps in the C&A life cycle are as follows:

Step 1 - Initiation and Planning: The C&A process begins with the contractor initiating and planning the certification and accreditation of their information system.

Step 2 - System Development: In system development, the contractor builds, configures, and tests their system.

Step 3 - Review and Certification: Here, DSS reviews and certifies whether or not the contractor's system meets C&A requirements.

Step 4 - Accreditation Decision: Once the system has been reviewed and certified, DSS can then accredit it.

Step 5 - Continuous Review: Once the system is accredited, in order to maintain its accreditation, the contractor must continue to operate it at an acceptable level of risk. If the contactor does not maintain the information system at an acceptable operation level, DSS can withdraw the accreditation and stop any classified processing until risks are addressed or it may be disestablished.

Step 6 - Disestablishment: When an information system has come to the end of its usefulness – such as at the end of a contract or program – DSS withdraws the system's accreditation.

a. Step 1: Initiation and Planning

The C&A process begins with initiation and planning. The government provides the contractor with DD Form 254, DoD Contract Security Classification Specification, which outlines the security requirements for the contractual data. The contractor then uses that information to determine the requirements of the system.

The contractor should identify and contact their local DSS Representative and Information System Security Professional (ISSP) to obtain an understanding of the C&A requirements, C&A manual and general questions and answers. The contractor may purchase or receive equipment to meet these requirements.

Finally, the contractor creates a System Security Plan and System Profile that document the protection measures needed to secure the system's information.

Initiation and Planning

Contractor:

- Receives DD Form 254, DoD Contract Security Classification Specification
- Determines security requirements
- Identifies and contacts DSS Representative and Information System Security Professional (ISSP)
- Purchases or receives equipment
- Develops System Security Plan

Outputs:

- System Security Plan (SSP):
  - Identifies the protection measures to safeguard the information being processed in a classified environment
  - Provides a description of the system, classification level, protection level, operations, procedures, and security requirements
- IS Profile

b. Step 2: System Development

Once the initiation and planning phase is complete, the process moves to the system development phase. In this phase, the contractor builds, configures, tests, and certifies the system.

Once successfully configured and controls in place, the contractor submits the system security plan. The outputs of this phase are the certification statement, certification checklist, plan of action and milestones (POA&M) and system security plan.

System Development

Contractor:

- Builds system
- Configures system
- Tests system
- Certifies system
- Submits System Security Plan

Outputs:

- Certification Statement: The contractor creates the certification statement to certify that the information system has undergone a comprehensive evaluation of all technical and non-technical security features and safeguards.
- Certification Checklist: This document is used to help the contractor ensure all regulatory requirements are met.
- Plan of Action and Milestones (POA&M), the document addresses:
  - Vulnerabilities the information system is exposed to
  - Specific corrective actions necessary to demonstrate that assigned information assurance controls have been properly implemented
  - Resources required and available to properly complete the corrective actions
- 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.

c. Step 3: Review and Certification

Once the system development phase is complete and the contractor has submitted the certification statement, the information system can be reviewed by DSS. In this phase, the DSS C&A reviewers plan the review or onsite validation. Based on the results, the DSS reviewers make a recommendation to the Regional Designated Approving Authority (RDAA.)

Review and Certification

DSS:

- Plans review or onsite validation
- Makes recommendation to Regional Designated Approving Authority (RDAA)

Output: Recommendation to the RDAA

d. Step 4: Accreditation Decision

Once the information system has been reviewed, DSS issues an accreditation. This activity involves the RDAA evaluating the recommendation from the DSS ISSP or Industrial Security Representative. If DSS is able to accredit the system, they issue an Interim Approval to Operate (IATO) or an Approval to Operate (ATO.) If the system cannot be accredited, DSS does not approve operation.

Accreditation Decision

Regional Designated Approving Authority (RDAA):

- Evaluates the recommendation from reviewers
- Issues accreditation determination

Output: Accreditation determination

- Interim Approval to Operate (IATO):
  - Is granted after the security plan is reviewed and determined to be in compliance and acceptable
  - Allows the information system to operate prior to final accreditation
- Approval to Operate (ATO):
  - Is 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
  - Is the Designated Approving Authority'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):
  - Is the determination that a contractor information system cannot operate because of inadequate design, failure to adequately implement assigned IA Controls, or other lack of adequate security
  - If the system is already operational, the operation of the system is halted

e. Step 5: Continuous Review

Once the information system has been accredited, it must continue to operate at an acceptable level of risk in order to maintain its accreditation.

The system is *reaccredited* when security relevant changes occur or at 3 year intervals – whichever is first. The system is also *reevaluated* when security relevant changes occur.

As part of continuous review, the contractor conducts periodic self-assessments of the system. DSS also does periodic system assessments during facility reviews.

Continuous Review

Includes:

- Reaccreditation
- Reevaluation
- Self-assessments
- Facility reviews

f. Step 6: Disestablishment

When the contractor information system is no longer needed or it has come to the end of its usefulness – such as due to the end of a contract or program - accreditation for the system is withdrawn. As part of disestablishing the system, the contactor removes classification markings, returns classified media to the government customer or destroys classified media using approved methods, and clears all other equipment with volatile memory according to manufacturer's procedures.

Disestablishment

Occurs when:

- System is no longer needed, OR
- Contract expires

Includes:

- Removing classification markings
- Returning classified media to the government customer or destroying classified media using approved methods
- Clearing all other equipment with volatile memory according to manufacturers procedures

Regulatory Basis

1. Principal Regulations

To be authorized to operate, cleared contractor information systems must meet DSS requirements of key information assurance (IA) procedures and guidance.

The National Industrial Security Program Operating Manual (NISPOM) establishes the standard procedures and requirements for all government contractors, with regards to classified information. Chapter 8 contains the requirements for information system security; Section 2 specifically addresses the C&A process.

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

Contractors should also refer to the ODAA Process Manual. It contains certification and accreditation process standards. Adherence to the standards in this process manual is required in order for DSS to be able to issue Approvals to Operate (ATOs.)

Other publications that provide important guidance are the ODAA Standardization of Baseline Technical Security Configurations documents. The purpose of these documents is to establish a baseline standard of technical security controls for information systems for the DSS National Industrial Security Program (NISP) and its participants.

The ODAA documents are living documents. In order to stay abreast of changing technologies and the security controls necessary in this changing environment, these documents are subject to change. DSS strives to issue these documents twice a year. They are available to cleared industry personnel upon request. Please refer to the Industrial Security section of the DSS website.

2. Other Regulations

There are a variety of other policies that govern the C&A process. As part of DSS responsibilities under the NISP, the C&A process must stay consistent with Federal and the Intelligence community general policies.

One of these is the Director of National Intelligence (DNI) Committee of National Security System Instruction 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 National Institute of Standards and Technology (NIST) Special Publication 800-37: Guide for Security Certification and Accreditation of Federal Information Systems provides guidelines for the security authorization of federal information systems.

National Institute of Standards and Technology (NIST) Special Publication 800-53 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.

Federal Information Processing Standards Publication (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 National Industrial Security Program (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 1

You are part of a team that is certifying or accrediting a contractor information system. You know your job is important to the overall DSS mission. Which of the following does the certification and accreditation process protect against? *Select all that apply. Then check your answers 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

Review Activity 2

You are preparing to certify or accredit a contractor information system. Before you do so, you want to revisit the certification accreditation regulations. *Match each regulation with its description. Then check your answer in the Answer Key at the end of this Student Guide.*

Question	Response	Answer Options
You need to review the overarching policy that establishes the procedures for government contractors. Which document should you consult?		A. CNSSI 1253: Security Categorization & Control Selection for National Security Systems B. National Industrial Security Operating Manual (NISPOM) C. ODAA Standardization of Baseline Technical Specifications
You need to check the technical specifications that contractor information systems should use as a baseline. Which document should you consult?		

Lesson Conclusion

1. Summary

In this lesson, you learned about the certification and accreditation process. You learned about its purpose, the requirements that govern it, and the steps it entails.

Answer Key

Review Activity 1

Which of the following does the certification and accreditation process protect against?

- ☑ Threats from outside users
- ☑ Threats from insider or authorized users
- ☑ Vulnerabilities in information systems
- ☑ Information leaks
- ☑ Malicious software and virus attacks
- ☑ Hackers

Review Activity 2

Question	Response
You need to review the overarching policy that establishes the procedures for government contractors. Which document should you consult?	B. National Industrial Security Operating Manual (NISPOM)
You need to check the technical specifications that contractor information systems should use as a baseline. Which document should you consult?	C. ODAA Standardization of Baseline Technical Specifications

Student Guide

Course: Introduction to the NISP Certification and Accreditation Process

Lesson 3: Roles and Responsibilities

Introduction

Objectives

The certification and accreditation process relies upon a large team of professionals to ensure accredited information systems operate at an acceptable level of risk.

This lesson will introduce you to both DSS and cleared contractor roles and responsibilities related to the certification and accreditation process.

The lesson objective is:

- Identify and define DSS and contractor roles and responsibilities related to the certification and accreditation process

Background

1. Introduction to DSS and Contractor Roles

The certification and accreditation (C&A) process relies on the actions of both DSS and cleared contractor personnel.

Cleared contractor personnel work to ensure their systems are developed, operated, and maintained following the requirements of the C&A process.

There are DSS C&A professionals available to support the cleared contactors' C&A efforts and there are DSS C&A professionals who make the ultimate certification decision and accreditation determination.

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

Contractor Roles

1. Overview

Cleared contractor facilities must ensure their information systems are developed, operated, and maintained following the requirements of the C&A process.

Within the cleared contractor's 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 the key management personnel, such as the FSO, Vice President, or Directory 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.

2. FSO

The Facility Security Officer (FSO) is responsible for ensuring that his or her facility complies with DSS requirements. As part of his or her 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.

FSO Responsibilities:

- Supervises and directs all security measures for implementation of regulatory requirements at the facility
- Supports the Information System Security Manger (ISSM) with the management of information systems at the facility

3. 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 one, 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 systems. The ISSM must be trained to a level that commensurate 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 Information System Security Officer (ISSO) to do so.

If the ISSM does not meet the requirements, the accreditation of the facility's information systems may be in jeopardy.

ISSM Responsibilities:

- Is responsible for the security of the information systems at their facility
- Certifies to DSS that all security requirements are in place and the system is properly configured and protected
- Must be able to respond to security instances that impact the facility's information systems

Role Requirements:

- Have an access authorization
- Understand duties and responsibilities
- Possess technical skills to manage the systems under their authority, OR
- Appoint a local Information System Security Officer (ISSO) with the appropriate technical skills

4. 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: when the cleared contractor has multiple accredited information systems, or when the technical complexity of the cleared contractor's information system security warrants the appointment.

When an ISSO is appointed, the ISSM will determine the responsibilities for him or her. 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; developing and implementing a certification test.

In facilities that have an ISSO role, the ISSO must meet the NISP requirements for the facility's information system. If not, its accreditation may be in jeopardy.

ISSO is appointed by the ISSM when:

- Facility has multiple accredited information systems
- Complexity of information system technical features exceeds the capability or knowledge of the ISSM

Responsibilities may include:

- Ensuring the implementation of security measures
- Identifying and document any threats
- Performing risk assessments
- Developing and implementing a certification test

5. 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.

All users must:

- Comply with security requirements
- Know their security responsibilities
- Be accountable for actions
- Protect authentication mechanisms
- Acknowledge responsibilities in writing

General users: May only process data

Privileged users:

- Have elevated access
- Can control the actions that general users can or cannot take

DSS Roles

1. Overview

The Office of the Designated Approving Authority (ODAA) is the entity within DSS that is responsible for accrediting cleared contractor information systems and providing C&A oversight. Within the ODAA, there are several DSS C&A officials responsible for ensuring that cleared contractor facilities meet the C&A process requirements.

The ODAA divides contractor facilities geographically by regions. The Designated Approving Authority (DAA) has ultimate approving responsibility and authority. However, the DAA delegates this responsibility regionally to the *Regional* Designated Approving Authority (RDAA.)

Information System Security Professionals (ISSPs), ISSP Team Leads and Industrial Security Representatives (IS Reps) evaluate, certify and inspect all information system technical features and safeguards. There are several professionals in this role. Each reviews and inspects systems within their level of competence. In addition, IS Reps are also the primary point of contact to between the DSS and cleared contractor facilities.

Finally, there are a number of other DSS personnel that support the C&A process.

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

2. RDAA

The RDAA is the accrediting authority of cleared contractor classified systems, and oversees and manages the C&A of cleared contractor classified information systems to ensure consistency with national computer security information assurance policy.

When an information system plan is reviewed and determined to be in compliance and acceptable, it is the RDAA that grants the interim approval to operate. Once the system successfully passes an on-site validation, the RDAA grants the final approval to operate. The ATO is the official and final acceptance of the information system to process classified information.

RDAA Responsibilities:

- Serves as subject matter expert on information systems
- Oversees and manages status of C&A activities within region
- Grants the Interim Authorization to Operate (ATO) and Authorization to Operate (ATO)

3. ISSPs and Team Leads

ISSPs are organized into teams and managed by a team lead. The primary role of the ISSP is technical in nature. ISSPs are experts in how classified information systems must operate and are usually the primary point of contact of C&A guidance, support, and advice. ISSPs evaluate, certify, and inspect the technical features and safeguards for all types of information systems within their level of competence. Additionally, ISSPs ensure physical, operational, and technical controls are implemented and are adequate to protect the classified information resident on the information system.

The ISSP's assessment enables the RDAA to grant the accreditation determination.

ISSPs and Team Leads:
- Are organized into teams and managed by a team lead
- Are subject matter experts in information systems
- Are normally the primary point of contact of C&A guidance, support, and advice
- Evaluate, certify, and inspect information systems' technical features and safeguards

ISSPs: Notify the RDAA on system compliance

4. IS Reps

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 C&A process for certain IS systems and other security related matters. Finally, IS Reps keep the ISSP and RDAA updated on the status of the cleared contractor's overall security compliance posture.

IS Rep:
- Is the primary DSS POC to Industry
- May provide advice and assistance to cleared contractors on the C&A Process for certain IS systems and other security related matters
- Keeps the ISSP and RDAA updated on the status of the contractor's overall security compliance posture

5. Other Agency Personnel

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

Other Agency Roles	Responsibilities
Government Designated Approving Authorities	• Approves systems under their control for classified processing and communicates this approval to DSS via a memorandum of understanding (MOU) or signed agreement
Government Contracting Authority(GCA)	• Issues DD Form 254, DoD Contract Security Classification Specification to allow classified processing • Approves special procedures: – Clean-up procedures for data spills – Alternate trusted downloading procedures – Risk Acceptance Letters
Government Contracting Officers Technical Representative (COTR)	• Assist GCA and Contracting Officer with technical decision in contract implementation and changes

Review Activity 1

You need to contact a contractor facility's Information System Security Manager (ISSM). Who should you contact? *Select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.*

❍ Maria: Certifies contractor information systems
❍ John: Is responsible for the security of the information systems at his facility and certifies the system
❍ Saul: Main responsibility in the C&A process is to follow security procedures
❍ Louise: Validates that protection measures are correctly implemented on the contractor information system and recommends accreditation

Review Activity 2

As part of your role in certifying and accrediting a contractor's information system, you need to interview a user. Who should you interview? *Select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.*

❍ Maria: Certifies contractor information systems
❍ John: Is responsible for the security of the information systems at his facility and certifies the system
❍ Saul: Main responsibility in the C&A process is to follow security procedures
❍ Louise: Validates that protection measures are correctly implemented on the contractor information system and recommends accreditation

Review Activity 3

You need to see the recommendations received from Information System Security Professional. Who should you contact? *Select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.*

- ❍ Maria: Certifies contractor information systems
- ❍ John: Is responsible for the security of the information systems at his facility and certifies the system
- ❍ Saul: Main responsibility in the C&A process is to follow security procedures
- ❍ Louise: Validates that protection measures are correctly implemented on the contractor information system and recommends accreditation

Review Activity 4

Match each role of the certification and accreditation process on the left to its matching description on the right. Then check your answers in the Answer Key at the end of this Student Guide.

A. Other Agency Personnel	___	Is responsible for C&A oversight for Contractors
B. Information System Security Professional (ISSP) / Team Leads	___	Verifies security measures are implemented
C. Facility Security Officer (FSO)	___	May support the C&A process for a particular contactor facility depending on the agency with which the facility interfaces
D. Industrial Security Representative (IS Rep)	___	Supports the ISSM in implementing NISP requirements at facilities with multiple accredited information systems
E. Office of the Designated Approving Authority (ODAA)	___	Supports the ISSM in implementing NISP requirements
F. Information System Security Officer (ISSO)	___	Is primary DSS point of contact to Industry

Lesson Conclusion

1. Summary

In this lesson, you learned about the contractor and DSS roles and responsibilities related to the certification and accreditation process.

Answer Key

Review Activity 1

You need to contact a contractor facility's Information System Security Manager (ISSM). Who should you contact?

- John: Is responsible for the security of the information systems at his facility and certifies the system

Review Activity 2

As part of your role in certifying and accrediting a contractor's information system, you need to interview a user. Who should you interview?

- Saul: Main responsibility in the C&A process is to follow security procedures

Review Activity 3

You need to see the recommendations received from Information System Security Professional. Who should you contact?

- Louise: Validates that protection measures are correctly implemented on the contractor information system and recommends accreditation

Review Activity 4

A. Other Agency Personnel	E	Is responsible for C&A oversight for Contractors
B. Information System Security Professional (ISSP) / Team Leads	B	Verifies security measures are implemented
C. Facility Security Officer (FSO)	A	May support the C&A process for a particular contactor facility depending on the agency with which the facility interfaces
D. Industrial Security Representative (IS Rep)	F	Supports the ISSM in implementing NISP requirements at facilities with multiple accredited information systems
E. Office of the Designated Approving Authority (ODAA)	C	Supports the ISSM in implementing NISP requirements
F. Information System Security Officer (ISSO)	D	Is primary DSS point of contact to Industry

Student Guide

Course: Introduction to the NISP Certification and Accreditation Process

Lesson 4: The Risk Management Process

Introduction

Objectives

Risk management is a critical factor in the certification and accreditation process.

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, protection levels, and confidentiality, integrity and availability.

The lesson objectives are:

- Identify and define the components of the risk management process
- Identify key sources of risk
- Identify and define security objectives, protection levels and the need-to-know basis for confidentiality, integrity, and availability

Risk, Vulnerabilities, and Threats

1. Risk

As you learned earlier in this course, risk is a function of the likelihood of a threat exploiting a vulnerability, and the resulting impact of that adverse event on the organization.

Risk is a major factor in the certification and accreditation process. Information systems that are deemed to operate at an *acceptable* level of risk are granted an approval to operate. While those which do *not* are not granted approval to operate. It is important to understand what threats and vulnerabilities mean in the context of the C&A process.

2. 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.

3. Threats

Threats are any source or event with the potential to cause harm to an IS 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 or deliberate actions
- **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?

1. Overview

Risk management is essential to the certification and accreditation process.
It is the tool organizations use to minimize the overall risk to their information systems.
Within the certification and accreditation process, the plan of action and milestones (POA&M) is one tool used to address risk.

Risk management includes:

- Risk assessment
- Risk mitigation
- Evaluation

Risk assessment involves identifying and evaluating risks and risk impacts and recommending risk-reducing measures.

Risk mitigation takes the measures recommended as part of the risk assessment and prioritizes, implements, and maintains them.

Evaluation of the process is continual and is essential for implementing a successful risk management program

2. Risk Assessment

Risk assessment is used to determine the extent of the potential threat to and the risk associated with an information system.

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.

3. Risk Mitigation

Risk mitigation takes the measures 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.

Take a moment to review the approaches and risks to mitigating risks.

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 that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls).

4. 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 policies and new technologies.

Cleared contractor information systems are re-accredited when security relevant changes occur or three years from issuance date of the ATO, whichever comes first.

It is recommended that contractors evaluate risk management functions on a continual basis in addition to the required annual self-assessment.

Security Objectives and IA Controls

1. 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 three main objectives, though the requirements for each objective depends 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, confidentially guards against a user without proper clearance accessing classified information.

Integrity guards against improper modification to or destruction of information. For example, integrity guards against a user 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.

2. Protection Levels

Cleared contractor facilities must meet requirements based on the protection level defined for their information systems. There are three protection levels, which are defined based on: clearance, formal access approval, and need-to-know of the system's users and the sensitivity level of the information on the system.

Systems are operating at Protection Level 1 when all users have all required approvals for access to all information on the system.

Systems are operating at Protection Level 2 when all users have all required clearances, and all required formal access approvals, but at least one user lacks the need-to-know for some of the information on the system.

Systems are operating at Protection Level 3 when all users have all required clearances, but at least one user lacks formal access approval for some of the information on the system.

The risk management process considers the protection 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 accreditation decisions.

Take a moment to review the requirements of each protection level.

Protection Level	Lowest Clearance	Formal Access Approval	Need-to-Know
Protection Level 1	At least equal to highest data	All users have approval for all data	All users have a need-to-know for all data
Protection Level 2	At least equal to highest data	All users have approval for all data	Not all users have a need-to-know for all data
Protection Level 3	At least equal to highest data	Not all users have approval for all data	Not contributing to the decision

3. IA Controls

An information system's protection level identifies a specific set of required IA controls. IA controls are organized into subject areas. The IA controls in each of these subject areas must have certain characteristics.

An IA 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 IA 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 IA controls are assignable, there is ***accountability*** for keeping information systems secure.

Review Activity 1

You are helping a contractor facility with its risk management process. Which of the following are potential sources of threat? *Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.*

- ☐ An untrained user who unknowingly shares sensitive information
- ☐ A leaking pipe in the facility's server room
- ☐ A hacker who targets the facility's local area network
- ☐ A local weather report that forecasts severe thunderstorms in the area

Review Activity 2

You are working with a contractor facility and share with them that they need to conduct this activity at least once every three years; though, as a best practice, it should be done annually. Which step to the risk management function are you referring to? *Select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.*

- ❍ Risk Assessment
- ❍ Risk Mitigation
- ❍ Evaluation

Review Activity 3

You are helping a contractor to identify risk-reducing measures. In which phase of the risk management process are you in? *Select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.*

- ❍ Risk Assessment
- ❍ Risk Mitigation
- ❍ Evaluation

Review Activity 4

You are helping a contractor to prioritize risk-reducing measures. In which phase of the risk management process are you in? *Select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.*

- ❍ Risk Assessment
- ❍ Risk Mitigation
- ❍ Evaluation

Review Activity 5

How well do you understand security objectives, protection levels, and IA controls?
Select True or False for each statement. Then check your answer in the Answer Key at the end of this Student Guide.

	True	False
Integrity refers to an information system's protection against unauthorized modification or destruction of information.	○	○
In an information system with a Protection Level 1, all users have approval to access all data.	○	○
The IA Controls that are implemented on an information system depend upon that information system's assigned protection level.	○	○

Lesson Conclusion

1. Summary

In this lesson, you learned about risk. You learned about the components of the risk management process. You learned about security objectives and protection levels and how protection levels identify IA controls.

Answer Key

Review Activity 1

Which of the following are potential sources of threat?

- ☑ An untrained user who unknowingly shares sensitive information
- ☑ A leaking pipe in the facility's server room
- ☑ A hacker who targets the facility's local area network
- ☑ A local weather report that forecasts severe thunderstorms in the area

Review Activity 2

You are working with a contractor facility and share with them that they need conduct this activity at least once every three years; though, as a best practice, it should be done annually. Which step to the risk management function are you referring to?

- ● Evaluation

Review Activity 3

You are helping a contractor to identify risk-reducing measures. In which phase of the risk management process are you in?

- ● Risk Assessment

Review Activity 4

You are helping a contractor to prioritize risk-reducing measures. In which phase of the risk management process are you in?

- ● Risk Mitigation

Review Activity 5

	True	False
Integrity refers to an information system's protection against unauthorized modification or destruction of information.	●	○
In an information system with a Protection Level 1, all users have approval to access all data.	●	○
The IA Controls that are implemented on an information system depend upon that information system's assigned protection level.	●	○

Student Guide

Course: Introduction to the NISP Certification and Accreditation Process

Lesson 5: Course Conclusion

Course Summary

To ensure that contractor information systems are able to properly safeguard the critical information they contain, each system must be certified and accredited to meet established standards.

The certification and accreditation process plays an essential role in fulfilling the mission of the Defense Security Service (DSS.) The C&A process supports this mission. It is the method DSS uses to approve the operation of information systems processing classified information.

Ensuring that cleared contractors have strong information security programs that are authorized to operate by the C&A process 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
- Certification and Accreditation Overview
- Roles and Responsibilities
- The Risk Management Process
- Course Conclusion

Course Objectives

You should now be able to:

- ✓ Define certification and accreditation and the purpose of certifying and accrediting contractor information technology systems
- ✓ Identify the legal, regulatory, and contractual requirements that govern the certification and accreditation process
- ✓ Identify and define the DSS and contractor roles and responsibilities related to the certification and accreditation process
- ✓ Identify and define the components of the risk management process
- ✓ Identify key sources of risk
- ✓ Identify and define security objectives, protection levels, and the need-to-know basis for confidentiality, integrity, and availability

Conclusion

Congratulations. You have completed the Introduction to the NISP Certification and Accreditation Process course.

To receive course credit, you *MUST* take the Introduction to the NISP Certification and Accreditation Process examination. Please use the CDSE STEPP system to register for the online exam.