Student Guide

Continuous Monitoring

Lesson 1: Course Introduction

Contents

Introduction 2

Welcome 2

Objectives..2

Introduction

Welcome

Ensuring security requirements are implemented on classified contracts is essential to protect classified information and national security. However, without continuous monitoring how can you be sure that your information systems are effectively detecting, deterring, and mitigating risks from insider threats, adversarial exploitation, compromise, or other unauthorized disclosures? The continuous monitoring process includes a formal change control methodology of all security relevant aspects of the information system to protect classified and unclassified information.

Adversaries attack the weakest link … where is yours? Have you reported activities discovered through continuous monitoring and audits of your information systems? Welcome to the Continuous Monitoring course.

Objectives

This course provides awareness training on the role of continuous monitoring of information systems in risk management. It explores continuous monitoring strategy and tasks and the roles and responsibilities for continuous monitoring to identify and mitigate vulnerabilities and threats to government information systems, contractor systems processing government information, and technology infrastructure.

Here are the course objectives.

- Identify the role of continuous monitoring through risk management
- Examine how ISCM supports the three-tiered approach to risk management
- Describe how configuration management controls enable continuous monitoring
- Examine audit log support to continuous monitoring
- Understand counterintelligence and cybersecurity personnel support to continuous monitoring

Student Guide

Continuous Monitoring

Lesson 2: Risk Management

Contents

Introduction 3
Objectives 3
NISP Overview 3
National Industrial Security Program 3
Government and Industry Roles 4
Security Policy and Guidance for Continuous Monitoring 4
NISPOM 4
NIST 5
DoD Policy and Guidance 6
Review Activities 8
Review Activity 1 8
Review Activity 2 8
Risk Management Framework (RMF) Overview 9
Risk and Risk Assessment 9
RMF Purpose and Benefits 9
RMF Benefits 9
RMF 3-Tiered Approach 10
RMF 6-Step Process 10
Review Activity 11
Review Activity 3 11
Risk Management Roles and Responsibilities 12
Roles and Responsibilities Overview 12
CIO 12

SISO 12
Risk Executive Function 13
Principal Authorizing Officials (PAOs) 13
DoD Component CIO 13
DoD Component SISO 13
AO 14
AODR 14
ISO 14
PM/SM 15
UR 15
ISSM 15
ISSO 16
Review Activity 17
Review Activity 4 17
Conclusion 18
Lesson Summary 18
Answer Key 19
Review Activity 1 19
Review Activity 2 19
Review Activity 3 20
Review Activity 4 20

Introduction

Objectives

The United States' digital infrastructure is a strategic national asset. Protecting the networks and computers that deliver essential services such as our oil and gas, power, and water is a national security priority. The private sector owns and operates more than 90% of US critical assets. These are systems and assets, whether physical or vital, so vital to the US that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. These risks mean that information security solutions must be broad-based, consensus-driven, and address the ongoing needs of and risks to the government and industry.

Here are the lesson objectives.

- Identify the role of continuous monitoring through risk management
    - Recognize the Risk Management Framework and the role of continuous monitoring
    - Identify the important role of the National Industrial Security Program (NISP) in continuous monitoring
    - Recognize security policy and guidance that supports continuous monitoring of information systems
    - Distinguish the roles and responsibilities for continuous monitoring
    - Identify how the RMF supports risk management

NISP Overview

National Industrial Security Program

While U.S. industry develops and produces the majority of our nation's technology, much of it is classified by the US government.

The National Industrial Security Program (NISP) was established to ensure that cleared industry safeguards classified information in their possession. The NISP is a partnership between the federal government and private industry to safeguard classified information. It applies to all Executive Branch Departments and Agencies and contractors within the U.S. and its territories.

The National Industrial Security Program Operating Manual (NISPOM) defines the requirements, restrictions, and safeguards that industry must follow. These protections are in place before any classified work may begin. As critical assets are increasingly vulnerable to attack from an array of cyber threats, Government agencies have the responsibility to ensure contractor systems compliance with security requirements and continuous monitoring.

Government and Industry Roles

Regardless of where the classified work takes place, at a minimum, the facility must adhere to the NISP and the prescribed requirements, restrictions, and other safeguards defined in the NISPOM to prevent unauthorized disclosure of classified information. It is the Government’s role to establish requirements, advise and assist, and provide oversight in the NISP. Industry’s role is to implement security requirements defined in the NISPOM and the contract.

Security Policy and Guidance for Continuous Monitoring

Continuous monitoring of information systems is a requirement and a necessity to prevent loss of classified information, proprietary industry technology and innovation as well as personal data. Continuous monitoring of information systems requirement applies to industry, federal agencies, and DoD enterprise security personnel.

NISPOM

The NISPOM (DoD 5220.22-M) prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors.

The NISPOM provides detailed industrial security policy and operating instructions for contractors. Chapter 8, Information System Security, delineates the responsibilities, common requirements, protection measures and requirements for classified systems.

- **8-101(a).** The Cognizant Security Agency (CSA) will conduct a risk management evaluation based on the contractor's facility, the classification, and sensitivity of the information processed.
- **8-103(b).** The Information System Security Manager (ISSM) monitors the IS Security Program; **(c).** Identifies and documents unique local threats/vulnerabilities to an information system (IS).
- **8-104.** The Information System Security Officer (ISSO) ensures each IS is covered by the facility Configuration Management Program; implements and documents protection measures; and implements and maintains security-related software for the detection of malicious code, viruses, and intruders.

- **8-303(a).** Each user shall be uniquely identified and that identity shall be associated with all auditable actions taken by that individual.
- **8-602.** Audit Capability

You will learn more about audit capability in continuous monitoring in Lesson 5.

NIST

The National Institute of Standards and Technology (NIST) provides valuable guidance for protection of information systems, published in the following NIST Special Publications:

- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

These NIST SPs were published in accordance with the provisions of the Federal Information Security Management Act (FISMA). These standards, as well as DoD Policy and Guidance, also support the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. This policy and guidance supports the Presidential Memorandum of November 21, 2012 that mandates monitoring of classified information systems.

NIST Special Publication (SP)	Description
NIST SP 800-37, revision 1 **Guide for Applying the Risk Management Framework to Federal Information Systems**	• Provides guidelines for applying the Risk Management Framework (RMF) • Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes
NIST SP 800-137 **Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations**	• Provides guidance on the development and implementation of an ISCM program that: • Supports threat/vulnerability awareness • Provides visibility into organizational assets • Provides effective, measurable security controls

NIST Special Publication (SP)	Description
NIST SP 800-128 **Guide for Security-Focused Configuration Management of Information Systems**	• Addresses how information system components are networked, configured, and managed to provide adequate information security and support an organization's risk management process.
NIST SP 800-53, revision 4 **Security and Privacy Controls for Federal Information Systems and Organizations**	• Provides guidance on security and privacy controls for federal information systems, including selection and customization

DoD Policy and Guidance

As cybersecurity issues continue to arise and evolve into deeper and more complex threats and vulnerabilities, it is important to recognize the key guidance for maintaining secure information systems.

DoD Policy/Guidance	Description
DoDD 5205.16 **The DoD Insider Threat Program**	• Calls for "an integrated capability to monitor and audit information for insider threat detection and mitigation."
DoDD 5240.06 **Counterintelligence Awareness and Reporting**	• Provides guidance on reportable foreign intelligence contracts, activities, indicators, and behaviors related to the requirement for continuous monitoring.
DoDI 8500.01 **Cybersecurity**	• Calls for the implementation of "a multi-tiered cybersecurity risk management process to protect U.S. interests, DoD operational capabilities, and DoD individuals, organizations, and assets." • Requires "operational resilience using automation in support of cybersecurity objectives including …continuous monitoring …"
DoDI 8510.01 **Risk Management Framework (RMF)**	• Calls for "cybersecurity requirements for DoD information technologies will be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37" • Defines continuous monitoring in step 6 of the RMF

DoD Policy/Guidance	Description
CNSSI 1253 **Security Categorization and Control Selection for National Security Systems**	• Provides guidance on control selection within the RMF

Review Activities

Review Activity 1

Which of the following are important roles of the NISP in continuous monitoring?

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

- □ To establish organizational business processes
- □ To ensure that cleared industry safeguards classified information and information systems
- □ To protect critical assets
- □ To thwart foreign adversaries and insider threats to information systems

Review Activity 2

Indicate the policy guidance to which the description applies. For each statement, select the best response. Check your answer in the Answer Key at the end of this Student Guide.

Statement 1 of 3. This guidance requires that all individuals' actions on a classified contractor information system be auditable.

- ○ National Industrial Security Program Operating Manual (NISPOM)
- ○ National Institute of Standards and Technology Special Publication (NIST SP)
- ○ DoD Policy and Guidance

Statement 2 of 3. These policies and guidance establishes the requirement for an integrated and continuous capability to monitor and audit for threats and vulnerabilities from internal and external sources.

- ○ NISPOM
- ○ NIST SP
- ○ DoD Policy and Guidance

Statement 3 of 3. These publications provide detailed guidance on the development and implementation of an ISCM program and security-focused configuration management.

- ○ NISPOM
- ○ NIST SP
- ○ DoD Policy and Guidance

Risk Management Framework (RMF) Overview

Risk and Risk Assessment

Is a “threat” the same as a “vulnerability” to an information system? A threat may be defined as a potential for the accidental or deliberate compromise of security. A weakness or lack of controls that could facilitate, or allow, a compromise is considered a vulnerability. Risk is the possibility that a threat will adversely impact an information system by exploiting a vulnerability. These threats and vulnerabilities are mitigated through the risk assessment process. Risk assessment is the process of analyzing threats and vulnerabilities of an information system and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures.

RMF Purpose and Benefits

Cybersecurity requirements for DoD information technologies are managed through the RMF consistent with the principals established in the NIST SP 800-37, 800-53, 800-53A, and Committee on National Security Systems Instruction (CNSSI) 1253. There are four overarching purposes of the RMF process. The RMF process informs acquisition processes for all DoD IT, including requirements development, procurement, and both developmental T&E (DT&E) and operational T&E (OT&E), but does not replace these processes. The process also implements cybersecurity through the use of security controls and emphasizes continuous monitoring and timely correction of deficiencies. The RMF process adopts reciprocity and codifies reciprocity tenets with procedural guidance.

Term	**Definition**
Reciprocity Tenets	Reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).

RMF Benefits

There are significant benefits that result from enterprise risk management. Integrated risk management ensures traceability and transparency of risk-based decisions. Enterprise risk management ensures organization-wide risk awareness and operational resilience—information resources are trustworthy, missions are ready for information resources degradation or loss, and network operations have the means to prevail in the face of adverse events. Another benefit of enterprise risk management is to ensure operational integration. Cybersecurity is fully integrated into system life cycles and is a visible element of organizational portfolios. Finally, it ensures interoperability through adherence to DoD architecture principles, use of a risk-based approach, and management of the risk inherent in interconnecting systems.

RMF 3-Tiered Approach

The RMF presents a 3-tiered approach to risk management. Tier 1 is the Organization level. It addresses risk from an organization perspective and is influenced by risk decisions made at Tiers 2 and 3. Tier 2 is the mission and business process level. Addressing risk at this level is guided by Tier 1 decisions and informed and influenced by Tier 3 risk decisions. Tier 3, the Information System level, is concerned with the environment of operation and addresses the risks from an information system and platform information technology system perspective. This approach provides for continuous improvement through the feedback loop and communication between the tiers. It ensures traceability and transparency of risk-based decisions as well as organization-wide risk awareness.

RMF 6-Step Process

There are six steps in the RMF process. Step 1 is to categorize the system. Step 2 is to select Security Controls. In Step 3, the security controls are implemented and then, in Step 4 they are assessed. Step 5 is to authorize the information system. Step 6 is to monitor the security controls.

Review Activity

Review Activity 3

Which of the following identify how the RMF supports risk management?

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

- □ The RMF process ensures that business process decisions can override user information system concerns.
- □ The RMF process provides a flexible approach with decision-making at Tier 3.
- □ The RMF process ensures traceability and transparency across all levels of the organization.
- □ The RMF process emphasizes continuous monitoring and timely correction of deficiencies.

Risk Management Roles and Responsibilities

Roles and Responsibilities Overview

Risk Management implementation requires the effort of key professionals at all levels.

CIO

Chief Information Officer

- Designates a Senior Information Security Officer
- Develops and maintains information security policies, procedures, and control techniques to address all applicable requirements
- Ensures an organization-wide information security program is effectively implemented
- Determines the appropriate allocation of resources dedicated to the protection of the information systems supporting the organization's missions and business functions
- Ensures information security considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles

Note: Has inherent U.S. Government authority and is assigned to Government personnel only

SISO

Senior Information Security Officer

- Directs and coordinates the establishment and maintenance of the RMF
- Advises and informs the principal authorizing officials (PAOs) and their representatives (Tier 2)
- Oversees the RMF Technical Advisory Group and the online Knowledge Service
- Heads an office with the mission and resources to assist in ensuring agency compliance with FISMA

Note: Has inherent U.S. Government authority and is assigned to Government personnel only

Risk Executive Function

- Provides strategic guidance to Tiers 2 and 3
- Assess Tier 1 risk
- Authorizes information exchanges and connections for enterprise information systems and other connections

Note: Has inherent U.S. Government authority and is assigned to Government personnel only

Principal Authorizing Officials (PAOs)

- Appointed for each DoD mission area and represent the mission area interests
- As required, issue authorization guidance specific to the MA, consistent with DoD Instruction 8510.01
- Resolve authorization issues within the mission area and work with other PAOs to resolve issues among mission areas
- Designate AOs for mission area IS and PIT systems
- Designate information security architects or IS security engineers for MA segments or systems of systems, as needed

DoD Component CIO

- Responsible for administration of the RMF within the DoD Component cybersecurity program
- Participates in the RMF Technical Advisory Group (TAG)
- Shares the RMF status of assigned ISs and PIT systems
- Enforces training requirements for persons participating in the RMF

DoD Component SISO

- Has authority and responsibility for security controls assessment
- Establishes and manages a coordinated security assessment process for information technologies governed by the DoD Component cybersecurity program
- Advises AOs

AO

Authorizing Official

- Ensures all appropriate RMF tasks are initiated and completed, with appropriate documentation, for assigned systems
- Monitors and tracks overall execution of system-level POA&Ms
- Reviews and approves the security categorizations of information systems
- Reviews and approves system security plans
- Reviews security status reports from continuous monitoring operations; initiates reaccreditation actions
- Promotes reciprocity to the maximum extent possible
- Does NOT delegate authorization decisions

Note: Has inherent U.S. Government authority and is assigned to Government personnel only

AODR

Authorizing Official Designated Representative

- Is appointed by the AO
- Carries out all responsibilities and tasks delegated by the AO, with the exception of making authorization to operate (ATO), ATO with conditions, or denial of authorization to operate (DATO) decisions

ISO

Information System Owner

- In coordination with the information owner (IO), categorizes systems
- Prepares plan of action and milestones to reduce or eliminate vulnerabilities in the information system
- Appoints user representative (UR) for assigned ISs and PIT systems
- Develops, maintains, and tracks security plans
- Conducts and participates in risk assessments

PM/SM

Program manager/system manager

- Appoints ISSM for each assigned IS or PIT system
- Implements RMF for assigned ISs and PIT systems
- Enforces AO authorization decisions for hosted or interconnected ISs and PIT systems
- Ensures each program acquiring an IS or PIT system has an assigned IS security engineer and that they are fully integrated into the systems engineering process.
- Ensures the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system acquisition process
- Implements and assist the ISO in the maintenance and tracking of the security plan for assigned ISs and PIT systems
- Ensures POA&M development, tracking, and resolution
- Ensures periodic reviews, testing, and assessment of assigned ISs and PIT systems are conducted at least annually
- Registers the IS or PIT system in the DoD Component registry

UR

User representative

- Represents operation and functional requirements of user community
- Identifies mission and operational requirements
- Serves as liaison for the user community throughout the system development life cycle

ISSM

Information system security manager

- Supports implementation of RMF
- Maintains and reports system assessment and authorization status and issues
- Provides direction to Information system security officer (ISSO)
- Coordinates with organization’s security manager to ensure issues affecting the organization’s overall security are addressed appropriately

ISSO

Information system security officer

- Assists ISSMs in meeting their duties and responsibilities
- Implements and enforces all IS and PIT system cybersecurity policies and procedures
- Ensures that all users:
  - Have the requisite security clearances and access authorization
  - Are aware of their cybersecurity responsibilities before being granted system access
- In coordination with the ISSM:
  - Initiates protective or corrective measures when a cybersecurity incident or vulnerability is discovered
  - Ensures that a process is in place for authorized users to report all cybersecurity-related events and potential threats and vulnerabilities to the ISSO
  - Ensures that all IS cybersecurity-related documentation is current and accessible to properly authorized individuals

Review Activity

Review Activity 4

Indicate the tier to which the activity description applies. For each statement, select the best response. Check your answer in the Answer Key at the end of this Student Guide.

Statement 1 of 3. Information System Owner (ISO) categorizes systems at this level.

○ Tier 1: Organization
○ Tier 2: Mission/Business Process
○ Tier 3: Information Systems

Statement 2 of 3. The Program Manager/System Manager (PM/SM) enforces authorization decisions at this level.

○ Tier 1: Organization
○ Tier 2: Mission/Business Process
○ Tier 3: Information Systems

Statement 3 of 3. Authorizing Officials (AOs) monitor and track overall execution of system-level POA&Ms. AOs cannot delegate authorization decisions.

○ Tier 1: Organization
○ Tier 2: Mission/Business Process
○ Tier 3: Information Systems

Conclusion

Lesson Summary

You have completed the lesson “Risk Management.”

Answer Key

Review Activity 1

Which of the following are important roles of the NISP in continuous monitoring?

- □ To establish organizational business processes
- ☑ To ensure that cleared industry safeguards classified information and information systems (correct response)
- ☑ To protect critical assets (correct response)
- ☑ To thwart foreign adversaries and insider threats to information systems (correct response)

***Feedback**: The important roles of the NISP in continuous monitoring include ensuring cleared industry safeguards classified information and information systems; protecting critical assets; and thwarting foreign adversaries and insider threats.*

Review Activity 2

Statement 1 of 3. This guidance requires that all individuals' actions on a classified contractor information system be auditable.

- ⦿ National Industrial Security Program Operating Manual (NISPOM) (correct response)
- ○ National Institute of Standards and Technology Special Publication (NIST SP)
- ○ DoD Policy and Guidance

***Feedback**: The NISPOM's Chapter 8-303(c) requires that each user be uniquely identified and that identity must be associated with all auditable actions taken by that individual.*

Statement 2 of 3. These policies and guidance establishes the requirement for an integrated and continuous capability to monitor and audit for threats and vulnerabilities from internal and external sources.

- ○ NISPOM
- ○ NIST SP
- ⦿ DoD Policy and Guidance (correct response)

***Feedback**: DoD Policy and Guidance calls for a multi-tiered cybersecurity risk management process capable of continuous monitoring for insider and foreign adversary threats and vulnerabilities.*

Statement 3 of 3. These publications provide detailed guidance on the development and implementation of an ISCM program and security-focused configuration management.

- ○ NISPOM
- ⊙ NIST SP (correct response)
- ○ DoD Policy and Guidance

Feedback*: DoD Policy and Guidance calls for a multi-tiered cybersecurity risk management process capable of continuous monitoring for insider and foreign adversary threats and vulnerabilities.*

Review Activity 3

Which of the following identify how the RMF supports risk management?

- □ The RMF process ensures that business process decisions can override user information system concerns.
- □ The RMF process provides a flexible approach with decision-making at Tier 3.
- ☑ The RMF process ensures traceability and transparency across all levels of the organization. (correct response)
- ☑ The RMF process emphasizes continuous monitoring and timely correction of deficiencies. (correct response)

Feedback*: The RMF supports risk management by providing a process ensures traceability and transparency across all levels of the organization and emphasizes continuous monitoring and timely correction of deficiencies.*

Review Activity 4

Statement 1 of 3. Information System Owner (ISO) categorizes systems at this level.

- ○ Tier 1: Organization
- ○ Tier 2: Mission/Business Process
- ⊙ Tier 3: Information Systems (correct response)

Feedback*: Performing at the Tier 3 Information Systems level, the ISO categorizes the systems.*

Statement 2 of 3. The Program Manager/System Manager (PM/SM) enforces authorization decisions at this level.

○ Tier 1: Organization
○ Tier 2: Mission/Business Process
◉ Tier 3: Information Systems (correct response)

***Feedback**: Performing at the Tier 3 Information Systems level, the PM/SM enforces authorization decisions.*

Statement 3 of 3. Authorizing Officials (AOs) monitor and track overall execution of system-level POA&Ms. AOs cannot delegate authorization decisions.

○ Tier 1: Organization
○ Tier 2: Mission/Business Process
◉ Tier 3: Information Systems (correct response)

***Feedback**: Performing at the Tier 3 Information Systems level, Authorizing Officials (AOs) monitor and track overall execution of system-level POA&Ms. AOs cannot delegate authorization decisions.*

Student Guide

Continuous Monitoring

Lesson 3: Continuous Monitoring Strategy and Tasks

Contents

Introduction 3

Objectives....3

Information System Continuous Monitoring Overview 3

What is ISCM?....3

ISCM Strategy 3

ISCM – Three Tiered Approach 4

TIER 1 Organization....4

TIER 2 Mission/Business Processes 4

TIER 3 Information Systems....5

ISCM Processes....5

Review Activity....7

Review Activity 1 7

Continuous Monitoring Process and Major Tasks....8

Continuous Monitoring Process Steps 8

Risk Tolerance....8

ISCM Strategy – Tier 1/Tier 2 Inputs and Outputs....9

Available Tools....9

ISCM Strategy – Tier 3 Inputs and Outputs....10

Review Activity....11

Review Activity 2 11

Conclusion 13

Lesson Summary....13

Answer Key 14

Review Activity 1 14

Review Activity 2 15

Introduction

Objectives

Cyber systems and networks are fundamental to all facets of daily life and work, whether you are conducting an ATM transaction, making a flight reservation, or designing an engineering spec on a computer. In this lesson, you will delve into the information system continuous monitoring (ISCM) process as described in the National Institute of Standards and Technology (NIST) Special Publication 800-137. Then you will examine the ISCM tasks.

Here are the learning objectives for this lesson.

- Examine how ISCM supports the three-tiered approach to risk management
- Distinguish how the ISCM strategy supports the three-tiered approach to risk management
- Match the ISCM tasks to the ISCM process

Information System Continuous Monitoring Overview

What is ISCM?

ISCM is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM is a tactic in a larger strategy of organization-wide risk management. It helps to provide situational awareness of the security status of the organization’s systems based on information collected from resources, including people, processes, technology, and the operational environment. It is also based on the capabilities in place to react as the situation changes.

ISCM Strategy

ISCM metrics originating at the information systems tier can be used to assess, respond, and monitor risk across the organization. In order to effectively address ever-increasing security challenges, a well-designed ISCM strategy addresses monitoring and assessment of security controls for effectiveness, security status monitoring, and security status reporting.

Let’s examine the tasks associated with each facet of the strategy.

Configuration management and security control monitoring and assessment tasks include consolidating documentation and supporting materials including methods and procedures. Tasks also include conducting the security assessment and security impact analysis on changes to the system, and submitting the security assessment report (SAR).

Security status monitoring tasks include selecting the security controls and assessment. The assessment frequency is based on drivers from all three tiers.

Security status reporting tasks include updating the System Security Plan (SSP) and the Plan of Action and Milestones (POA&M). The last part of this strategy leg is designed to report weaknesses. The status report describes threats, vulnerabilities, and security control effectiveness for the information systems.

ISCM – Three Tiered Approach

An organization-wide approach to continuous monitoring of information and information system security supports risk-related decision-making at the organization level (Tier 1), the mission/business processes level (Tier 2), and the information systems level (Tier 3).

TIER 1 Organization

At the organization level, risk management activities address high-level information security governance policy as it relates to risk to the organization as a whole, to its core missions, and to its business functions.

While ISCM strategy, policy, and procedures may be developed at any tier, typically, the organization-wide ISCM strategy and associated policy are developed at the organization tier with general procedures for implementation developed at the mission/business processes tier. The criteria for ISCM are defined by the organization’s risk management strategy, including how the organization plans to assess, respond to, and monitor risk, and the oversight required to ensure that the risk management strategy is effective. Security controls, security status, and other metrics defined and monitored by officials at this tier are designed to deliver information necessary to make risk management decisions in support of governance.

TIER 2 Mission/Business Processes

If the organization-wide strategy is developed at the mission/business processes tier, Tier 1 officials review and approve the strategy to ensure that organizational risk tolerance across all missions and business processes has been appropriately considered. This information is communicated to staff at the mission/business processes and information systems tiers. It is reflected in Tier 2 and Tier 3’s strategy, policy, and procedures. The Tier 2 criteria for continuous monitoring of information security are defined by:

- How core mission/business processes are prioritized with respect to the overall goals and objectives of the organization
- Types of information needed to execute the stated mission/business processes successfully
- Organization-wide information security program strategy

Controls in the Program Management (PM) family are an example of Tier 2 security controls. They address the establishment and management of the organization's information security program and establish the minimum frequency with which each security control or metric is to be assessed or monitored.

TIER 3 Information Systems

ISCM activities at Tier 3 address risk management from an information system perspective. Activities include:

- Ensuring that all system-level security controls (technical, operational, and management controls):
  - Are implemented correctly
  - Operate as intended
  - Produce the desired outcome with respect to meeting the security requirements for the system
  - Continue to be effective over time.
- Assessing and monitoring hybrid and common controls implemented at the system level.
  - Security status reporting at this tier often includes but is not limited to:
    - Security alerts
    - Security incidents
    - Identified threat activities.
- Ensuring that security-related information supports the monitoring requirements of other organizational tiers.

ISCM Processes

ISCM supports organizational risk management decisions to include risk response decisions, ongoing system authorization decisions, and POA&M resource and prioritization decisions. ISCM incorporates processes to assure that response actions are taken in accordance with findings and organizational risk tolerances and have the intended effects.

The ISCM users' data needs vary by tier. Careful design of ISCM capabilities provides each user with the data content in the format they need and with the frequency of data collection they require to make effective decisions. System administrators at Tier 3 may be interested in technical details to support system-level actions such as configuration changes. Management officials at Tier 1 may be more interested in aggregated data to enable organization-wide decision making such as, changes in security policies, an increase in resources for security awareness programs, or modifications to the security architecture.

Review Activity

Review Activity 1

Identify the tier that each ISCM strategy statement supports. Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

Statement 1 of 3. ISCM strategy at this level is focused on the controls that address the establishment and management of the organization's information security program, including establishing the minimum frequency with which each security control or metric is to be assessed or monitored.

○ Tier 1
○ Tier 2
○ Tier 3

Statement 2 of 3. ISCM strategy at this level is focused on high-level information security governance policy as it relates to risk to the organization as a whole, to its core missions, and to its business functions.

○ Tier 1
○ Tier 2
○ Tier 3

Statement 3 of 3. ISCM strategy at this level is focused on ensuring that all system-level security controls are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time.

○ Tier 1
○ Tier 2
○ Tier 3

Continuous Monitoring Process and Major Tasks

Continuous Monitoring Process Steps

The process for developing an ISCM strategy and implementing the program is comprised of six steps that map to risk tolerance, adapt to ongoing needs, and actively involve management. Risk tolerance, enterprise architecture, security architecture, security configurations, plans for changes to the enterprise architecture, and available threat information provide data that is fundamental to the execution of these steps and to ongoing management of information security-related risks. Security-related information is analyzed for its relevance to organizational risk management at all three tiers.

Process Step	**Description**
Define	Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
Establish	Establish an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
Implement	Implement an ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.
Analyze/Report	Analyze the data collected and Report findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.
Respond	Respond to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
Review and Update	Review and Update the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization's information infrastructure, and increase organizational resilience.

Risk Tolerance

At the Organization level, the Risk Executive Function determines the overall organizational risk tolerance and risk mitigation strategy. Within the NISP, however, the organizational structure is much different than a government entity. Although these are contractor systems, it is the responsibility of the government to accept the risk associated with their operation. This means the government will be more responsible for the organization. As Tiers 1 and/or 2 develop the policies, procedures, and templates that facilitate organization-wide, standardized processes in support of the ISCM strategy, risk tolerance is part of the equation. Policies and procedures to mitigate risk are fundamental to an effective ISCM strategy:

- Key metrics
- Status monitoring and reporting
- Assessing risk and gaining threat information
- Configuration management and security impact analysis
- Implementation and use of tools
- Monitoring frequencies
- Sample sizes and populations
- Security metrics and data sources

ISCM Strategy – Tier 1/Tier 2 Inputs and Outputs

The primary roles for defining the ISCM strategy are performed by the Risk Executive Function, CIO, SISO, and AOs. The ISO performs a supporting role.

Decisions and activities by Tier 1 and 2 officials may be constrained by things such as mission/business needs, limitations of the infrastructure (including the human components), immutable governance policies, and external drivers. The expected input to the ISCM strategy includes: Organizational risk assessment and current risk tolerance, current threat information, organizational expectations and priorities, available tools. Automated support tools include vulnerability scanning tools and network scanning devices. The expected output is updated information on organizational risk tolerance, organization-wide ISCM strategy and associated policy, procedures, templates, tools.

When implementing policies, procedures, and templates developed at higher tiers, lower tiers fill in any gaps related to their tier-specific processes.

Available Tools

Consideration is given to ISCM tools that pull information from a variety of sources. These sources can include assessment objects such as number and types of tests conducted on source code, number of software modules reviewed, number of network nodes and mobile devices scanned for vulnerabilities, and number of individuals interviewed to check basic understanding of contingency responsibilities. Other considerations in selecting ISCM tools include:

- Use open specifications such as the Security Content Automation Protocol (SCAP)

- Offer interoperability with other products such as help desk, inventory management, configuration management, and incident response solutions;
- Support compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines
- Provide reporting with the ability to tailor output and drill down from high-level, aggregate metrics to system-level metrics
- Allow for data consolidation into Security Information and Event Management (SIEM) tools and dashboard products

ISCM Strategy – Tier 3 Inputs and Outputs

Although the ISCM strategy is defined at Tiers 1 or 2, system-specific policy and procedures for implementation are also developed at Tier 3. Primary Roles at this tier include the ISO and ISSO, supported by the SISO, AO, and Security Control Assessor.

Tier 3 strategy is based on Government provided guidance, such as NIST 800-137 and NISPOM.

Inputs to the Tier 3 ISCM strategy include information from Tiers 1 and 2, such as organizational risk tolerance information and organizational ISCM strategy, policy, procedures, and templates. System-specific threat information and system information such as the System Security Plan, Security Assessment Report, Plan of Action and Milestones, Security Assessment Plan, and System Risk Assessment, are essential inputs as well. System owners establish a system-level strategy for ISCM by considering factors such as the system's architecture and operational environment. ISOs also consider organizational and mission-level requirements as well as drivers from all three tiers to determine assessment frequencies of security controls.

The expected output is a system-level ISCM strategy that complements the Tier 1 and 2 strategies and the organizational security program. This system-level strategy will also provide security status information for all tiers and real-time updates for ongoing system authorization decisions as directed by the organizational ISCM strategy.

Review Activity

Review Activity 2

Identify the step each statement describes. Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

Statement 1 of 4. Given the ISCM process, in this step security-related information required for metrics, assessments, and reporting is collected and, where possible the collection, analysis, and reporting of data is automated.

○ Step 1: Define an ISCM strategy
○ Step 2: Establish an ISCM program
○ Step 3: Implement an ISCM program
○ Step 4: Analyze data and Report findings
○ Step 5: Respond to findings
○ Step 6: Review and Update the monitoring program

Statement 2 of 4. Given the ISCM process, in this step adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization’s information infrastructure, and increase organizational resilience.

○ Step 1: Define an ISCM strategy
○ Step 2: Establish an ISCM program
○ Step 3: Implement an ISCM program
○ Step 4: Analyze data and Report findings
○ Step 5: Respond to findings
○ Step 6: Review and Update the monitoring program

Statement 3 of 4. Given the ISCM process, in this step the metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture are determined.

○ Step 1: Define an ISCM strategy
○ Step 2: Establish an ISCM program
○ Step 3: Implement an ISCM program
○ Step 4: Analyze data and Report findings
○ Step 5: Respond to findings
○ Step 6: Review and Update the monitoring program

Statement 4 of 4. Given the ISCM process, in this step the ISCM strategy is developed based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

○ Step 1: Define an ISCM strategy

○ Step 2: Establish an ISCM program

○ Step 3: Implement an ISCM program

○ Step 4: Analyze data and Report findings

○ Step 5: Respond to findings

○ Step 6: Review and Update the monitoring program

Conclusion

Lesson Summary

You have completed the lesson “Continuous Monitoring Strategy and Tasks.”

Answer Key

Review Activity 1

Statement 1 of 3. ISCM strategy at this level is focused on the controls that address the establishment and management of the organization's information security program, including establishing the minimum frequency with which each security control or metric is to be assessed or monitored.

- ○ Tier 1
- ⦿ Tier 2 (correct response)
- ○ Tier 3

***Feedback**: Tier 2 MISSION/BUSINESS PROCESSES ISCM strategies focus on the controls that address the establishment and management of the organization's information security program, including establishing the minimum frequency with which each security control or metric is to be assessed or monitored.*

Statement 2 of 3. ISCM strategy at this level is focused on high-level information security governance policy as it relates to risk to the organization as a whole, to its core missions, and to its business functions.

- ⦿ Tier 1 (correct response)
- ○ Tier 2
- ○ Tier 3

***Feedback**: Tier 1 ORGANIZATION ISCM strategy focuses on high-level information security governance policy as it relates to risk to the organization as a whole, to its core missions, and to its business functions.*

Statement 3 of 3. ISCM strategy at this level is focused on ensuring that all system-level security controls are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time.

- ○ Tier 1
- ○ Tier 2
- ⦿ Tier 3 (correct response)

***Feedback**: Tier 3 INFORMATION SYSTEMS ISCM strategy focuses on ensuring that all system-level security controls are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time.*

Review Activity 2

Statement 1 of 4. Given the ISCM process, in this step security-related information required for metrics, assessments, and reporting is collected and, where possible the collection, analysis, and reporting of data is automated.

- ○ Step 1: Define an ISCM strategy
- ○ Step 2: Establish an ISCM program
- ⊙ Step 3: Implement an ISCM program (correct response)
- ○ Step 4: Analyze data and Report findings
- ○ Step 5: Respond to findings
- ○ Step 6: Review and Update the monitoring program

Feedback*: In Step 3: Implement and ISCM program, security-related information required for metrics, assessments, and reporting is collected and, where possible the collection, analysis, and reporting of data is automated.*

Statement 2 of 4. Given the ISCM process, in this step adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization’s information infrastructure, and increase organizational resilience.

- ○ Step 1: Define an ISCM strategy
- ○ Step 2: Establish an ISCM program
- ○ Step 3: Implement an ISCM program
- ○ Step 4: Analyze data and Report findings
- ○ Step 5: Respond to findings
- ⊙ Step 6: Review and Update the monitoring program (correct response)

Feedback*: In Step 6: Review and Update the monitoring program adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization’s information infrastructure, and increase organizational resilience.*

Statement 3 of 4. Given the ISCM process, in this step the metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture are determined.

○ Step 1: Define an ISCM strategy

◉ Step 2: Establish an ISCM program (correct response)

○ Step 3: Implement an ISCM program

○ Step 4: Analyze data and Report findings

○ Step 5: Respond to findings

○ Step 6: Review and Update the monitoring program

***Feedback**: In Step 2: Establish an ISCM program the metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture are determined.*

Statement 4 of 4. Given the ISCM process, in this step the ISCM strategy is developed based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

◉ Step 1: Define an ISCM strategy (correct response)

○ Step 2: Establish an ISCM program

○ Step 3: Implement an ISCM program

○ Step 4: Analyze data and Report findings

○ Step 5: Respond to findings

○ Step 6: Review and Update the monitoring program

***Feedback**: In Step 1: Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.*

Student Guide

Continuous Monitoring

Lesson 4: Security Configuration Management

Contents

Introduction 3

Objectives 3

Why Configuration Management Is Needed 3

Configuration Management Overview 3

IS Changes 3

Review Activity 5

Review Activity 1 5

Four Phases of Security Configuration Management 6

What is SecCM? 6

Planning 6

Identifying and Implementing Configurations 7

Controlling Configuration Changes 7

Monitoring 7

CM Policies and Procedures 8

Review Activity 9

Review Activity 2 9

Configuration Management Controls 10

CM Controls for Continuous Monitoring 10

CM Policy and Procedures 10

Baseline Configuration 10

Configuration Change Control 10

Security Impact Analysis (SIA) 11

Access Restrictions for Change 11

Configuration Settings 12
Least Functionality 12
Information System Component Inventory....................12
Configuration Management Plan (CMP) 13
Software Usage Restrictions 13
User-Installed Software 13
Review Activity 15
Review Activity 3 15
Patch Management 17
Why Do We Need Patches? 17
Patch Management and SecCM 17
Review Activity 18
Review Activity 4 18
Conclusion 19
Lesson Summary....................19
Answer Key....................20
Review Activity 1 20
Review Activity 2 20
Review Activity 3 22
Review Activity 4 24

Introduction

Objectives

Changes to an information system’s configuration are often needed to stay up to date with changing business functions and services, and information security needs. These changes can adversely impact the previously established security posture. That’s why effective configuration management is vital to the establishment and maintenance of security for information and information systems.

In this lesson, you will examine how configuration management controls enable continuous monitoring of information systems. Take a moment to review the learning objectives for this lesson.

- Describe how configuration management controls enable continuous monitoring
    - Recognize the role of security-focused configuration management (SecCM) in risk management
    - Differentiate the four phases of security configuration management (SecCM)
    - Identify configuration management controls in support of continuous monitoring
    - Identify the role of the patch management process in security-focused configuration management (SecCM)

Why Configuration Management Is Needed

Configuration Management Overview

Information systems are composed of many interconnected components in multiple ways to meet a variety of business, mission, and information security needs. How these information system (IS) components are networked, configured, and managed is critical in providing adequate information security and supporting an organization’s risk management process. The configuration management (CM) process ensures that the protection features are implemented and maintained on the system. The CM process includes a formal change control process of all security relevant aspects of the IS.

IS Changes

An IS typically is in a constant state of change in response to new, enhanced, corrected, or updated hardware and software capabilities. IS change also occurs when patches for correcting software flaws and other errors to existing components are implemented. New security threats and changing business functions can also require IS changes.

Implementing IS changes almost always results in some adjustment to the system configuration. To ensure that the required adjustments to the system configuration do not adversely affect the security of the information system or the organization from operation of the information system, a well-defined CM process that integrates information security is needed. CM is applied to establish baselines and for tracking, controlling, and management of many aspects of business development and operations (e.g., products, services, manufacturing, business processes, and information technology).

Review Activity

Review Activity 1

Which of the following are security-focused configuration management (SecCM) roles in risk management?

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

- □ Ensuring that adjustments to the system configuration do not adversely affect the security of the information system
- □ Establishing configuration baselines and tracking, controlling, and managing aspects of business development
- □ Ensuring that adjustments to the system configuration do not adversely affect the organization's operations
- □ Establishing a firm schedule for security patch updates every six months

Four Phases of Security Configuration Management

What is SecCM?

Security-focused configuration management (SecCM) is the management and control of configurations for information systems. SecCM enables security and facilitates the management of information security risk.There are four phases in SecCM:

- Planning
- Identifying and Implementing Configurations
- Controlling Configuration Changes
- Monitoring

Planning

The Planning Phase involves developing policy and procedures for the baseline configuration and subsequent configuration changes. Industry is not required to have a formal Change Control Board; however, they must still document their change control process. The policies and procedures include:

- Implementation plans
- Integration into existing security program plans and Configuration Control Boards (CCBs)
- Configuration change control processes
- Tools and technology
- Use of common secure configurations and baseline configurations
- Monitoring
- Metrics for compliance

The Baseline Configuration is the documented, formally reviewed, and approved sets of specifications for information systems or configuration items (CIs) within those systems. It serves as a basis for future builds, releases, and/or changes to information systems. The documentation includes information about information system components, such as the standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices. It specifies current version numbers and patch information on operating systems and applications; and configuration settings/parameters. The baseline configuration details the network topology, and the logical placement of those components within the system architecture. Baseline configurations of information systems reflect the current enterprise architecture. This requires creating new baselines as organizational information systems change over time.

Identifying and Implementing Configurations

After the planning and preparation activities are completed, a secure baseline configuration for the information system is developed, reviewed, approved, and implemented. The approved baseline configuration for an information system and associated components represents the most secure state consistent with operational requirements and constraints. For a typical information system, the secure baseline may address configuration settings, software loads, patch levels, how the information system is physically or logically arranged, how various security controls are implemented, and documentation. Where possible, automation is used to enable interoperability of tools and uniformity of baseline configurations across the information system.

Controlling Configuration Changes

In phase 3, Controlling Configuration Changes, emphasis is put on the management of change to maintain the secure, approved baseline of the information system. Changes are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation. Security Impact Analysis ensures changes have been implemented as approved and determines whether there are any unanticipated effects of the change on existing security controls. In this phase, a variety of access restrictions for change are employed, including:

- Access controls
- Process automation
- Abstract layers
- Change windows
- Verification and audit activities

Monitoring

Monitoring activities in Phase 4 of SecCM are used as the mechanism to validate that the information system is adhering to organizational policies, procedures, and the approved secure baseline configuration. Monitoring identifies undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose organizations to increased risk. SecCM monitoring is done through assessment and reporting activities. Reports address the secure state of individual information system configurations and are used as input to Risk

Management Framework information security continuous monitoring requirements.

CM Policies and Procedures

The System Security Plan (SSP) or your organization’s equivalent of the system security plan, describes the CM procedures and documentation process for changes to any IS hardware, software, and security documentation. The ISSM and/or ISSO are responsible for authorizing all security relevant baseline changes to the applicable ISs profile(s) to include hardware, software, procedures, reports, and audit records.

Local Policies define the security settings associated with user activities conducted within the computer system. Through local policies, activities are recorded on the audit log, user rights are granted, and specific operating system (OS) security parameters are defined. These parameters include digital signatures, guest accounts, secure channel encryption, and access to network resources.

Review Activity

Review Activity 2

Identify the SecCM phase for each activity description. Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

Description 1 of 4. In this phase, a variety of access restrictions for change are employed.

○ Phase 1
○ Phase 2
○ Phase 3
○ Phase 4

Description 2 of 4. In this phase, activities focus on validating the IS adheres to the policies, procedures, and approved baseline configuration.

○ Phase 1
○ Phase 2
○ Phase 3
○ Phase 4

Description 3 of 4. In this phase, activities address configuration settings, software loads, patch levels, how the IS is arranged, and how various security controls are implemented.

○ Phase 1
○ Phase 2
○ Phase 3
○ Phase 4

Description 4 of 4. In this phase, activities involve developing policy and procedures including implementation plans, change control processes, and metrics for compliance, to name a few.

○ Phase 1
○ Phase 2
○ Phase 3
○ Phase 4

Configuration Management Controls

CM Controls for Continuous Monitoring

NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, details CM controls in support of continuous monitoring. Security controls address both security functionality and security assurance.

CM Policy and Procedures

This control addresses:

- Purpose, scope, roles, responsibilities
- Management commitment
- Coordination among organizational entities
- Compliance
- Procedures to facilitate the implementation of CM controls

The organizational risk management strategy is a key factor in establishing policy and procedures.

Baseline Configuration

This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. It includes information about:

- IS components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters)
- Network topology
- Logical component placement within the system architecture

Configuration Change Control

This control involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. It includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Auditing of changes takes place before and after changes are made.

Security Impact Analysis (SIA)

Analyzes changes to the IS to determine potential security impacts prior to change implementation. The analysis may include:

- Reviewing security plans and system design documentation for control implementation and how specific changes might affect the controls
- Assessing the risk of the change to understand the impact
- Determining if additional controls are needed

It is performed by organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers).

Access Restrictions for Change

This control:

- Includes physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).
- Supports auditing of the enforcement actions
- Prevents the installation of software and firmware unless verified with an approved certificate, to include: updates, patches, service packs, device drivers, and basic input output system (BIOS) updates.
- Supports two-person dual authorization
- Limits privileges to change IS components and software within the libraries

Configuration Settings

This control applies to the parameters that can be changed in hardware, software, or firmware components that affect the security posture and/or functionality of the system. Security-related parameters include:

- Registry settings
- Account, file, directory permission settings
- Settings for functions, ports, protocols, services, and remote connections

Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing.

Least Functionality

This control configures the IS to provide only essential capabilities to limit risk. Organizations determine which functions and services are candidates for:

- Elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing)
- Disabling unused or unnecessary physical and logical ports/protocols (e.g., USB, FTP, and HTTP)

The purpose is to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

Information System Component Inventory

This inventory control is for information deemed necessary for effective accountability of IS components, including: hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include: manufacturer, device type, model, serial number, and physical location.

The organization can employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system; and take the following actions when unauthorized components are detected:

- Disable network access by such components
- Isolate the components
- Notify designated personnel

Configuration Management Plan (CMP)

The CMP control details processes and procedures for how CM is used to support system development life cycle activities at the IS level. The plans describe how to:

- Move changes through change management processes
- Update configuration settings and baselines
- Maintain IS component inventories,
- Control development, test, and operational environments,
- Develop, release, and update key documents

Software Usage Restrictions

This control ensures that software use:

- Complies with contract agreements and copyright laws
- Tracks usage
- Is not used for unauthorized distribution, display, performance, or reproduction

The organization can impose restrictions on open source software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.

User-Installed Software

To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation.

Permitted software installations may include, updates and security patches to existing software and downloading applications from organization-approved "app stores."

Prohibited software installations may include software with unknown or suspect pedigrees or software that organizations consider potentially malicious.

Policy enforcement methods include:

- Procedural methods (e.g., periodic examination of user accounts)
- Automated methods (e.g., configuration settings implemented on organizational information systems), or both.
- Control enhancements can include alerts for unauthorized installations and prohibiting installation without privileged status.

Review Activity

Review Activity 3

For each question, select the best response. Check your answer in the Answer Key at the end of this Student Guide.

Question 1 of 4: This control includes physical and logical access controls and prevents the installation of software and firmware unless verified with an approved certificate.

○ Configuration Change Control
○ Access Restrictions for Change
○ Configuration Settings
○ Least Functionality
○ Software Usage Restrictions
○ User-Installed Software

Question 2 of 4: This control ensures that software use complies with contract agreements and copyright laws, tracks usage, and is not used for unauthorized distribution, display, performance, or reproduction.

○ Configuration Change Control
○ Access Restrictions for Change
○ Configuration Settings
○ Least Functionality
○ Software Usage Restrictions
○ User-Installed Software

Question 3 of 4: This control involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications.

○ Configuration Change Control
○ Access Restrictions for Change
○ Configuration Settings
○ Least Functionality
○ Software Usage Restrictions
○ User-Installed Software

Question 4 of 4: This control applies to the parameters that can be changed in hardware, software, or firmware components that affect the security posture and/or functionality of the system, including registry settings, account/directory permission settings, and settings for functions, ports and protocols.

○ Configuration Change Control
○ Access Restrictions for Change
○ Configuration Settings
○ Least Functionality
○ Software Usage Restrictions
○ User-Installed Software

Patch Management

Why Do We Need Patches?

As pointed out on the Alerts page of US-CERT, as many as 85 percent of targeted attacks are preventable! Why? Cyber threat actors continue to exploit unpatched software to conduct attacks against critical infrastructure and organizations.

Patches are prioritized and approved through the configuration change control process. They are tested for their impact on existing secure configurations and integrated into updates to approved baseline configurations. Recall that the Access Restrictions for Change control limits privileges to users with a verified certificate to implement patches.

It is important that IT operations and maintenance staff who support the IS are active participants in the configuration change control process and are aware of their responsibility for following it. If significant business process reengineering is needed, updating a patch management process and training may be required.

Patch Management and SecCM

An organization’s patch management process is important in reducing vulnerabilities in an information system. It is integrated at a number of points within the four SecCM phases, including updating baseline configurations to the current patch level. Patch management in the SecCM Phase 2, includes testing and approving patches as part of the configuration change control process. It also integrates with this phase in performing the Security Impact Analysis to ensure changes have been implemented properly and to determine whether there are any unanticipated effects of the change on existing security controls. Patch management is integral to SecCM Phase 4 in monitoring systems and components for current patch status.

Review Activity

Review Activity 4

Which phase of SecCM is the patch Security Impact Analysis conducted?

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

○ Phase 1: Planning

○ Phase 2: Identifying and Implementing Configurations

○ Phase 3: Controlling Configuration Changes

○ Phase 4: Monitoring

Conclusion

Lesson Summary

You have completed the lesson “Security Configuration Management.”

Answer Key

Review Activity 1

Which of the following are security-focused configuration management (SecCM) roles in risk management?

☑ Ensuring that adjustments to the system configuration do not adversely affect the security of the information system (correct response)

☑ Establishing configuration baselines and tracking, controlling, and managing aspects of business development (correct response)

☑ Ensuring that adjustments to the system configuration do not adversely affect the organization's operations (correct response)

□ Establishing a firm schedule for security patch updates every six months

***Feedback**: SecCM roles in risk management ensure adjustments to the system configuration do not adversely affect the security of the information system or the organization's operations as well as establishing configuration baselines and tracking, controlling, and managing aspects of business development.*

Review Activity 2

Description 1 of 4. In this phase, a variety of access restrictions for change are employed.

○ Phase 1

○ Phase 2

◉ Phase 3 (correct response)

○ Phase 4

***Feedback**: In Phase 3, Controlling Configuration Changes, a variety of access restrictions for change are employed, including: Access controls, process automation, abstract layers, change windows, and verification and audit activities.*

Description 2 of 4. In this phase, activities focus on validating the IS adheres to the policies, procedures, and approved baseline configuration.

○ Phase 1

○ Phase 2

○ Phase 3

◉ Phase 4 (correct response)

Feedback*: In Phase 4, Monitoring, activities focus on validating the IS adheres to the policies, procedures, and approved baseline configuration as well as to identify undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes.*

Description 3 of 4. In this phase, activities address configuration settings, software loads, patch levels, how the IS is arranged, and how various security controls are implemented.

○ Phase 1

◉ Phase 2 (correct response)

○ Phase 3

○ Phase 4

Feedback*: In Phase 2, Identifying and Implementing Configurations, activities address configuration settings, software loads, patch levels, how the IS is arranged, and how various security controls are implemented.*

Description 4 of 4. In this phase, activities involve developing policy and procedures including implementation plans, change control processes, and metrics for compliance, to name a few.

◉ Phase 1 (correct response)

○ Phase 2

○ Phase 3

○ Phase 4

Feedback*: In Phase 1, Planning, activities involve developing policy and procedures including implementation plans, change control processes, and metrics for compliance, to name a few.*

Review Activity 3

Question 1 of 4: This control includes physical and logical access controls and prevents the installation of software and firmware unless verified with an approved certificate.

○ Configuration Change Control

◉ Access Restrictions for Change (correct response)

○ Configuration Settings

○ Least Functionality

○ Software Usage Restrictions

○ User-Installed Software

***Feedback**: The Access Restrictions for Change control includes physical and logical access controls and prevents the installation of software and firmware unless verified with an approved certificate.*

Question 2 of 4: This control ensures that software use complies with contract agreements and copyright laws, tracks usage, and is not used for unauthorized distribution, display, performance, or reproduction.

○ Configuration Change Control

○ Access Restrictions for Change

○ Configuration Settings

○ Least Functionality

◉ Software Usage Restrictions (correct response)

○ User-Installed Software

***Feedback**: The Software Usage Restrictions control ensures that software use complies with contract agreements and copyright laws, tracks usage, and is not used for unauthorized distribution, display, performance, or reproduction.*

Question 3 of 4: This control involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications.

- ⦿ Configuration Change Control (correct response)
- ○ Access Restrictions for Change
- ○ Configuration Settings
- ○ Least Functionality
- ○ Software Usage Restrictions
- ○ User-Installed Software

***Feedback**: The Configuration Change Control involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications.*

Question 4 of 4: This control applies to the parameters that can be changed in hardware, software, or firmware components that affect the security posture and/or functionality of the system, including registry settings, account/directory permission settings, and settings for functions, ports and protocols.

- ○ Configuration Change Control
- ○ Access Restrictions for Change
- ⦿ Configuration Settings (correct response)
- ○ Least Functionality
- ○ Software Usage Restrictions
- ○ User-Installed Software

***Feedback**: The Configuration Settings control applies to the parameters that can be changed in hardware, software, or firmware components that affect the security posture and/or functionality of the system, including registry settings, account/directory permission settings, and settings for functions, ports and protocols.*

Review Activity 4

Which phase of SecCM is the patch Security Impact Analysis conducted?

○ Phase 1: Planning

○ Phase 2: Identifying and Implementing Configurations

⦿ Phase 3: Controlling Configuration Changes (correct response)

○ Phase 4: Monitoring

Feedback*: During Phase 3: Controlling Configuration Changes, the SIA is conducted on patches to ensure proper implementation and to determine whether unanticipated effects occurred.*

Student Guide

Continuous Monitoring

Lesson 5: Auditing and Log Reviews

Contents

Introduction 3

Objectives 3

Audit Capability 3

What Is Security Auditing? 3

Audits – Operational Resilience 3

Operational Resilience 4

Audits Requirements in the NISPOM 4

Audit Log Information 5

Event Logs 5

Application (Program) Events 6

Security-Related Events 6

Setup Events 6

System Events 6

Forwarded Events 6

Security-Relevant Objects 6

Review Activity 7

Review Activity 1 7

Locating the Event Logs – A Practical Exercise 8

Practical Exercise Overview 8

Review Activity 9

Review Activity 2 9

Interpreting Audit Logs 10

Audit Trail Analysis 10

Audit Codes 10
Review Activity 11
Review Activity 3 11
Conclusion 12
Lesson Summary 12
Answer Key 13
Review Activity 1 13
Review Activity 2 13
Review Activity 3 13

Introduction

Objectives

An audit is an independent review and examination of records and activities to assess the adequacy of security controls identified in NIST 800-53. Audits ensure compliance with established policies and operational procedures.

In this lesson, you will examine how audit logs support continuous monitoring. Take a moment to review the objectives.

- Examine how audit logs support continuous monitoring
  - Identify audit requirements
  - Locate the Security Event Log on a computer
  - Define key information provided in an audit trail analysis

Audit Capability

What Is Security Auditing?

Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them. Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. Audit trails, also known as audit logs, can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events (actions that happen on a computer system), intrusion detection, and problem analysis. The audit log runs in a privileged mode, so it can access and supervise all actions from all users.

Audits – Operational Resilience

Audit logs are an important part of continuous monitoring and fundamental to operational resilience. As stated in DoDI 8500.01, Cybersecurity policy on operational resilience, “Attempts made to reconfigure, self-defend, and recover should produce an incident audit trail.”

Audit policy is also established in DoDD 5205.16, The DoD Insider Threat Program. This policy states, “Through an integrated capability to monitor and audit information for insider threat detection and mitigation, the DoD Insider Threat Program will gather, integrate, review, assess, and respond to information derived from counterintelligence, security, cybersecurity, civilian and military personnel management, workplace violence, antiterrorism risk management, law enforcement, the monitoring of user activity on DoD information networks, and other sources as necessary and appropriate to identify, mitigate, and counter insider threats."

Operational Resilience

To ensure operational resilience, the DoD information technology will be planned, developed, tested, implemented, evaluated, and operated to ensure availability anytime, anywhere. From DoDI 8500.01, Cybersecurity:

> 3.b. Operational Resilience. DoD IT will be planned, developed, tested, implemented, evaluated, and operated to ensure that:
>
> (1) Information and services are available to authorized users whenever and wherever required according to mission needs, priorities, and changing roles and responsibilities.
>
> (2) Security posture, from individual device or software object to aggregated systems of systems, is sensed, correlated, and made visible to mission owners, network operators, and to the DoD Information Enterprise consistent with DoDD 8000.01 (Reference (r)).
>
> (3) Whenever possible, technology components (e.g., hardware and software) have the ability to reconfigure, optimize, self-defend, and recover with little or no human intervention. Attempts made to reconfigure, self-defend, and recover should produce an incident audit trail.

Audits Requirements in the NISPOM

The NISPOM Chapter 8, Information System Security, Section 6, Protection Requirements, defines audit requirements.

There are four progressive audit requirements in the NISP to ensure information system security.

Audit 1 requirements include providing the system with the capability to automatically create and maintain an audit trail or log, or an alternative method of accountability for user activities. The contents of audit trails must be protected against unauthorized access, modification, or deletion. It requires an audit trail analysis and reporting of security events at least weekly. Audit records must also be retained for at least one review cycle or as required by the Cognizant Security Agency.

In addition to the Audit 1 requirements, Audit 2 requirements address individual accountability with unique identification and periodic testing of the security posture by the ISSO or ISSM. Audit 3 adds to the previous requirements with scheduled audit analysis and reporting using automated tools.

Finally, in addition to Audit 1, 2, and 3 requirements, the information system must create an audit trail capable of recording changes to user formal access permissions.

Audit Log Information

The audit log allows organization administrators to review the actions performed by members of your organization quickly. It includes details such as who performed the action, what the action was, and when it was performed. The Audit Log records activities by user accounts and is a routine tool for system security. The log provides records of such activities as:

- Unauthorized activity
- Access attempts
- Connections to specific resources
- Modifications to folders, files, and directories
- System events
- Password changes

You can define the activities recorded in the Audit Log in terms of successful or failed attempts at the specific User actions.

Event Logs

Event logs are special files that record significant events on your computer, such as when a user logs on to the computer or when a program encounters an error. Whenever these types of events occur, Windows and other operating systems, or OS, record the event. The Event Viewer tracks information in several different logs including Application (program) events, Security-related events, Setup events, System events, and Forwarded events. Once the system auditing options are set, the event logs will record events that occur on the computer system. An event is defined as an action that elicits a response from the programs, software, and applications residing within the computer system. Event logs can be filtered and should be archived. The filter option within Event Viewer can be used to analyze the event logs.

Note: This information is specific to Windows. Users of other operating systems should refer to their help guide.

Application (Program) Events

Events are classified as error, warning, or information, depending on the severity of the event. An error is a significant problem, such as loss of data. A warning is an event that isn't necessarily significant, but might indicate a possible future problem. An information event describes the successful operation of a program, driver, or service.

Security-Related Events

These events are called audits and are described as successful or failed depending on the event, such as whether a user trying to log on to Windows was successful.

Setup Events

Computers that are configured as domain controllers will have additional logs displayed here.

System Events

System events are logged by Windows and Windows system services, and are classified as error, warning, or information.

Forwarded Events

These events are forwarded to this log by other computers.

Security-Relevant Objects

Security-relevant objects and directories are part of all OSs but are not identified in the same way or may not reside in the same folders/directories. They include OS executables, OS configuration, system management and maintenance executables, audit data and security-relevant software.

Security-relevant software includes, but is not limited to virus protection software and definitions, clearing and sanitization software, and auditing and audit reduction software. It also includes password generators and trusted downloading process software (Hex editors). Security-relevant software also includes maintenance and diagnostic software—that is, software that is capable of verifying system performance and/or configuration, software disconnect routines, and archived audit logs. Security-relevant objects must be protected and audited.

The primary purpose of audits is to promote User accountability. While DoD Component requirements may be different, the following requirements are recommended as a good baseline: conduct Audit Log Reviews weekly and archive Audit Logs for a period of one year or one review cycle. Applicable laws, regulations, and policies may mandate a different period of retention.

Review Activity

Review Activity 1

Which of the following is an audit requirement in the NISP?

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

- □ Audit records limited to user access log-on
- □ Audit Trail creation, protection, and analysis
- □ Individual accountability with capability to record changes to user access permissions
- □ Audit trails limited to network-level activity and applications
- □ Periodic security posture testing

Locating the Event Logs – A Practical Exercise

Practical Exercise Overview

Though more and more critical systems within the DoD are using Linux, and the DoD has released its own secure flavor of the OS, for this exercise, you can find and view the Security Event Log on a computer with Windows 7.

Instructions for finding the security event log in Windows 7:

1. Select the Windows Start button at the lower left of the screen
2. Select Control Panel
3. Select System and Security
4. Select Administrative Tools
5. Double-click Event Viewer
6. Expand the Windows Logs folder in the left pane
7. Select the Security event log
8. Double-click the first event to view the details

Review Activity

Review Activity 2

Which of the following correctly identifies the initial steps to find the security event log on a computer?

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

○ Control Panel > Event Viewer > Security event log

○ Control Panel > System and Security > Administrative Tools

○ System and Security > Security event log > Event Viewer

○ Event Viewer > Security event log > System and Security

Interpreting Audit Logs

Audit Trail Analysis

While your command may have different requirements, the NISPOM specifies the type of information that must be gathered and the standard events that must be audited when using automated auditing on a system. These automated audit trails must include enough information to determine the action, the date and time of the action, the system entity that initiated/completed the action, and the resources involved. They must include changes in user authentication; blocking of a user ID, terminal or access port (and the reason); and denial of access for excessive logon attempts. This information includes successful and unsuccessful logons and logoffs as well as unsuccessful accesses to security-relevant objects and directories. It also includes changes in user authentication, blocking of a user ID, terminal or access port, and the reason. Automated audit trails also provide denial of access for excessive logon attempts information. The NISPOM also requires that the contents of audit trails must be protected against unauthorized access, modification or deletion.

Audit Codes

There are many audit codes to help you interpret what was happening when an event occurred. Depending on your operating system the audit codes may vary. Review the audit codes listed to familiarize yourself with these often seen Windows audit codes.

- 528 logon – successful
- 529-537 - unsuccessful logons
- 538 logoff – successful
- 539 - account lockout
- 567 - permissions error
- 608/609 - User right assigned/removed

Review Activity

Review Activity 3

Which of the following is key information provided in an audit trail analysis?

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

- □ Successful and unsuccessful logons/logoffs
- □ Denial of access for excessive logon attempts
- □ Unsuccessful accesses to security-relevant objects and directories
- □ Changes in user authentication
- □ Blocking of a user ID, terminal or access port (and the reason)

Conclusion

Lesson Summary

You have completed the lesson “Auditing and Log Reviews.”

Answer Key

Review Activity 1

Which of the following is an audit requirement in the NISP?

- □ Audit records limited to user access log-on
- ☑ Audit Trail creation, protection, and analysis (correct response)
- ☑ Individual accountability with capability to record changes to user access permissions (correct response)
- □ Audit trails limited to network-level activity and applications
- ☑ Periodic security posture testing (correct response)

Feedback*: Audit requirements in the NISP include: Audit Trail creation, protection, and analysis; individual accountability with capability to record changes to user access permissions; and periodic security posture testing.*

Review Activity 2

Which of the following correctly identifies the initial steps to find the security event log on a computer?

- ○ Control Panel > Event Viewer > Security event log
- ⦿ Control Panel > System and Security > Administrative Tools (correct response)
- ○ System and Security > Security event log > Event Viewer
- ○ Event Viewer > Security event log > System and Security

Feedback*: The progression to access the security event log is to select the Control Panel, then the System and Security hyperlink, and then the Administrative Tools hyperlink.*

Review Activity 3

Which of the following is key information provided in an audit trail analysis?

- ☑ Successful and unsuccessful logons/logoffs (correct response)
- ☑ Denial of access for excessive logon attempts (correct response)
- ☑ Unsuccessful accesses to security-relevant objects and directories (correct response)
- ☑ Changes in user authentication (correct response)
- ☑ Blocking of a user ID, terminal or access port (and the reason) (correct response)

Feedback*: All of these answer choices are key information for an audit trail analysis.*

Student Guide

Continuous Monitoring

Lesson 6: Counterintelligence and Cybersecurity in Continuous Monitoring

Contents

Introduction 3

Objectives 3

Why Multiple Security Disciplines Are Needed 3

Hardening the DoD Information Enterprise 3

What Threats and Vulnerabilities Does CM Detect? 4

Vulnerabilities and Threats to Investigate 4

Trends – Suspicious Network Activity 5

Review Activities 6

Review Activity 1 6

Review Activity 2 6

Recognizing Possible Insider Threat Activities 7

What Does CM Disclose? 7

Cybersecurity Reciprocity 7

Implementing Information Systems Security Aspects of Configuration Management ... 8

Implement EPPs 8

Use Cryptography 8

Review Activity 9

Review Activity 3 9

Conclusion 10

Lesson Summary 10

Answer Key 11

Review Activity 1 11

Review Activity 2 11
Review Activity 3 12

Introduction

Objectives

Security vulnerabilities and threats are very real in today's complex and interrelated environment. Threats come in many forms and may materialize in different ways. Some threats are found within your office. Others originate within foreign intelligence entities. Electronic threats may be carried out by hackers and cyber criminals. In order to identify these threats and vulnerabilities, counterintelligence and cybersecurity personnel must work with system owners to employ continuous monitoring of information systems and networks.

Lesson 6 describes the importance of multiple security disciplines involved in continuous monitoring. It then identifies insider threat activities and how continuous monitoring ensures operational resilience as well as interoperability and reciprocity as mandated by DoD. The lesson concludes with best practices.

Take a moment to review the learning objectives.

- Examine how counterintelligence and cybersecurity personnel support continuous monitoring
  - Describe the role of counterintelligence and cybersecurity in identifying threats to Government assets
  - Describe continuous monitoring capabilities for detecting threats and mitigating vulnerabilities
  - Recognize how continuous monitoring supports interoperability, operational resilience, and operational reciprocity

Why Multiple Security Disciplines Are Needed

Hardening the DoD Information Enterprise

Monitoring, analysis, and detection activities, including trend and pattern analysis, are performed by multiple disciplines in the Department of Defense. Continuous monitoring ensures detection of unauthorized activity that can include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. Cyberspace defense uses architectures, cybersecurity, intelligence, counterintelligence (CI), other security programs, law enforcement, and other military capabilities to harden the DoD Information Enterprise. Hardening DoD infrastructure ensures it is more resistant to penetration and disruption. It also strengthens the U.S. ability to respond to unauthorized activity and defend DoD information and networks against sophisticated and agile cyber threats. Cyberspace defense methods translate into quick recovery from cyber incidents.

What Threats and Vulnerabilities Does CM Detect?

DSS counterintelligence and cybersecurity personnel support DoD Security Specialists and cleared industry to apply CM for the identification and mitigation of vulnerabilities and threats. While adversaries are interested in anything that will strengthen their advantage - whether it is a military, competitive, or economic advantage - technology assets are the greatest target.

So, what are key vulnerabilities and threats to investigate?

Vulnerabilities and Threats to Investigate

Security functionality that is highly resistant to penetration, tamper, and bypass requires a significant work factor on the part of adversaries to compromise the confidentiality, integrity, or availability of the information system or system components where that functionality is employed. Vulnerabilities and threats that are investigated as part of your continuous monitoring role include:

- Actual or attempted unauthorized access
- Password cracking, key logging, encryption, hacking activities, and account masquerading
- Use of account credentials by unauthorized parties
- Tampering with or introducing unauthorized elements into information systems
- Unauthorized downloads or uploads of sensitive data; unexplained storage of encrypted data
- Unauthorized use of removable media or other transfer devices
- Downloading or installing non-approved computer applications
- Unauthorized email traffic to and from foreign destinations
- Denial of service attacks or suspicious network communications failures
- Data exfiltrated to unauthorized domains
- Unexplained user accounts
- Social engineering, electronic elicitation, email spoofing, or spear phishing

Trends – Suspicious Network Activity

When adversaries are able to collect enough information, they can piece it together and learn things even classified things which have serious consequences to U.S. national security. The DSS CI Directorate produces the *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry* report annually to apprise security professionals of trends from both insider and external threats. A common method of collection indicated in the annual "Trends" is Suspicious Network Activity via cyber intrusion, viruses, malware, backdoor attacks, acquisition of user names and passwords, and similar targeting. Countermeasures to guard against these collection methods include frequent audits, not relying on firewalls to protect against all attacks, reporting intrusion attempts, and requests from unknown sources.

Review Activities

Review Activity 1

Which of the following describe the role of counterintelligence and cybersecurity in identifying threats to DoD assets?

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

- □ Sharing and reporting unauthorized accesses attempts, denial of service attacks, exfiltrated data, and other threats/vulnerabilities in a timely manner
- □ Monitoring and auditing on an annual basis
- □ Conducting trend analysis as part of the monitoring and detection activities
- □ Implementing cyberspace defenses to ensure DoD information systems and networks are resistant to penetration and disruption

Review Activity 2

Which of the following are detectable threats and vulnerabilities that can be captured and mitigated through continuous monitoring (CM) capabilities?

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

- □ Unexplained storage of encrypted data
- □ Use of account credentials by unauthorized parties
- □ Hacked personal mobile phone directory
- □ Downloading or installing non-approved computer applications

Recognizing Possible Insider Threat Activities

What Does CM Disclose?

Audits and monitoring of information systems may disclose anomalous behaviors which may indicate potential insider threats. Some of these activities may include evidence of logging onto a system at strange hours or working hours inconsistent with job assignment. Printing or downloading of files without permissions or excessively even with permissions could be an indicative of insider threat activity. Attempts to gain access to unauthorized files or the removal of classification markings on documents also pose an insider threat. Finally, transmission of information to foreign IP addresses, unreported foreign contacts, and contact with a known or suspected intelligence officer also send up red flags. As a key component of the risk management framework, CM ensures operational resilience whereby information resources are trustworthy, missions are ready for information resources degradation or loss, and network operations have the means to prevail in the face of adverse events.

Cybersecurity Reciprocity

DoD mandates a continuous monitoring capability that provides cohesive collection, transmission, storage, aggregation, and presentation of data that conveys current operational status, including intrusions and illicit insider access, to affected DoD stakeholders. DoD Components must use the common continuous monitoring framework, lexicon, and workflow as specified in NIST SP 800-137. Integration and interoperability of DoD IT is managed to minimize shared risk by ensuring that the security posture of one system is not undermined by vulnerabilities of interconnected systems. Cybersecurity products, such as firewalls, file integrity checkers, virus scanners, intrusion detection systems, and anti-malware software, should operate in a net-centric manner to enhance the exchange of data and shared security policies.

Effective cybersecurity depends on three conditions implemented across DoD: organization direction, a culture of accountability, and insight and oversight. This includes measuring, reviewing, verifying, monitoring, facilitating, and remediating to ensure coordinated and consistent cybersecurity implementation and reporting across all organizations without impeding local missions. The DoD CIO in partnership with the DoD Components define, collect, and report on strategic cybersecurity metrics.

In turn, integration and interoperability lead to cybersecurity reciprocity. This reciprocity ensures that the security posture of an IS or platform information technology system is available. An authorizing official from another organization can use that evidence to make credible, risk-based decisions regarding the acceptance and use of that system or the information it processes, stores, or transmits.

Implementing Information Systems Security Aspects of Configuration Management

Although there is no one-size-fits-all approach to SecCM, there are practices that organizations can consider when developing and deploying secure configurations. These practices can serve to detect and deter possible insider threat activities. The NIST SP 800-128, Appendix F, provides a list of best practices to reduce and decrease risks to information systems and information technology. These include:

- Use Common Secure Configurations for Settings
- Centralize Policy and Common Secure Configurations for Configuration Settings
- Tailor Secure Configurations according to System/Component Function and Role
- Eliminate Unnecessary Ports, Services, and Protocols (Least Functionality)
- Limit the Use of Remote Connections
- Develop Strong Password Policies
- Develop a Patch Management Process
- Implement EPPs
- Use Cryptography

Implement EPPs

Endpoint Protection Platforms include:

- Anti-malware
- System Firewalls
- Host-based Intrusion Detection and Prevention System (IDPS)
- Restrict the use of mobile code

Use Cryptography

Through algorithms, secure information delivery is ensured anywhere on the Global Information Grid (GIG), assuring confidentiality, integrity, and availability by enabling ISs to use PKI for authentication, digital signatures, and encryption. DoDI 8500.01 mandates, “DoD will public key-enable DoD ISs and implement a DoD-wide Public Key Infrastructure (PKI) solution.”

Review Activity

Review Activity 3

Which of the following is an example of how continuous monitoring (CM) supports operational resilience, interoperability, and operational reciprocity?

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

□ Recommendation based on monitoring and analysis to move to an unlimited remote connection usage policy

□ Detection of transmitted information to foreign IP addresses

□ Monitoring the collection, transmission, storage, aggregation, and presentation of data that conveys current operational status

□ Recommendation based on monitoring and analysis to move to an opt-out policy on the Public Key Infrastructure (PKI) solution

□ Collection and reporting on strategic cybersecurity metrics

□ Analysis of cybersecurity products (e.g., firewalls, intrusion detection systems) that operate in a net-centric manner

Conclusion

Lesson Summary

You have completed the lesson "Counterintelligence and Cybersecurity in Continuous Monitoring."

Answer Key

Review Activity 1

Which of the following describe the role of counterintelligence and cybersecurity in identifying threats to DoD assets?

☑ Sharing and reporting unauthorized accesses attempts, denial of service attacks, exfiltrated data, and other threats/vulnerabilities in a timely manner (correct response)

□ Monitoring and auditing on an annual basis

☑ Conducting trend analysis as part of the monitoring and detection activities (correct response)

☑ Implementing cyberspace defenses to ensure DoD information systems and networks are resistant to penetration and disruption (correct response)

***Feedback**: Counterintelligence and cybersecurity go hand-in-hand to protect DoD assets by: Sharing and reporting unauthorized accesses attempts, denial of service attacks, exfiltrated data, and other threats/vulnerabilities in a timely manner; Conducting trend analysis as part of the monitoring and detection activities; and Implementing cyberspace defenses to ensure DoD information systems and networks are resistant to penetration and disruption.*

Review Activity 2

Which of the following are detectable threats and vulnerabilities that can be captured and mitigated through continuous monitoring (CM) capabilities?

☑ Unexplained storage of encrypted data (correct response)

☑ Use of account credentials by unauthorized parties (correct response)

□ Hacked personal mobile phone directory

☑ Downloading or installing non-approved computer applications (correct response)

***Feedback**: Through CM capabilities the following would be investigated and analyzed: Unexplained storage of encrypted data; Use of account credentials by unauthorized parties; and Downloading or installing non-approved computer applications.*

Review Activity 3

Which of the following is an example of how continuous monitoring (CM) supports operational resilience, interoperability, and operational reciprocity?

- □ Recommendation based on monitoring and analysis to move to an unlimited remote connection usage policy
- ☑ Detection of transmitted information to foreign IP addresses (correct response)
- ☑ Monitoring the collection, transmission, storage, aggregation, and presentation of data that conveys current operational status (correct response)
- □ Recommendation based on monitoring and analysis to move to an opt-out policy on the Public Key Infrastructure (PKI) solution
- ☑ Collection and reporting on strategic cybersecurity metrics (correct response)
- ☑ Analysis of cybersecurity products (e.g., firewalls, intrusion detection systems) that operate in a net-centric manner (correct response)

Feedback*: CM supports operational resilience, interoperability, and operational reciprocity in the following ways: Detection of transmitted information to foreign IP addresses; Monitoring the collection, transmission, storage, aggregation, and presentation of data that conveys current operational status; Collection and reporting on strategic cybersecurity metrics; and Analysis of cybersecurity products (e.g., firewalls, intrusion detection systems) that operate in a net-centric manner.*

Student Guide

Continuous Monitoring

Lesson 7: Course Conclusion

Contents

Course Conclusion 2

Course Summary 2

Lesson Review 2

Course Objectives 2

Course Conclusion

Course Summary

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. In this course, you learned about the role of CM in risk management as it supports the organization, the mission/business process, and the information system. Next, you examined how the information system continuous monitoring process and its tasks support the 3-tiered approach to risk management. You then delved deeper into security-focused configuration management and the CM controls, including patch management. You discovered in the Auditing and Log Reviews the importance of audit trails as a CM activity and then found the event logs in a practical exercise. Finally, you learned about the importance of multiple security disciplines involved in CM and how CM ensures operational resilience, interoperability, and operational reciprocity.

Lesson Review

Here is a list of the lessons in the course.

- Lesson 1: Course Introduction
- Lesson 2: Risk Management
- Lesson 3: Continuous Monitoring Strategy and Tasks
- Lesson 4: Security Configuration Management
- Lesson 5: Auditing and Log Reviews
- Lesson 6: Counterintelligence and Cybersecurity in Continuous Monitoring
- Lesson 7: Course Conclusion

Course Objectives

Congratulations. You have completed the *Continuous Monitoring* course.

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

- Identify the role of continuous monitoring through risk management
- Examine how ISCM supports the three-tiered approach to risk management
- Describe how configuration management controls enable continuous monitoring
- Examine how audit logs support continuous monitoring
- Examine how counterintelligence and cybersecurity personnel support continuous monitoring

To receive course credit, you must take the *Continuous Monitoring* 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.

Glossary

Course: Continuous Monitoring

Authorization to Operate (ATO): The official management decision given 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 based on the implementation of an agreed-upon set of security controls.

Authorizing Official (AO): A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations, (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Center for Development of Security Excellence (CDSE): The Center for Development of Security Excellence is responsible for providing security education and training to DoD and other U.S. Government personnel, DoD contractors, and sponsored representatives of foreign governments.

Chief Information Officer (CIO): The CIO leads the organization's Information Security Continuous Monitoring (ISCM) program. The CIO ensures that an effective ISCM program is established and implemented for the organization by establishing expectations and requirements for the organization's ISCM program; working closely with authorizing officials to provide funding, personnel, and other resources to support ISCM; and maintaining high-level communications and working group relationships among organizational entities.

Cognizant Security Agency (CSA): Agencies of the Executive Branch that have been authorized to establish an industrial security program to safeguard classified information when disclosed or released to U.S. Industry.

Configuration Item (CI): Items under a configuration management system.

Configuration Management Plan (CMP): Control details processes and procedures for how Configuration Management is used to support system development life cycle activities at the IS level.

Counterintelligence (CI): Defense Security Service (DSS) CI identifies threats to U.S. technology and programs resident in cleared industry and articulates that threat to stakeholders.

Defense Security Service (DSS): The Defense Security Service (DSS) is an agency of the Department of Defense (DoD) located in Quantico, Virginia with field offices throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction, and control over DSS. DSS provides the military services, DoD Agencies, 30 federal agencies, and approximately 13,500 cleared contractor facilities with security support services. DSS is the Cognizant Security Office for most DoD classified contracts.

DSS supports the National Security and the warfighter, secures the nation's technological base, and oversees the protection of U. S. and foreign classified information in the hands of industry. DSS accomplishes this mission by clearing industrial facilities, accrediting information systems, facilitating the personnel security clearance process, delivering security education and training, and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.

Developmental Test & Evaluation (DT&E): Testing that verifies that the system's design is satisfactory and that all technical specifications and contract requirements have been met.

Endpoint Protection Platforms (EPPs): Single endpoint solution that delivers antivirus, anti-spyware, personal firewall, application control, and other styles of host intrusion prevention.

Facility Security Officer (FSO): A U.S. citizen employee, appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other federal requirements for classified information.

Global Information Grid (GIG): Globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Information Owner (IO): Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security (IS): The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Continuous Monitoring (ISCM): Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Information System Owner (ISO): Establishes processes and procedures in support of system-level implementation of the organization's ISCM program. This includes developing and documenting an ISCM strategy for the information system; participating in the organization's configuration management process; establishing and maintaining an inventory of components associated with the information system; conducting security impact analyses on changes to the information system; conducting, or ensuring conduct of, assessment of security controls according to the ISCM strategy; preparing and submitting security status reports in accordance with organizational policy and procedures; conducting remediation activities as necessary to maintain system authorization; revising the system-level security control monitoring process as required; reviewing ISCM reports from common control providers to verify that the common controls continue to provide adequate protection for the information system; and updating critical security documents based on the results of ISCM.

Information System Security Manager (ISSM): An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information systems.

Information System Security Officer (ISSO): ISSOs may be appointed by the ISSM in facilities with multiple accredited information systems. The ISSM will determine the responsibilities to be assigned to the ISSO in accordance with NISPOM Chapter 8.

Information System Security Professional (ISSP): Representative from the Office of Designated Approving Authority (ODAA) that provides advice and assistance visits to improve the security posture with regard to Information Systems and helps facilitate the process of getting your information systems accredited to process classified information.

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Interim Authority to Operate (IATO): Temporary authorization granted for an information system to process information based on preliminary results of a security evaluation of the system.

Intrusion Detection and Prevention System (IDPS): Systems primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Master System Security Plan (MSSP): Contains specific information to support a self-certification decision.

National Industrial Security Program (NISP): The National Industrial Security Program (NISP) was established by Executive Order 12829 for the protection of classified information released or disclosed to industry in connection with classified contracts. The NISP applies standards for the protection of classified information released or disclosed to contractors of all federal executive branch departments and agencies. Requirements of the NISP are stated in the National Industrial Security Program Operating Manual (NISPOM), (DoD 5220.22-M).

National Industrial Security Program Operating Manual (NISPOM): DoD Manual 5220.22-M issued in accordance with the NISP that prescribes the requirements, restrictions, and other safeguards for government contractors to prevent unauthorized disclosure of classified information.

National Institute of Standards and Technology (NIST): The federal technology agency that works with industry to develop and apply technology, measurements, and standards.

National Institute of Standards and Technology Special Publication (NIST SP): These publications provide guidelines for applying the Risk Management Framework and the development and implementation of an ISCM program that mitigates the threats and vulnerabilities to information systems.

Office of Designated Approving Authority (ODAA): Office within DSS that facilitates the certification and accreditations process for information systems at cleared contractor facilities.

Operating System (OS): A program that is loaded into the computer by a boot program that directs a computer's operations, controlling and scheduling the execution of other programs, and managing storage, input/output, and communication resources.

Operational Test & Evaluation (OT&E): Follows DT&E and validates that the system under test can effectively execute its mission in a realistic operational environment when operated by typical operators against representative threats. The difference between DT&E and OT&E is that DT&E verifies that the system is built correctly in accordance with the specification and contract, and OT&E validates that the system can successfully accomplish its mission is a realistic operational environment.

Plan of Action and Milestone (POA&M): A document that reports progress on items in SSP, identifies vulnerabilities, and addresses action to reduce, eliminate, or accept those vulnerabilities.

Platform Information Technology (PIT) Systems: A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Principal Authorizing Official (PAO): Senior official with authority and responsibility for all systems within an agency.

Protection Level 1 (PL-1): An indication of the implicit level of trust that is placed in a system's technical capabilities and is based on the classification and sensitivity of information, clearances, formal access approvals, and the need-to-know. PL-1 indicates that all users are cleared, all users have access, and all users have a need to know.

Public Key Infrastructure (PKI): The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of PK certificates.

Risk Management Framework (RMF): A common information security framework developed to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies.

Security Assessment Report (SAR): A report containing the assessment and characterization of the aggregate level of the risk to the system, based on the determined risk level for each non-compliant security control.

Security-focused Configuration Management (SecCM): The management and control of configurations for information systems.

Security Impact Analysis: Analysis performed by organizational personnel with information security responsibilities to analyze changes to the IS to determine potential security impacts prior to change implementation.

Security Training Education and Professionalization Portal (STEPP): The learning management system used by the Center for Development of Security Excellence (CDSE). STEPP is where the list of courses is maintained and where student information and course transcripts are maintained.

Senior Information Security Officer (SISO): Establishes, implements, and maintains the organization's ISCM program; develops organizational program guidance (i.e., policies/procedures) for continuous monitoring of the security program and information systems; develops configuration management guidance for the organization; consolidates and analyzes POA&Ms to determine organizational security weaknesses and deficiencies; acquires or develops and maintains automated tools to support ISCM and ongoing authorizations; provides training on the organization's ISCM program and process; and provides support to information owners/information system owners and common control providers on how to implement ISCM for their information systems.

System Security Plan (SSP): A formal agreement that specifies the security requirements, describes security controls, and contains security-related documents (e.g., risk assessment, contingency plan, incident response plan, interconnection agreements).