Continuous Monitoring
Student Guide

May 2024

Center for Development of Security Excellence

Lesson 1: Course Introduction

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 Information Security Continuous Monitoring (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

Lesson 2: Risk Management

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 U.S. critical assets. These are systems and assets so vital to the United States 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 (RMF) 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 U.S. government.

The National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry safeguards classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. 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 32 Code of Federal Regulations Part 117, National Industrial Security Program Operating Manual (NISPOM) rule, 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 rule 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 rule 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 Rule

The NISPOM rule (32 CFR Part 117) prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The rule implements policy, assigns responsibilities, establishes requirements, and provides procedures consistent with:

- Executive Order 12829, "National Industrial Security Program"
- Executive Order 10865, "Safeguarding Classified Information within Industry"
- 32 Code of Regulation Part 2004," National Industrial Security Program"

That guidance outlines the protection of classified information that is disclosed to, or developed by, contractors of the U.S. Government.

The NISPOM rule provides detailed industrial security policy and operating instructions for contractors. 32 CFR Part 117.18, Information System Security, delineates the responsibilities, common requirements, protection measures and requirements for classified systems.

- **117.18(a)(1)** Contractor information systems that are used to capture, create, store, process, or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information. The contractor will implement protective measures using a risk-based approach that incorporates minimum standards for their insider threat program in accordance with CSA-provided guidance.
- **117.18(b)(6)** Change control processes to accommodate configuration management and to identify security relevant changes that may require re-authorization of the information system.
- **117.18(c)(2)** Contractors that are or will be processing classified information on an information system will appoint an employee ISSM.
- **117.18(c)(3)** The ISSM may assign an ISSO.

- **117.18(c)(4)** All information system users will be accountable for their actions.
- **117.18(d)(e)** Keeping contractor management informed to facilitate risk management decisions.

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, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- 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, Revision 5, Security and Privacy Controls for Information Systems and Organizations

These NIST SPs were published in accordance with the provisions of the Federal Information Security Modernization 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 2 **Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy**	• 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: o Supports threat/vulnerability awareness o Provides visibility into organizational assets o Provides effective, measurable security controls
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 5 **Security and Privacy Controls for 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 (CIAR)**	• 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, Rev 2." • Defines continuous monitoring in the RMF
CNSSI 1253 **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 implements policy, assigns responsibilities, establishes requirements, and provides procedures for the protection of classified information that is disclosed to, or developed by, contractors of the U.S. Government.

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

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

- ○ NISPOM Rule
- ○ NIST SP
- ○ DOD Policy and Guidance

Statement 3 of 3. These publications provide detailed guidance on the development and implementation of an Information System Continuous Monitoring (ISCM) program and security-focused configuration management.

- ○ NISPOM Rule
- ○ 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 Revision 2, 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 systems, including requirements development, procurement, and both developmental test and evaluation T&E (DT&E), operational T&E (OT&E), and sustainment; 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. Risk management at Tier 1 addresses risk across the entire organization and informs Tiers 2 and 3 of risk context and risk decisions made at Tier 1.

Tier 2 is the mission and business process level. Tier 2 addresses risk from a mission/business process perspective and is informed by risk context, risk decisions, and risk activities at Tier 1.

Tier 3, the Information System level, addresses risk from an information system and platform information technology system perspective and is guided by the risk context, decisions, and activities at Tiers 1 and 2.

Security-related information is obtained and acted on at Tier 3 and is communicated to Tiers 1 and 2 to be incorporated into organization-wide and mission/business process risk determinations. The ISCM program assessment verifies the flow of information between Tiers. It ensures traceability and transparency of risk-based decisions as well as organization-wide risk awareness.

RMF 7-Step Process

There are seven steps in the RMF process:

- Prepare
- Categorize System
- Select Security Controls
- Implement Security Controls
- Assess Security Controls
- Authorize System
- Monitor 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

The chief information officer is an organizational official responsible for designating a senior agency information security officer; developing and maintaining security policies, procedures, and control techniques to address security requirements; overseeing personnel with significant responsibilities for security and ensuring that the personnel are adequately trained; assisting senior organizational officials concerning their security responsibilities; and reporting to the head of the agency on the effectiveness of the organization's security program, including progress of remedial actions. The chief information officer, with the support of the senior accountable official for risk management, the risk executive (function), and the senior agency information security officer, works closely with authorizing officials and their designated representatives to help ensure that:

- An organization-wide security program is effectively implemented resulting in adequate security for all organizational systems and environments of operation.
- Security and privacy (including supply chain) risk management considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, the SDLC, and acquisitions.
- Organizational systems and common controls are covered by approved system security plans and possess current authorizations.
- Security activities required across the organization are accomplished in an efficient, cost effective, and timely manner.
- There is centralized reporting of security activities.

Senior Agency Information Security Officer

The senior agency information security officer is an organizational official responsible for carrying out the chief information officer security responsibilities under FISMA and serving as the primary liaison for the chief information officer to the organization's authorizing officials, system owners, common control providers, and system security officers. The senior agency information security officer is also responsible for coordinating with the senior agency official for privacy to ensure coordination between privacy and information security programs. The senior agency information security officer possesses the professional qualifications, including training and experience, required to administer security program functions; maintains security duties as a primary responsibility; and heads an office with the specific mission and resources to assist the organization in achieving trustworthy, secure information and systems in accordance with the requirements in FISMA. The senior agency information security officer may serve as authorizing official designated representative or as a security control assessor. The role of senior agency information security officer is an inherent U.S. Government function and is therefore assigned to

government personnel only. Organizations may also refer to the senior agency information security officer as the senior information security officer or chief information security officer.

Risk Executive (Function)

The risk executive (function) is an individual or group within an organization that provides a comprehensive, organization-wide approach to risk management.

The risk executive (function) ensures that risk considerations for systems (including authorization decisions for those systems and the common controls inherited by those systems), are viewed from an organization-wide perspective regarding the organization's strategic goals and objectives in carrying out its core missions and business functions. The risk executive (function) ensures that managing risk is consistent throughout the organization, reflects organizational risk tolerance, and is considered along with other types of risk to ensure mission/business success.

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 Platform Information Technology (PIT)i systems
- Designate information security architects or IS security engineers for MA segments or systems of systems, as needed

DOD Component Chief Information Officer (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 Senior Information Security Officer 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 Plan of Action and Milestones 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
- Has the authority to formally assume responsibility and accountability for operating a system
- Provides common controls inherited by organizational systems
- Has a level of authority commensurate with understanding and accepting such security and privacy risks
- Approves plans, memorandums of agreement or understanding, plans of action and milestones, and determines whether significant changes in the information systems or environments of operation require reauthorization

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

AODR

Authorizing Official Designated Representative

- Is designated by the AO

- Empowered to act on behalf of the AO to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations

The only activity that cannot be delegated by the authorizing official to the designated representative is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk).

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

System User

The system user is an individual or (system) process acting on behalf of an individual that is authorized to access information and information systems to perform assigned duties. System user responsibilities include, but are not limited to, adhering to organizational policies that govern acceptable use of organizational systems; using the organization-provided information technology resources for defined purposes only; and reporting anomalous or suspicious system behavior.

ISSM

Information system security manager

- Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures.
- Ensure that information owners and stewards associated with DOD information received, processed, stored, displayed, or transmitted on each DOD IS and PIT system are identified in order to establish accountability, access approvals, and special handling requirements.
- Maintain a repository for all organizational or system-level cybersecurity-related documentation.

- Ensure that Information Systems Security Officers (ISSOs) are appointed in writing and provide oversight to ensure that they are following established cybersecurity policies and procedures.
- Monitor compliance with cybersecurity policy, as appropriate, and review the results of such monitoring.
- Ensure that cybersecurity inspections, tests, and reviews are synchronized and coordinated with affected parties and organizations.
- Ensure implementation of IS security measures and procedures.
- Ensure that the handling of possible or actual data spills of classified information resident in ISs, are conducted in accordance with policy.
- Act as the primary cybersecurity technical advisor to the AO for DOD IS and PIT systems under their purview.
- Ensure that cybersecurity-related events or configuration changes that may impact DOD IS and PIT systems authorization or security posture are formally reported to the AO and other affected parties.
- Ensure the secure configuration and approval of IT below the system level in accordance with applicable guidance prior to acceptance into or connection to a DOD IS or PIT system.

ISSO

Information system security officer

- Assist the ISSMs in meeting their duties and responsibilities.
- Implement and enforce all DOD IS and PIT system cybersecurity policies and procedures, as defined by cybersecurity-related documentation.
- Ensure that all users have the requisite security clearances and access authorization and are aware of their cybersecurity responsibilities for DOD IS and PIT systems under their purview before being granted access to those systems.
- In coordination with the ISSM, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered and ensure that a process is in place for authorized users to report all cybersecurity-related events and potential threats and vulnerabilities to the ISSO.

- Ensure that all DOD 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 DOD Component SISO has authority and responsibility for security controls assessment 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

Lesson 3: Continuous Monitoring Strategy and Tasks

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 an organization-wide risk management first, and then a system-level responsibility. It also includes mission and business processes. ISCM encompasses all of the people, policies, processes, technologies, and standards that are used to perform the continuous monitoring function. It is an enabling process that supports or provides organizational sustainment in the face of cybersecurity threats and risks.

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 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.

Term	Definition
SSP	System Security Plan - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
POA&M	Plan of Action and Milestones - Reports progress on items in SSP, identifies weaknesses, resources, milestones and completion dates, and evaluates response and mitigation actions.

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. Tier 1 addresses risk from an organizational perspective by establishing and implementing governance structures that are consistent with the strategic goals and objectives of organizations and the requirements defined by federal laws, directives, policies, regulations, standards, and missions/business functions. 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. Tier 2 addresses risk from a mission/business process perspective by designing, developing, and implementing

mission/business processes that support the missions/business functions defined at Tier 1. 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. The risk management activities at Tier 3 reflect the organization's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual systems supporting the mission/business functions of organizations. These 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 user 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, Senior Agency Information Security Officer, 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. Metrics determined through ISCM provide

important information about the security posture across the organization and relative to individual systems and inform the risk management process.

- 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 Senior Agency Information Security Officer, 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.

ISCM Program Assessment

As you learned earlier in this course, the NIST SP 800-137 provides guidance on the development and implementation of an ISCM program. To assess the effectiveness of an ISCM program, NIST provides guidance in the NIST SP 800-137A, Assessing ISCM Programs: Developing an ISCM Program Assessment. NIST SP 800-137A offers an overall process for ISCM program assessment, including the use an organization should get from conducting an assessment, the steps involved, and the elements of an assessment.

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

Lesson 4: Security Configuration Management

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.

Here are the lesson objectives.

- 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 (for example, products, services, manufacturing, business processes, and information technology).

NIST Special Publication 800-137A provides a three-step traceability chain to focus system CM on security. First, there should be an organization-wide policy. Next, there should be procedures for security focused CM. Finally, those procedures must be followed.

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

A Baseline Configuration is a set of specifications for a system, or configuration items (CI), within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. 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. Impact Analyses ensure 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 (e.g., privileged access and what type of change is permitted)
- 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. It also facilitates situational awareness and documents deviations. All of these, 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 with the assistance of the ISSO, if designated, are responsible for authorizing all security relevant baseline changes to the applicable ISs profile(s) to include hardware, software, procedures, reports, and audit records.

The ISSO supports the organization's ISCM program by assisting the ISO in completing ISCM responsibilities and by participating in the configuration management process.

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 5, Security and Privacy Controls for Information Systems and Organizations, details CM controls in support of continuous monitoring of information systems and organizations. This continuous monitoring determines the ongoing effectiveness of controls, changes in information systems and environments of operation, and the state of security and privacy organization wide.

Security controls address both security functionality and security assurance. CM controls supporting continuous monitoring include:

- CM-1 Policy and Procedures
- CM-2 Baseline Configuration
- CM-3 Configuration Change Control
- CM-4 Impact Analyses
- CM-5 Access Restrictions for Change
- CM-6 Configuration Settings
- CM-7 Least Functionality
- CM-8 System Component Inventory
- CM-9 Configuration Management Plan (CMP)
- CM-10 Software Usage Restrictions
- CM-11 User-Installed Software
- CM-12 Information Location
- CM-13 Data Action Mapping
- CM-14 Signed Components

CM-1 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

It is consistent with:

- Applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
- Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls

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

CM-2 Baseline Configuration

This control establishes baseline configurations for operational 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)
- It serves as a basis for future builds, releases, or changes to systems and includes:
  - Security and privacy control implementations
  - Operational procedures
  - Information about system components
  - Network topology
  - Logical placement of components in the system architecture

CM-3 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. The Configuration Control Board (CCB) is the establishment of—and charter for—a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational lifecycle of products and systems. This may also be referred to as a change control board.

The Configuration Change Control includes changes to baseline configurations for components and configuration items of information systems, operational procedures, changes to configuration settings for system components, remediate vulnerabilities, unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Auditing of changes takes place before and after changes are made.

CM-4 Impact Analyses

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).

CM-5 Access Restrictions for Change

This control:

- Defines, documents, approves and enforces physical and logical access restrictions associated with changes to the system
- Includes physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes implemented into external interfaces rather than directly into systems), and change windows (e.g., changes occur only during specified times)
- Supports auditing of the enforcement actions
- Only qualified and authorized individuals are permitted to initiate changes in the system

CM-6 Configuration Settings

This control applies to the parameters that can be changed in hardware, software, or firmware components that affect the security and privacy posture 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
- Configuration settings: mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications
- Privacy parameters (impact privacy posture of systems) include settings for access controls, data processing preferences, and processing and retention permissions

Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

CM-7 Least Functionality

This control configures the system to provide only organization-defined mission essential capabilities to limit risk. Prohibit or restrict the use of Ports, Protocols, and Services Management (PPSM). PPSM standardizes procedures to catalog, regulate, and control the use and management of protocols in the Internet protocol suite, and associated ports (also known as protocols, data services, and associated ports or ports, protocols, and services). This can also be referred to as PPS on DOD information networks (DODIN), including the connected information systems, platform IT systems, platform IT (PIT), and products based on the potential that unregulated PPSM can damage DOD operations and interests. It applies to all PPS used throughout planned, newly developed, acquired, and existing DODIN (whether used internal or external to the enclave), which include DOD IT.

Organizations determine which functions and services are candidates for:

- Removing unused or unnecessary software
- Disabling unused or unnecessary physical and logical ports/protocols (e.g., USB, FTP, and HTTP)

The purpose is to prevent unauthorized connection of unauthorized connection of components, transfer of information, and tunneling.

Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protection technologies such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

CM-8 Information System Component Inventory

This control is to:

- A. Develop an inventory of the system components that:
  - Accurately reflects the system
  - Includes all components within the system
  - Does not include duplicate accounting of components assigned to any other system
  - Is at the level of granularity deemed necessary for tracking and reporting
  - Includes organization-defined information deemed necessary to achieve effective system accountability
- B. Review and update the system component inventory

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

CM-9 Configuration Management Plan (CMP)

The CMP is generated during the development and acquisition phase of the system development lifecycle. CM activities occur throughout the system development life cycle. CMPs define processes and procedures for how configuration management is used to support system development life cycle activities. A CMP is developed, documented and implemented for the system that:

- Addresses roles, responsibilities, and configuration management processes and procedures
- Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items
- Defines the configuration items for the system and places the configuration items under configuration management
- Is reviewed and approved by organization-defined personnel or roles
- Protects the configuration management plan from unauthorized disclosure and modification

There are two types of CM activities:

- Developmental CM activities such as the control of code and software libraries
- Operational CM activities such as control of installed components and how the components are configured

CM-10 Software Usage Restrictions

This control ensures that software use:

- Complies with contract agreements and copyright laws
- Tracks usage of software and associated documentation protected by quantity licenses to control copying and distribution; and

- Controls and documents the use of peer-to-peer file sharing technology to prevent unauthorized distribution, display, performance, or reproduction of copyrighted work.

The organization can impose restrictions on open-source software.

CM-10(1): 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, remediating vulnerabilities in open-source software may be problematic and there are also various licensing issues associated with open-source software including, for example, the constraints on derivative use of such software.

CM-11 User-Installed Software

Establishes governance over installation of software by users, enforces software installation policies through identified methods and monitors policy compliance at a defined frequency.

> **Permitted software** installations may include updates and security patches to existing software and downloading new applications from organization-approved "app stores."
>
> **Prohibited software** installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity.

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.
- Organizations should identify permitted and prohibited actions regarding software installation. Control enhancements can include alerts for unauthorized installations and prohibiting installation without privileged status.

CM-12 Information Location

- Identify and document the location of organization-defined information and the specific system components on which the information is processed and stored.
- Identify and document the users who have access to the system and system components where the information is processed and stored.
- Document changes to the location (i.e., system or system components) where the information is processed and stored.

CM-13 Data Action Mapping

Develop and document a map of system data actions. Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal.

CM-14 Signed Components

Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates.

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 supports auditing of the enforcement actions. Only qualified and authorized individuals are permitted to initiate changes in the system.

- ○ 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 documents the use of peer-to-peer file sharing technology to prevent unauthorized distribution, display, performance, or reproduction of copyrighted work.

- ○ 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 and privacy posture 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 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.

Patch Management defines how patches are prioritized and approved through the configuration change control process. Patches 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: Phase 1:

Planning; Phase 2: Identifying and Implementing Configurations; Phase 3: Controlling Configuration Changes; and Phase 4: Monitoring.

This includes 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 Impact Analyses 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 involves the management of change to maintain the secure, approved baseline of a system?

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

Lesson 5: Auditing and Log Reviews

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.

Here are the lesson 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 individual entries in an audit log related to an audited event used to determine what type of event occurred; when it occurred; where it occurred; source of the event' outcome of the event; and identify individuals, subjects, or objects/entities associated with the event.

Audit trails are chronological records that reconstruct and examine the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to result.

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: It is DOD's policy that 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 Rule

32 CFR 117.18 details audit requirements to ensure information system security. These requirements can be categorized into general requirements, information system security program requirements, and insider threat program requirements.

It is essential that contractor information systems are properly managed to protect against unauthorized disclosure of classified information. The contractor will use a risk-based approach and implement protective measures that include minimum standards for their insider threat program. Protective measures must align with guidance in the Federal Information Security Modernization Act.

Contractors must also maintain information system security programs that incorporate a risk-based set of management, operational, and technical security controls. The program must include policies and procedures to reduce information security risks to an acceptable level and that address information security throughout the full information system life cycle. The program must also address plans and procedures to manage data spills and compromises, including sanitization and recovery methods.

Finally, contractor information system security programs must address information system security training for authorized users. Under the NISPOM Rule, contractors must establish and maintain an insider threat program that address key components, such as user activity monitoring, information sharing procedures, continuous monitoring, and limiting user activity data to privileged users.

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 record observable occurrences in a system, such as password changes, failed logons or accesses, security or privacy attribute changes, and more. The types of events logged are significant and relevant to system security and individual privacy.

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
- ☐ Systems are properly managed to protect against unauthorized disclosure of classified information
- ☐ A risk-based set of management, operational, and technical security controls
- ☐ Audit trails limited to network-level activity and applications
- ☐ Policies that address key components of the insider threat program

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 11.

Instructions for finding the security event log in Windows 11:

Step 1: Select the Windows icon at the lower left of the screen.

Step 2: Type Event Viewer in the Search box.

Step 3: Expand the Windows Logs folder in the left pane by selecting the plus sign.

Notice there are 5 types of event logs set up on this computer.

Step 4: Select the Security event log in the left navigation pane.

Step 5: Double-click the first event to view the details.

Step 6: Examine the details for the selected event.

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.

- ○ Windows icon > Select Event Viewer > Security event log
- ○ Windows icon > Type Event Viewer > Expand Windows Logs folder
- ○ 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 rule 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 rule also requires that the contents of audit trails must be protected against unauthorized access, modification or deletion. The organization System Security Plan (SSP) will define specific auditing requirements

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.

- 4624 - successful logon
- 4625 - unsuccessful logons
- 4634 - successful logoff
- 4625 - account lockout
- 4657 - permissions error
- 4704/4705 - 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)

Lesson 6: Counterintelligence and Cybersecurity in Continuous Monitoring

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 addition, the increasing number of emerging threats can have severely adverse effects on operations, assets, and people.

In order to identify these threats and vulnerabilities, counterintelligence and cybersecurity personnel must work with system owners to employ continuous monitoring to facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.

This lesson 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.

Here are the lesson 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?

DCSA 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. Common methods of Suspicious Network Activity are cyber intrusion, viruses, malware, backdoor attacks, acquisition of usernames 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.

Organizations should implement effective logging and log management tools; employ security controls to protect confidentiality, integrity, and availability of the system; log in using least privilege and separation of duties; and secure supply chain operations. Organizations should also disable or uninstall unused/unnecessary operating system, or OS, functionality, protocols, ports, and services. Limit the software that can be installed and the functionality of that software.

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 indicator 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 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 will establish and maintain a continuous monitoring capability that provides cohesive collection, transmission, storage, aggregation, and presentation of data that conveys current operational status to affected DOD stakeholders. DOD Components will achieve cohesion through using 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. This can be achieved by ensuring that the security posture of one system is not undermined by vulnerabilities of interconnected systems. Full integration into system life cycles as a visible element of DOD Component IT portfolios, and through adherence to DOD architecture principles, adopting a standards-based approach, and sharing the level of risk necessary to achieve mission success. t

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.

Insight and oversight include measuring, reviewing, verifying, monitoring, facilitating, and remediating. Effective insight and oversight depend on three conditions implemented across DOD: coordinated and consistent implementation, organization direction, and a culture of accountability. First, ensure coordinated and consistent cybersecurity implementation and reporting across all organizations without impeding local missions. Next, organization direction includes organizational mechanisms for establishing and communicating priorities and objectives, principles, policies, standards, and performance measures. Finally, a culture of accountability aligns internal processes, maintains accountability, and informs, makes, and follows through on decisions with implications for cyberspace protection and defense.

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 systems and the information that they process, store, or transmit.

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
- Control Software Installation
- 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 Endpoint Protection Platforms (EPPs)
- Use Cryptography

Implement Endpoint Protection Platforms (EPPs)

Endpoint Protection Platforms include:

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

Use Cryptography

- In many systems, cryptography is considered to be part of the secure configuration of the system. There are a variety of places to implement cryptography to protect data, including individual file encryption, full disk encryption, Virtual Private Network connections, etc.
- 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

Lesson 7: Course Conclusion

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 Information Security Continuous Monitoring (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. Please use the Security Training, Education, and Professionalization Portal (STEPP) system to access the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

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 implements policy, assigns responsibilities, establishes requirements, and provides procedures for the protection of classified information that is disclosed to, or developed by, contractors of the U.S. Government.

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

Feedback*: The NISPOM Rule implements policy, assigns responsibilities, establishes requirements, and provides procedures for the protection of classified information that is disclosed to, or developed by, contractors of the U.S. Government.*

Statement 2 of 3. This 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 Rule
- ○ 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 Information System Continuous Monitoring (ISCM) program and security-focused configuration management.

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

***Feedback**: The NIST 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.*

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 that 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 DOD Component SISO has authority and responsibility for security controls assessment at this level.

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

***Feedback**: The DOD Component SISO has authority and responsibility for security controls assessment at this level.*

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.*

Lesson 3 Review Activities

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 an ISCM program, security-related information required for metrics, assessments, and reporting is collected and, where possible, the collection, analysis, and reporting of data are 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.*

Lesson 4 Review Activities

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 supports auditing of the enforcement actions. Only qualified and authorized individuals are permitted to initiate changes in the system.

- ○ 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 supports auditing of the enforcement actions. Only qualified and authorized individuals are permitted to initiate changes in the system.*

Question 2 of 4: This control ensures that software use complies with contract agreements and copyright laws, tracks usage, and documents the use of peer-to-peer file sharing technology to prevent unauthorized distribution, display, performance, or reproduction of copyrighted work.

- ○ 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 documents the use of peer-to-peer file sharing technology to prevent unauthorized distribution, display, performance, or reproduction of copyrighted work.*

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 and privacy posture 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 and privacy posture 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 involves the management of change to maintain the secure, approved baseline of a system?

- ○ Phase 1: Planning
- ○ Phase 2: Identifying and Implementing Configurations

- ⦿ Phase 3: Controlling Configuration Changes (correct response)
- ○ Phase 4: Monitoring

***Feedback**: Phase 3: Controlling Configuration Changes, involves the management of change to maintain the secure, approved baseline of a system.*

Lesson 5 Review Activities

Review Activity 1

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

- ☐ Audit records limited to user access log-on
- ☑ Systems are properly managed to protect against unauthorized disclosure of classified information
- ☑ A risk-based set of management, operational, and technical security controls (correct response)
- ☐ Audit trails limited to network-level activity and applications
- ☑ Policies that address key components of the insider threat program (correct response)

***Feedback**: Audit requirements in the NISP include: systems that are properly managed to protect against unauthorized disclosure of classified information; a risk-based set of management, operational, and technical security controls; and policies that address key components of the insider threat program.*

Review Activity 2

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

- ○ Windows icon > Select Event Viewer > Security event log
- ⦿ Windows icon > Type Event Viewer > Expand Windows Logs folder (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 Windows icon; then type Event Viewer; and then expand the Windows Logs folder.*

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.*

Lesson 6 Review Activities

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.*