Cybersecurity for Security Personnel

Student Guide

September 2017

Center for Development of Security Excellence

Lesson 1: Course Introduction

Introduction

Welcome

The world of security has many areas that require our protection. You have probably heard the term cybersecurity. It is an important topic within the world of security. But, what is cybersecurity? And, what is your role? Why is cybersecurity important?

Welcome to the Cybersecurity for Security Personnel course!

Objectives

This course provides an overview of Security Personnel's role in cybersecurity including the describing the need for cybersecurity, cybersecurity roles and responsibilities, an overview of risk management, and emphasis on those responsibilities of Security Personnel in risk management. Here are the course objectives. Take a moment to review them.

- Describe the need for cybersecurity
- Describe cybersecurity roles and responsibilities
- Explain the role of risk management in protecting against cyber attacks
- List the step in the Risk Management Framework (RMF) process designed to assess risk
- List the two steps in RMF process designed to mitigate risk
- List the three evaluation steps in the RMF process

Lesson 2: Cybersecurity for Security Personnel

Introduction

Objectives

Before we can discuss your role in cybersecurity and prevention methods, we need to start with an overview of cybersecurity. You might be asking yourself the following questions:

- Why do we need cybersecurity?
- What exactly is cybersecurity?
- Why is it important to me and my role?
- What policies and DoD regulations apply?
- Do I need special skills in order to support cybersecurity?

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

- Describe the need for cybersecurity
- Define cybersecurity
- Recognize the importance of cybersecurity
- List the policy and DoD regulation drivers of a cybersecurity program
- List the cybersecurity skill standards needed by security personnel

What is Cybersecurity?

Attributes

Cybersecurity consists of five attributes:

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-repudiation

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

Integrity guards against improper modification to or destruction of information. For example, integrity prevents a user from improperly or maliciously modifying a database.

Availability ensures timely and reliable access to and use of information. For example, availability ensures that an information system is accessible when an authorized user needs it.

Authentication is critical, as it is the mechanism that authorizes or allows access to computer systems and networks and the data that resides there. Loss of or incorrect authentication services could allow unauthorized access to classified data. For example, a Common Access Card (CAC) is one method to provide system identification that authenticates the user.

Non-repudiation ensures that a party in an electronic exchange cannot deny their participation or the authenticity of the message. For example, a digital signature in an email message confirms the identity of the sender.

Importance

Each of the five attributes is susceptible to threats and vulnerabilities. As security personnel, you need to be aware of the attributes to ensure that you appropriately manage the risk across all areas. Overlooking one attribute could create a vulnerability that leaves data susceptible to attack. You must maintain these areas to prevent loss. Confidentiality and authentication may be most important from an information security perspective. Together, these two concepts ensure that our nation's private information is contained and that anyone who wants access to it must prove who they are and why they need access.

Policy and DoD Regulation Drivers

Cybersecurity Drivers

Several policies and DoD regulations set our cybersecurity standards:

- The DoDI 8500.01, Cybersecurity document outlines the overarching risk management process
- The DoD 5200.01, DoD Security Policy which addresses the processes, roles, and responsibilities
- The DoD 8510.01, Risk Management Framework which outlines the risk management framework that applies to DoD information technology and identifies the process to follow and specific roles and responsibilities
- The DoD 8530.01, Cybersecurity Activities Support to DoD Information Network Operations which states that the DoD needs to ensure information is confidently protected by vulnerability assessment and analysis, vulnerability management,

malware protection, continuous monitoring, cyber incident handling, DoDIN user activity monitoring for the DoD Insider Threat Program, and warning intelligence and attack sensing and warning (AS&W)

- The NIST 800-30 Guide for Conducting Risk Assessments

When you compile and look at all of these policies and drivers together, the overarching Security Policy emerges. It is to do the following:

- Identify and protect national security information and controlled unclassified information (CUI) in accordance with national-level policy issuances
- Promote information sharing, facilitate judicious use of resources, and simplify management through implementation of uniform and standardized processes
- Employ, maintain, and enforce standards for safeguarding, storing, destroying, transmitting, and transporting classified information
- Actively promote and implement security education and training throughout the Department of Defense
- Mitigate the adverse effects of unauthorized access to classified information by investigating and acting upon reports of security violations and compromises of classified information

Go to the course resources page to access these policies.

DoD Cybersecurity Policies

The DoD cybersecurity policies include risk management, operational resilience, integration and interoperability, cyberspace defense, performance, DoD information, identity assurance, information technology, cybersecurity workforce, and mission partners.

Risk Management

Take a moment to review the specific language regarding risk management from the DODI 8500.01, Cybersecurity, March 2014:

- DoD will implement a multi-tiered cybersecurity risk management process.
- DoD must consider all cybersecurity risks.
- All DoD IT will participate in a cybersecurity program to manage risk.
- Risk management will be addressed as early as possible.
- Documentation regarding the security posture of DoD IS and platform information technology (PIT) systems will be made available.

Operational Resilience

Now review the details regarding operational resilience from the DODI 8500.01, Cybersecurity, March 2014:

- Information and services are available to authorized users.
- Security posture is sensed, correlated, and made visible to mission owners, network operators, and to the DoD Information Enterprise.
- Whenever possible, technology components have the ability to reconfigure, optimize, self-defend, and recover with little or no human intervention.

Integration and Interoperability

Review this additional information on integration and interoperability:

- Cybersecurity must be fully integrated into system life cycles.
- Interoperability will be achieved through adherence to DoD architecture principles, adopting a standards-based approach, and by all DoD Components sharing the level of risk necessary to achieve mission success.
- All interconnections of DoD IT will be managed to minimize shared risk.

Cyberspace Defense

Take a moment to explore cyberspace defense:

- Employed to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities.
- Shared with all appropriately cleared and authorized personnel.

Performance

Review these performance details:

- Implementation of cybersecurity will be overseen and governed through the integrated decision structures and processes.
- Performance will be measured, assessed for effectiveness, and managed.
- Data will be collected to support reporting and cybersecurity management activities.
- Standardized information technology tools, methods, and processes will be used to the greatest extent possible.

DoD Information

Now review DoD information categorization:

- All DoD information in electronic format will be given an appropriate level of confidentiality, integrity, and availability.

Identity Assurance

Take a moment to review the specifics about identity assurance:

- Identity assurance must be used to ensure strong identification, authentication, and eliminate anonymity.
- DoD will public key-enable DoD information systems (ISs) and implement a DoD-wide Public key Infrastructure (PKI) solution that will be managed by the DoD PKI Program Management Office.
- Biometrics will be managed.

Information Technology

Information technology is a broad topic. Take a moment to review what you need to know in relation to cybersecurity:

- All information technology that receives, processes, stores, displays, or transmits DoD information will be acquired, configured, operated, maintained, and disposed of.
- Risks, weaknesses or flaws, and vulnerabilities introduced through faulty design, configuration, or use will be managed, mitigated, and monitored.
- Cybersecurity requirements must be identified and included.

Cybersecurity Workforce

Now review the considerations for the cybersecurity workforce:

- Cybersecurity workforce functions must be identified and managed.
- Qualified cybersecurity personnel must be identified and integrated into all phases of the system development lifecycle.

Mission Partners

Review these considerations for working with mission partners:

- Capabilities that are shared with mission partners will be consistent.
- DoD-originated and DoD-provided information must be properly and adequately safeguarded, with documented agreements indicating required levels of protection.

Security Personnel Skills

Security Personnel Skills

In order to put the policies into action, you must be able to identify fundamental cybersecurity concepts that are related to the protection of classified and controlled unclassified information. You also need to be able to explain your role in protecting DoD's information systems and the information they process, transmit, and store.

Additional Topics

Take a moment to review the other topics associated with your role as security personnel.

- Information Assurance Attributes
- System Categorization
- Assessment and Authorization Process
- Data Spills
- Disposal of Computer Media
- Non-Traditional Work Environments
- Processing Requirements for Specific Types of Information
- New Technology and Equipment
- Social Networking Services
- Compilation and Data Aggregation
- Marking Requirements for Electronic Information
- Position Sensitivity Designation/Personnel Security Investigative Standards
- Cybersecurity Policy

Review Activities

Review Activity 1

What are the cybersecurity attributes?

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

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Authentication
- ☐ Non-repudiation

Review Activity 2

Why do you need to be aware of cybersecurity?

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

- ○ To uphold all elements of the National Industrial Security Program Operating Manual
- ○ To appropriately manage risk by mitigating threats and vulnerabilities
- ○ To examine your own actions and activities to uphold personal accountability
- ○ To ensure all appropriate measures are taken to protect a place and ensure only people with permission enter and leave it

Review Activity 3

What are the cybersecurity drivers?

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

- ☐ NIST 800-30 Rev 1, Guide for Conducting Risk Assessments
- ☐ DoD 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
- ☐ DoD 8510.01, Risk Management Framework
- ☐ DoD 8500.01, Cybersecurity
- ☐ DoD Security Policy

Review Activity 4

Which skills do security personnel need?

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

- ☐ Protect information systems.
- ☐ Identify all cybersecurity concepts.
- ☐ Identify fundamental cybersecurity concepts that are related to the protection of classified and controlled unclassified information.
- ☐ Examine their role in protecting DoD's information systems and the information they process, transmit, and store.

Lesson 3: Cybersecurity Roles and Responsibilities

Introduction

Objectives

Now that you have a better understanding of cybersecurity and its importance, we can describe what your security personnel role and responsibilities are.

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

- Describe cybersecurity roles and responsibilities
- Explain the role of security personnel in the protection of classified information and controlled unclassified information
- List specific skills and competencies found in the Department of Defense Security Skill Standards

Roles

Security Personnel

Let's first explore your responsibilities as security personnel. You must protect classified information and controlled unclassified information. You should have proactive and continuous engagement and collaboration between security, information technology (IT), and cybersecurity personnel, at all organizational levels. You must also manage threats, minimize vulnerabilities, use appropriate countermeasures, and respond to incidents swiftly and appropriately. You won't be doing all of this alone. Let's take a look at what other roles have responsibilities related to cybersecurity.

Other Roles

In addition to security personnel, there is a DoD Chief Information Officer (CIO), US Cyber Command (USCYBERCOM), and other cybersecurity staff.

The DoD CIO monitors, evaluates, and provides advice to the Secretary of Defense regarding all DoD cybersecurity activities and oversees implementation of this cybersecurity. The DoD CIO also develops and establishes DoD cybersecurity policy and guidance consistent with this instruction and in accordance with applicable federal law and regulations. For a full list of responsibilities, refer to DoD Instruction (DoDI) 8500.01, Cybersecurity, available through the course resources.

USCYBERCOM has the overall responsibility of directing the operation of and assuring the security of the global DoD network environment. USCYBERCOM leads the day-to-day

defense and protection of the DoD networks, coordinates all DoD network operations, and provides full spectrum support to military and counterterrorism mission.

At the Component and activity-level, you need to be aware of other cybersecurity staff as well, such as the Authorizing Official (AO), Personnel Security Specialist, Physical Security Specialist, Information Security Specialist, Industrial Security Specialist, Security Specialist, Security Officer, and the Risk Executive Function.

Security Personnel Skills and Accountabilities

Security Personnel Skills and Accountabilities

What skills do security personnel need to achieve their responsibilities?

The main skill of security personnel is to manage risk. Additionally, there are many implied skills. Security personnel have analyzing duties. They also counsel stakeholders on security-related concerns, issues, and challenges. Security personnel should support risk assessment and management. They execute security awareness training and education requirements and respond to security incidents.

Security personnel are also accountable for many areas including information assurance and cybersecurity within the DoD. Lastly, security personnel are accountable for cyber command readiness. Security personnel have implied accountability in information security, personnel security, physical security, counterintelligence, and vulnerabilities assessment and management. You may refer to the DS3 for more information on skills, competencies, and cross functional competencies.

Review Activities

Review Activity 1

What is the primary responsibility of security personnel?

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

- ○ Monitor, evaluate, and provide advice to the Secretary of Defense
- ○ Protect classified information and controlled unclassified information
- ○ Direct the operation of and assure the security of the global DoD network
- ○ Coordinate all DoD network operations

Review Activity 2

What is security personnel's ***primary*** skill in relationship to cybersecurity?

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

- ○ Analyze duties
- ○ Manage risk
- ○ Execute training
- ○ Respond to incidents

Lesson 4: Risk Management

Introduction

Objectives

Risk management is how you, as security personnel, can uphold your cybersecurity responsibilities. Here are the lesson objectives. Take a moment to review them.

- Explain the role of risk management in protecting against cyber attacks
- Describe the key components of a risk management system (assessment, mitigation, evaluation)
- List the steps in the Risk Management Framework (RMF)

Risk Management System Components

Components

The risk management system provides an overarching methodology to follow when managing risks. Using the risk management system is the recommended method to fulfilling this responsibility. At a high level, the risk management system consists of assessment, mitigation, and evaluation. You should look at these components sequentially. Assessing the risk comes first, then mitigating it, and finally evaluating it. You should, however, be aware of the impacts and reassess constantly as you deploy new solutions. As you move an identified risk through the phases, you should constantly be considering the other components as well.

Risk Assessment

When performing risk assessment, security personnel identify and evaluate risks, risk impacts, and countermeasures. This determines the extent of the threat and risk associated with the information system and is used to identify security controls to decrease the risk. Be sure to revisit risk assessment as you move through the other phases of risk management.

Mitigation

Security personnel mitigate risk by prioritizing, implementing, and maintaining risk-reducing measures. Your goal is to implement the most appropriate controls. When mitigating risk, you may accept the risk by simply continuing to operate the information system. You may also choose to avoid the risk by eliminating the risk cause and/or the consequence. Finally, you may limit the risk by implementing controls to minimize the adverse impact of a threat exploiting a vulnerability.

Evaluation

Risk evaluation is essential to the risk management process. It is the continual process of assessing and mitigating risk. Then purpose of evaluation is to ensure that as changes occur, you are reviewing and ensuring that new risks have not arisen.

Risk Management Framework

Overview

The risk management system is executed by adhering to the Risk Management Framework (RMF). There are six steps to the RMF:

- Step 1 is Categorize System.
- Step 2 is Select Security Controls.
- Step 3 is Implement Security Controls.
- Step 4 is Assess Security Controls.
- Step 5 is Authorize System.
- Step 6 is Monitor Security Controls.

The RMF is an integrated enterprise-wide decision structure for cybersecurity risk management that includes and integrates DoD mission areas. You can find more information in the DoD Instruction (DoDI) 8510.01, Cybersecurity. To facilitate reciprocity among federal agencies, use the RMF process to assess and authorize information systems. Risk management can help prevent issues and manage all information systems.

Review Activities

Review Activity 1

What are the components of the Risk Management System?

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

- ☐ Revision
- ☐ Analysis
- ☐ Evaluation
- ☐ Assessment
- ☐ Mitigation

Review Activity 2

What are the steps in the Risk Management Framework (RMF)?

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

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

Lesson 5: Assess Risk

Introduction

Objectives

This lesson focuses on Step 1 Categorize the System of the Risk Management Framework (RMF).

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

- List the step in the RMF process designed to assess risk
- Explain how to assess threats to your information technology (IT) infrastructure
- Describe ways to spot vulnerabilities to your IT program

Threats

Definition

Step 1 of the RMF corresponds to assessment in the risk management system. Your responsibility as Security Personnel is to know how to assess threats to your information technology (IT) infrastructure and how to spot vulnerabilities to your IT program. Threats are a potential activity that may contribute to the risks associated with operating an information system, or IS – controlled or uncontrolled, intentional or unintentional.

Threat Environment

The overall threat environment can be addressed in four areas:

- Adversarial
- Accidental
- Structural
- Environmental

Adversarial threats are from individual, group, organization, or nation-state seeking to exploit the organization's dependence on cyber resources. Accidental threats are unintentional threats made by a single user or privileged user or administrator when performing their everyday responsibilities. Structural threats are failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances. Environmental threats are natural or man-made disasters, unusual natural events, or an infrastructure failure or outage.

Evolving Threats

Within the overall threat environment, there are constant evolving threats and new technologies that leave the DoD vulnerable to attack. Cyber attacks are attempts by hackers to damage or destroy a computer network or system. Insider threats are malicious threats to an organization that come from people within the organization who have legitimate access to information concerning the organization's security practices, data and computer systems. Social media includes websites and applications that enable users to create and share content or to participate in social networking. Mobile computing is technology that allows transmission of data, voice, and video via a computer or any other wireless enabled device without having to be connected to a physical link. The challenge is keeping up with the new threats as new environments are created.

Threat Methods

There are many ways that cyber attackers can gain access.

Adversaries use probing and scanning to ascertain information about services, vulnerabilities, and hosts on a network.

Sniffing and eavesdropping allow adversaries to tap into network traffic and capture packets.

Malicious code or malware uses software to attack/damage computer systems and networks. Examples include viruses, worms, and Trojans.

Denial of Service (DOS) creates service outages by saturating resources on systems or network so that network or computers cannot provide required services to users. Examples include teardrop attack, Smurf attack, and Distributed DOS (DDOS).

Spoofing uses false information to gain unauthorized access to resources. Examples include forged IP addresses, Man-in-the-Middle attacks, and session hijacking attacks.

Password cracking allows adversaries to derive passwords, which are arguably the weakest link in the security chain. Easy-to-guess passwords, dictionary attacks, and brute force attacks are among the most common ways this threat is exposed.

Social engineering manipulates people into divulging confidential information through pretexting/scenarios, phishing, something to something, and dumpster diving. Information found from dumpster diving can provide an attacker with information to hack into system.

Please note that not all threats are issues. You must evaluate the threats and then make appropriate decisions.

Vulnerabilities

Vulnerabilities

Threats take advantage of weaknesses—or *vulnerabilities*–to gain unauthorized access to our information or systems. Vulnerabilities include physical security, IS software and hardware, and people. As security personnel, you need to assess the ease, rewards, likelihood, related threats, and residual risk of vulnerabilities. Vulnerabilities are categorized into three tiers. Tier 1 is the organization level. Tier 2 is mission/business process level. Tier 3 is the Information system level, which is where network vulnerabilities are categorized. Your goal as security personnel is to be aware of vulnerabilities so that you can coordinate the appropriate countermeasures to prevent exposure.

Review Activities

Review Activity 1

What threat environments should you consider?

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

- ☐ Adversarial
- ☐ Environmental
- ☐ Structural
- ☐ Accidental

Review Activity 2

What should you look for when assessing vulnerabilities?

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

- ☐ Residual risk
- ☐ Ease
- ☐ Likelihood
- ☐ Related threats
- ☐ Rewards

Lesson 6: Mitigate Risk

Introduction

Objectives

This lesson focuses on the Risk Management Framework (RMF) steps associated with mitigating risk and your role as security personnel. The associated steps within the RMF are Step 2, Select Security Controls, and Step 3, Implement Security Controls.

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

- List the two steps in the RMF designed to mitigate risk
- Explain Step 2 of the RMF – Select security controls
- Explain Step 3 of the RMF – Implement security controls

Countermeasures

Overview

In Step 2 of the RMF, Select Security Controls, four categories of activities occur. First is common control identification, followed by security baseline and overlay selection. Next is development of a monitoring strategy. Lastly, review and approval of the security plan and system level continuous monitoring strategy.

Common Control Identification

Common control identification is performed by the Information Security Officer (ISO) and the Common Control Provider. These two roles are responsible for the coordination and selection of the controls. The Chief Information Officer (CIO) provides resources and guidance for selecting security controls. The CIO also approves the selections made by the ISO and Common Control Provider.

Security Baseline and Overlay Selection

Security baseline and overlay selection is to identify the baseline for the system based on impact levels. It should also be documented in the security plan. It also identifies overlays that apply to the information system (IS) or platform information technology (PIT) system.

Monitoring Strategy

The monitoring strategy defines how the continuing effectiveness of security controls will be evaluated. The monitoring strategy includes a plan for annually assessing the implemented security controls.

Security Plan Review and Approval

Security plan and system-level continuous monitoring strategy review and approval is where the DoD Components develop and implement the processes. The Authorizing Official (AO) reviews the processes and decides whether to authorize the security plan and continuous monitoring.

Security Areas

There are three areas within cybersecurity:

- Physical
- Personnel
- Procedural

Security personnel must ensure the necessary countermeasures are applied.

Physical security limits physical access to the information systems. Examples include:

- ISs that process sensitive compartmented information (SCI) or are kept in a SCI facility (SCIF) that has higher physical protection
- Locking the server room door
- Securing workstations
- Protecting portable devices such as laptops, tablets, and phones
- Disabling drives
- Protecting printers and waste

Personnel security limits access to the IS to cleared personnel with a need-to-know and/or ensuring that IS users are aware of the policies associated with it and their responsibilities to protect the information it contains. Examples include:

- Implementing unique identification
- Correlating actions to users
- Maintaining user IDs
- Deactivating user IDs that are no longer eligible for access or no longer need-to-know
- Implementing authentication requirements

Procedural security puts organization-wide countermeasures into place. Examples include:

- Internal Detection Systems (IDS) firewalls
- Encryption
- Not permitting thumb drives

Implement Risks Controls

Step 3

In Step 3 of the RMF, Implement Security Controls, security controls are put in place. The implementation must be consistent with DoD Component Cybersecurity architectures and documented in the security plan. It must also identify any controls available for inheritance. To do this, products must be configured in accordance with the applicable Security Technical Implementation Guides (STIGs) or Security Requirements Guide (SRGs). The security controls must be implemented consistently with DoD architectures and standards, and employ system and software engineering methodologies, security principles, and secure coding techniques. Proposed security design must be addressed in preliminary and critical design reviews. Then, the security plan is updated to describe and document the security control implementation. Lastly, existing security controls are reviewed. If they do not pose a risk, then they are inherited into the new practice.

Review Activities

Review Activity 1

Which steps of the RMF are designed to mitigate risk?

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

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

Review Activity 2

Which of the following are the activities that occur when performing RMF Step 2, Select Security Controls?

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

- ☐ Common Control Identification
- ☐ Monitoring Strategy
- ☐ Security Baseline and Overlay Selection
- ☐ Security Plan and Review Approval

Review Activity 3

What activities occur during implementation of security controls?

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

- ☐ Communicate updates to appropriate audiences
- ☐ Seek approvals from CIO
- ☐ Create appropriate training and communication plans
- ☐ Ensure consistency with DoD architectures
- ☐ Document security control implementation in the security plan
- ☐ Identify security controls available for inheritance

Lesson 7: Evaluate Risk

Introduction

Objectives

This lesson focuses on the Risk Management Framework (RMF) steps associated with evaluating risk and your role as security personnel. The associated steps are:

- Step 4, assess security controls
- Step 5, authorize system
- Step 6, monitor security controls

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

- List the three evaluation steps in the RMF process
- Describe Step 4 – Assess security controls
- Describe Step 5 – Authorize system
- Describe Step 6 – Monitor security controls

Associated RMF Steps

Assess Security Controls

Step 4, assess security controls, has four major activities that should occur. First, the Security Assessment Plan is developed, reviewed, and approved. Next, security controls are assessed. The Security Controls Assessor (SCA) prepares the Security Assessment Report (SAR). You also need to conduct remediation actions on non-compliant (NC) security controls.

Security Assessment Plan

The Security Assessment Plan is developed, reviewed, and approved in the following ways. You need to ensure that security assessment activities are coordinated. The areas to review include interoperability and supportability certification efforts, Developmental Test and Evaluation (DT&E) events, and Operational Test and Evaluation (OT&E) events. Coordination of activities must also be documented in the Security Assessment Plan. The focus of the Security Assessment Plan is to maximize effectiveness, reuse, and efficiency.

Assess Security Controls

Security control assessment requires four activities. First, compare the security controls to the security assessment plan and the DoD assessment procedures. Next, record the security control compliance status. Additionally, you need to assign the vulnerability severity value for security controls. You must also determine the risk level for security controls. You do this by using SCA's determination that a credible or validated threat source and event exists. Consider the vulnerability severity level and pre-disposing conditions as well as the cybersecurity attributes and all impact levels related to the control. SCA's consider the impact of a successful threat event. Finally, assess and characterize the aggregate level of risk to the system.

Security Assessment Report

The SCA prepares the SAR. It documents issues, findings, and recommendations from the security control assessment. The SAR is required for an authorization decision.

Remediation Actions

When you conduct remediation actions on NC security controls, you base your findings and recommendations on the SAR. You will also reassess remediated controls.

Authorize System

In Step 5 of the RMF, Authorize System, the Authorizing Official (AO) issues an authorizing decision. To do this, the AO needs the security authorization package. This consists of the Plan of Action and Milestones (POA&M), the security plan, and the SAR. The AO may have feedback that requires revision of the security authorization package, which must then be resubmitted to the AO for review and final acceptance. The AO conducts the final risk determination and ultimately makes an authorization decision.

Monitor Security Controls

In Step 6 of the RMF, Monitor Security Controls, the impact of changes to the system and environment are determined; selected security controls are assessed according to the continuous monitoring strategy; remediation actions are taken; the security plan, SAR, and POA&M are updated as necessary; security status is reported to AO who reviews the status reports; and the system decommissioning strategy is implemented when needed.

Impact of Changes

When determining the impact of changes to the system and environment, the information system owner continuously monitors the system or information environment, periodically assesses the quality of security controls, and reports any significant change in the security posture of the system.

Assess Selected Controls

A selected subset of controls must be assessed in accordance with the continuous monitoring strategy. The assessor must create a written and signed SAR that indicates the results of the assessment. The AO must review the SAR.

Conduct Remediation

Remediation actions are based on ongoing monitoring activities, assessment of risk, and any outstanding items in the POA&M.

Update Documentation

Throughout monitoring, the security plan, SAR, and POA&M must be kept up-to-date. Updates result from changes due to system-level continuous monitoring. The Program Manager (PM) and/or Security Manager (SM) perform all primary activities.

Security Status Reports

The security status gets reported to the AO. Be sure to include the effectiveness of security controls employed within and inherited by the system.

AO

During continuous monitoring, the AO reviews the reported status. The AO review includes the effectiveness of security controls employed within and inherited by the system.

Decommissioning Strategy

When the system is no longer necessary, the decommissioning strategy is implemented. In this case, the information system (IS) owner executes the actions outlined in the decommissioning strategy in the security plan. When a system is removed from operation, assess the impact on control inheritance relationships, update security plan to reflect decommissioned status, dispose of artifacts and supporting documentation according to sensitivity or classification, and review data or objects that support DoD information enterprise.

Review Activities

Review Activity 1

Which steps of the RMF are designed to evaluate risk?

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

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

Review Activity 2

What activities occur when assessing security controls?

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

- ☐ Prepare the Plan of Action and Milestones (POA&M)
- ☐ Conduct final risk determination
- ☐ Develop, plan, and approve Security Assessment Plan
- ☐ Prepare Security Assessment Report (SAR)

Review Activity 3

What activities occur when authorizing the system?

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

- ☐ Implement decommissioning strategy
- ☐ Develop, review, and approve Security Assessment Plan
- ☐ Prepare the Plan of Actions and Milestones (POA&M)
- ☐ Submit security authorization package

Review Activity 4

What activities occur when monitoring security controls?

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

- ☐ Prepare the Plan of Actions and Milestones (POA&M)
- ☐ Develop, review, and approve Security Assessment Plan
- ☐ Implement decommissioning strategy
- ☐ Determine impact of changes

Lesson 8: Course Conclusion

Conclusion

Course Summary

This course provided an overview of cybersecurity and your role within it, introduced the risk management system, and provided an overview of the Risk Management Framework (RMF). Finally, you learned how the RMF supports the risk management system and your responsibilities within it.

Lesson Review

Congratulations! You have completed the *Cybersecurity for Security Personnel* course.

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

- Describe the need for cybersecurity
- Describe cybersecurity roles and responsibilities
- Explain the role of risk management in protecting against cyber attacks
- List the step in the Risk Management Framework (RMF) process designed to assess risk
- List the two steps in the RMF process designed to mitigate risk
- List the three evaluation steps in the RMF process

To receive course credit, you must take the *Cybersecurity for Security Personnel* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

What are the cybersecurity attributes?

- ☑ Confidentiality *(correct response)*
- ☑ Integrity *(correct response)*
- ☑ Availability *(correct response)*
- ☑ Authentication *(correct response)*
- ☑ Non-repudiation *(correct response)*

Feedback: *The five cybersecurity attributes are confidentiality, integrity, availability, authentication, and non-repudiation.*

Review Activity 2

Why do you need to be aware of cybersecurity?

- ○ To uphold all elements of the National Industrial Security Program Operating Manual
- ⊙ To appropriately manage risk by mitigating threats and vulnerabilities *(correct response)*
- ○ To examine your own actions and activities to uphold personal accountability
- ○ To ensure all appropriate measures are taken to protect a place and ensure only people with permission enter and leave it

Feedback: *Each of the cybersecurity attributes is susceptible to threats and vulnerabilities. Security personnel need to be aware of the attributes to ensure they are appropriately managing the risk across all areas.*

Review Activity 3

What are the cybersecurity drivers?

- ☑ NIST 800-30 Rev 1 Guide for Conducting Risk Assessments *(correct response)*
- ☑ DoD 8530.01 Cybersecurity Activities Support to DoD Information Network Operations *(correct response)*
- ☑ DoD 8510.01 Risk Management Framework *(correct response)*
- ☑ DoD 8500.01 *(correct response)*
- ☑ DoD Security Policy *(correct response)*

Feedback: *All of these are cybersecurity drivers.*

Review Activity 4

Which skills do security personnel need?

- ☐ Protect information systems.
- ☐ Identify all cybersecurity concepts.
- ☑ Identify fundamental cybersecurity concepts that are related to the protection of classified and controlled unclassified information. *(correct response)*
- ☑ Examine their role in protecting DoD's information systems and the information they process, transmit, and store. *(correct response)*

Feedback: *Security personnel must be able to identify fundamental cybersecurity concepts that are related to the protection of classified and controlled unclassified information AND examine their role in protecting DoD's information systems and the information they process, transmit, and store.*

Lesson 3 Review Activities

Review Activity 1

What is the primary responsibility of security personnel?

- ○ Monitor, evaluate, and provide advice to the Secretary of Defense
- ⦿ Protect classified information and controlled unclassified information *(correct response)*
- ○ Direct the operation of and assure the security of the global DoD network
- ○ Coordinate all DoD network operations

Feedback: *Security personnel protect classified information and controlled unclassified information.*

Review Activity 2

What is security personnel's ***primary*** skill in relationship to cybersecurity?

- ○ Analyze duties
- ⦿ Manage risk *(correct response)*
- ○ Execute training
- ○ Respond to incidents

Feedback: *Security Personnel's primary role is to manage risk. The other descriptions are all implied duties.*

Lesson 4 Review Activities

Review Activity 1

What are the components of the Risk Management System?

- ☐ Revision
- ☐ Analysis
- ☑ Evaluation *(correct response)*
- ☑ Assessment *(correct response)*
- ☑ Mitigation *(correct response)*

Feedback: *The components of a risk management system are assessment, mitigation, and evaluation.*

Review Activity 2

What are the steps in the Risk Management Framework (RMF)?

- ☑ Monitor Security Controls *(correct response)*
- ☑ Categorize System *(correct response)*
- ☑ Authorize System *(correct response)*
- ☑ Assess Security Controls *(correct response)*
- ☑ Select Security Controls *(correct response)*
- ☑ Implement Security Controls *(correct response)*

Feedback: *These are all steps to the RMF.*

Lesson 5 Review Activity

Review Activity 1

What threat environments should you consider?

- ☑ Adversarial *(correct response)*
- ☑ Environmental *(correct response)*
- ☑ Structural *(correct response)*
- ☑ Accidental *(correct response)*

Feedback: *These are the four types of threats you need to consider.*

Review Activity 2

What should you look for when assessing vulnerabilities?

- ☑ Residual risk *(correct response)*
- ☑ Ease *(correct response)*
- ☑ Likelihood *(correct response)*
- ☑ Related threats *(correct response)*
- ☑ Rewards *(correct response)*

Feedback: *You should consider all of these areas when assessing vulnerabilities.*

Lesson 6 Review Activities

Review Activity 1

Which steps of the RMF are designed to mitigate risk?

- ☐ Assess Security Controls
- ☐ Monitor Security Controls
- ☑ Select Security Controls *(correct response)*
- ☐ Authorize System
- ☑ Implement Security Controls *(correct response)*
- ☐ Categorize System

Feedback: *The two steps designed to mitigate risk from the RMF are Select Security Controls and Implement Security Controls.*

Review Activity 2

Which of the following are the activities that occur when performing RMF Step 2, Select Security Controls?

- ☑ Common Control Identification *(correct response)*
- ☑ Monitoring Strategy *(correct response)*
- ☑ Security Baseline and Overlay Selection *(correct response)*
- ☑ Security Plan and Review Approval *(correct response)*

Feedback: *These are all activities that occur during the RMF Step 2, Select Security Controls.*

Review Activity 3

What activities occur during implementation of security controls?

- ☐ Communicate updates to appropriate audiences
- ☐ Seek approvals from CIO
- ☐ Create appropriate training and communication plans
- ☑ Ensure consistency with DoD architectures *(correct response)*
- ☑ Document security control implementation in the security plan *(correct response)*
- ☑ Identify security controls available for inheritance *(correct response)*

Feedback: *In Step 3, Implement Security Controls, implement solutions consistent with DoD Component cybersecurity architectures, document security control implementation in the security plan, and identify security controls available for inheritance.*

Lesson 7 Review Activities

Review Activity 1

Which steps of the RMF are designed to evaluate risk?

- ☑ Select Security Controls
- ☑ Assess Security Controls *(correct response)*
- ☑ Monitor Security Controls *(correct response)*
- ☑ Authorize System *(correct response)*
- ☐ Categorize System
- ☐ Implement Security Controls

Feedback: *The three steps designed to evaluate risk are Assess Security Controls, Authorize System, and Monitor Security Controls.*

Review Activity 2

What activities occur when assessing security controls?

- ☐ Prepare the Plan of Action and Milestones (POA&M)
- ☐ Conduct final risk determination
- ☑ Develop, plan, and approve Security Assessment Plan *(correct response)*
- ☑ Prepare Security Assessment Report (SAR) *(correct response)*

Feedback: *When performing Step 4, Assess Security Controls, the Security Assessment Plan is developed, reviewed, and approved and the SAR is prepared.*

Review Activity 3

What activities occur when authorizing the system?

- ☐ Implement decommissioning strategy
- ☐ Develop, review, and approve Security Assessment Plan
- ☑ Prepare the Plan of Actions and Milestones (POA&M) *(correct response)*
- ☑ Submit security authorization package *(correct response)*

Feedback: *In Step 5, Authorize System, the POA&M is prepared and security authorization package is submitted.*

Review Activity 4

What activities occur when monitoring security controls?

- ☐ Prepare the Plan of Actions and Milestones (POA&M)
- ☐ Develop, review, and approve Security Assessment Plan
- ☑ Implement decommissioning strategy *(correct response)*
- ☑ Determine impact of changes *(correct response)*

Feedback: *In Step 6, Monitor Security Controls, the decommissioning strategy is implemented when needed and the impacts of changes are determined.*