Cybersecurity for Security Personnel

Student Guide

September 2024

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 need for cybersecurity, cybersecurity roles and responsibilities, an overview of risk management, and responsibilities of Security Personnel during the risk management process. 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 Overview

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 **DODM 5200.01**, Volume 3, DOD Information Security Program: Protection of Classified Information. It implements policy, assigns responsibilities, and provides procedures for designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information. This includes information categorized as collateral, sensitive compartmented information (SCI), and Special Access Programs (SAPs).
- The **DODI 8510.01**, Risk Management Framework for DOD Systems outlines the risk management framework that applies to DOD information technology and identifies the process to follow and specific roles and responsibilities
- The **DODM 8530.01**, Cybersecurity Activities Support Procedures establish policy, assign responsibilities, and provide procedures for DOD cyber incident response (CIR).
- The **NIST SP 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 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, October 2019:

- 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 Information System (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, October 2019:

- 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.
  - A visible element of organizational, joint, and DOD Component IT portfolios.
- 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 by ensuring the security posture of one system is not undermined by vulnerabilities of interconnected systems.

Cyberspace Defense

Cyberspace defense actions are taken within cyberspace to defeat specific threats that have breached or are threatening to breach system cybersecurity measures.
Actions include:

- Detecting, characterizing, countering, mitigating threats, such as malware, unauthorized activity, and vulnerabilities
- Restoring systems to a secure configuration

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 relative to contributions for mission outcomes, strategic goals, and objectives.
- Data will be collected to support reporting and cybersecurity management activities across the system life cycle.
- Standardized information technology tools, methods, and processes will be used to the greatest extent possible, to eliminate duplicate costs and to focus resources on creating technologically mature and verified solutions.

DOD Information

Now review DOD information categorization:

- All DOD information in electronic format will be given an appropriate level of confidentiality, integrity, and availability that reflects the importance of both information sharing and protection.

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 in DOD IS and PIT systems.
- 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 used in support of identity assurance 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 consistent with applicable DOD cybersecurity policies, standards, and architectures.
- Risks associated with global sourcing and distribution, weaknesses or flaws, and vulnerabilities introduced through faulty design, configuration, or use will be managed, mitigated, and monitored as appropriate.
- Cybersecurity requirements must be identified and included throughout the lifecycle of systems. This includes acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement of all DOD IT supporting DOD tasks and missions.

Cybersecurity Workforce

Now review the considerations for the cybersecurity workforce:

- Cybersecurity workforce functions must be identified and managed, and personnel performing cybersecurity functions will be appropriately screened and qualified.
- 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 and governed through integrated decision structures and processes.
- 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.

Security and Cybersecurity Personnel

Security and cybersecurity personnel must be able to—

- Interact with each other to ensure physical security, information security, personnel security policies and processes are reflected in the operation of cybersecurity security plans.
- Share with each other security standard operating procedures (SOPs) and any specific security requirements.

Additional Topics

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

- Cybersecurity 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 SP 800-30, Guide for Conducting Risk Assessments
- ☐ DODM 8530.01, Cybersecurity Activities Support to DOD Information Network Operations
- ☐ DODI 8510.01, Risk Management Framework
- ☐ DODI 8500.01, Cybersecurity
- ☐ DODM 5200.01 DOD Information Security Program

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.

- ☐ Create cybersecurity training programs for all personnel.
- ☐ Develop new cybersecurity concepts.
- ☐ Identify fundamental cybersecurity concepts that are related to the protection of classified and controlled unclassified information.
- ☐ Explain 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.
COMMANDER, USCYBERCOM coordinates and directs DOD Information Network (DODIN) operations and defense in accordance with the Unified Command Plan; ensures that orders addressing cybersecurity are consistent with the policy and guidance, in coordination with the DOD CIO; oversees and ensures timely implementation of international cybersecurity and cyberspace defense agreement involving the geographic combatant commands; and oversees DOD cybersecurity inspections.
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, Information System

Security Officer (ISSO) and Information System Security Manager (ISSM), Security Specialist, Security Officer, and the Risk Executive Function.
For a full list of responsibilities, refer to DODI 8500.01, Cybersecurity, available through the course resources.

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 create and update all the security policies and procedures. They should also support risk assessment and management with understanding specific security requirements. 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. It's helpful to understand the categorization of the DOD information systems within your area of responsibility. Those designations impact security and resource requirements needed to protect systems and the information processed. 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 in 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 process is executed by adhering to the Risk Management Framework (RMF). The RMF process includes seven steps:

- Prepare
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

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) 8500.01, 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 Framework process?
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
- ☐ Prepare
- ☐ Categorize
- ☐ Authorize
- ☐ Assess
- ☐ Select
- ☐ Implement

Lesson 5: Assess Risk

Introduction

Objectives

This lesson focuses on the Prepare and Categorize steps 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

RMF Steps for Security Professionals

RMF is an integrated, enterprise-wide decision structure for cybersecurity risk management. The RMF is a seven-step process.

The aim is to:

- Improve information system security.
- Strengthen the risk management process.
- Encourage reciprocity among Federal agencies.

Within the RMF there are four steps where the security professionals are directly involved in the RMF Process: Prepare, Categorize, Select, and Monitor. In these steps, security professionals assist by providing physical security, policies, and procedures to ensure that the systems are meeting the needs of the organization and mission.

Threats

Definition

The purpose of the Prepare step is to carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.
The Categorize step informs organizational risk management processes and tasks. This is done by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the nation, with respect to loss of confidentiality, integrity, and availability of systems – and the information involved in those systems.
Your responsibility as Security Personnel is to know how to assess threats to your information technology, or 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.
Within the Prepare step, there are 18 tasks. For this course, we will focus on the seven organizational level tasks and the three tasks associated with the Categorize step.

Task P-1: Risk Management Roles

Identify and assign individuals to specific roles associated with security and privacy risk management.
Primary Responsibility:

- Head of Agency
- Chief Information Officer
- Senior Agency Official for Privacy

Task P-2: Risk Management Strategy

Establish a risk management strategy for the organization that includes a determination of risk tolerance.
Primary Responsibility:

- Head of Agency

Task P-3: Risk Assessment—Organization

Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.
Primary Responsibility:

- Senior Accountable Official for Risk Management or Risk Executive (function)
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Task P-4: Organizationally-Tailored Control Baselines and Cybersecurity Framework (CSF) Profiles (Optional)

Establish, document, and publish organizationally-tailored control baselines and/or CSF profiles.
Primary Responsibility:

- Mission or business owner
- Senior Accountable Official for Risk Management or Risk Executive (function)

Task P-5: Common Control Identification

Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.
Primary Responsibility:

- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Task P-6: Impact-Level Prioritization (Optional)

Prioritize organizational systems with the same impact level.
Primary Responsibility:

- Senior Accountable Official for Risk Management or Risk Executive (function)

Task P-7: Continuous Monitoring (ConMon) Strategy—Organization

Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.

Primary Responsibility:
- Senior Accountable Official for Risk Management or Risk Executive (function)

Task C-1: System Description

Document the characteristics of the system.
Primary Responsibility:
- Information Security Officer (ISO)

Task C-2: Security Categorization

Categorize the system and document the security categorization results.
Primary Responsibility:
- ISO
- Information owner / steward

Task C-3: Security Categorization Review and Approval

Review and approve the security categorization results and decision.
Primary Responsibility:
- Authorizing Official (AO)
- AO Designated Representative (AODR)
- Senior Agency Official for Privacy

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

- List the two steps in the RMF designed to mitigate risk
- Explain the Select step of the RMF
- Explain the Implement step of the RMF

Countermeasures

Overview

After categorization occurs, the Select step of the RMF takes place. The purpose of the Select step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the nation. Within the Select step, there are six tasks.
First is control selection, followed by control tailoring, control allocation, documentation of planned control implementations, Continuous Monitoring strategy – system, and lastly, plan review and approval.

Task S-1: Control Selection

- Select control baselines necessary to protect the system commensurate with risk.
- Select the controls for the system and the environment of operation.

Primary Responsibility:

- System Owner (SO)
- Common Control Provider (CCP)

Task S-2: Control Tailoring

Tailor the controls selected for the system and the environment of operation, producing tailored control baselines.
Primary Responsibility:

- SO
- CCP

Task S-3: Control Allocation

- Controls are designated as system-specific, hybrid, or common controls.

- Controls are allocated to the specific system elements (machine, physical, or human elements) and to the environment of operation.

Primary Responsibility:

- Security Architect
- Privacy Architect
- Information System Security Officer (ISSO)
- System Privacy Officer

Task S-4: Documentation of Planned Control Implementations

Document the controls and associated tailoring actions for the system and environment of operation in security and privacy plans.
Primary Responsibility:

- SO
- CCP

Task S-5: Continuous Monitoring Strategy - System

Development of a continuous monitoring (ConMon) strategy for the system that reflects the organizational risk management strategy.
Primary Responsibility:

- SO
- CCP

Task S-6: Plan Review and Approval

Review and approve security and privacy plans to ensure they reflect the selection of controls necessary to protect the system and the environment of operation commensurate with risk.
Primary Responsibility:

- Authorizing Official (AO)
- Authorizing Official Designated Representative (AODR)

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:

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

Implement Risks Controls

Implement

The purpose of the Implement step of the RMF is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation. There are two tasks in the Implement step of the RMF.

The first task, I-1, is to implement the controls in the security and privacy plans. The implementation must be consistent with the organization's enterprise architecture and associated security and privacy architectures. It is then documented in the security and privacy plan, under the second task, Update Control Implementation Information. 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, or STIGs, or Security Requirements Guide (SRGs).

The security controls must be implemented consistently with DOD architectures and standards and employ best practices when implementing controls within the system, including the use of software engineering methodologies, security principles, and secure coding techniques. Proposed security design must be addressed in preliminary and critical design reviews. Then, the security and privacy plan is updated based on information obtained during the implementation of the controls. Lastly, existing security controls are reviewed. If they do not pose a risk, then they are inherited into the new practice.

Task I-1: Control Implementation

Implement the controls in the security and privacy plans.

Primary Responsibility:

- SO
- CCP

Task I-2: Update Control Implementation Information

Document changes to planned control implementations based on the “as-implemented” state of controls.
Primary Responsibility:

- SO
- CCP

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
- ☐ Monitor
- ☐ Select
- ☐ Authorize
- ☐ Prepare
- ☐ Implement
- ☐ Categorize

Review Activity 2

Which of the following are the activities that occur when performing the Select step of the RMF?
Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Control Allocation
- ☐ Plan Review and Approval
- ☐ Control Tailoring
- ☐ Control Selection

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.

- ☐ Seek approvals from CIO
- ☐ Create appropriate training and communication plans
- ☐ Implement controls in the security and privacy plans
- ☐ Document changes to planned control implementation

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 RMF steps related to evaluating risk are Assess, Authorize, and Monitor.
Here are the lesson objectives. Take a moment to review them.

- List the three evaluation steps in the RMF process
- Describe the Assess step
- Describe the Authorize step
- Describe the Monitor step

Associated RMF Steps

Assess Controls

The purpose of the Assess step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization. During the Assess step, an assessor or assessment team is selected, and the Security and Privacy Plans are developed, reviewed, and approved.
The Control Assessor conducts and prepares the Assessment Reports. You also need to conduct remediation actions to address deficiencies in the controls implemented in the system and environment of operation. Finally, a Plan of Action and Milestones (POA&M) is developed.

Task A-1: Assessor Selection

Select the appropriate assessor or assessment team for the type of control assessment to be conducted.
Primary Responsibility:

- Authorizing Official (AO)
- Authorizing Official Designated Representative (AODR)

Task A-2: Assessment Plan

Develop, review, and approve plans to assess implemented controls.
Primary Responsibility:

- AO or AODR
- Control Assessor

Task A-3: Control Assessments

Assess the controls in accordance with the assessment procedures described in assessment plans.
Primary Responsibility:
- Control Assessor

Task A-4: Assessment Reports

Prepare the assessment reports documenting the findings and recommendations from the control assessment.
Primary Responsibility:
- Control Assessor

Task A-5: Remediation Actions

Conduct initial remediation actions on the controls and reassess remediated controls.
Primary Responsibility:
- SO
- CCP
- Control Assessor

Task A-6: Plan of Action and Milestones (POA&M)

Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.
Primary Responsibility:
- SO
- CCP

Authorize

During the Authorize step, an authorization package is provided to the AO. The AO analyzes the package. To do this, the AO needs the:
- Security and privacy plans
- Security and privacy assessment reports
- POA&M
- Executive summary and other documentation, as required

The AO may have feedback that requires revision of the authorization package, which must then be resubmitted to the AO for review and final acceptance. The information in the authorization package is used by authorizing officials to make informed, risk-based decisions, which is then reported.

Task R-1: Authorization Package

Assemble the authorization package and submit the package to the authorizing official for an authorization decision.
Primary Responsibility:
- SO
- CCP
- Senior Agency Official for Privacy

Task R-2: Risk Analysis and Determination

Analyze and determine the risk from the operation or use of the system or the provision of common controls.
Primary Responsibility:

- AO or AODR

Task R-3: Risk Response

Identify and implement a preferred course of action in response to the risk determined.
Primary Responsibility:

- AO or AODR

Task R-4: Authorization Decision

Determine if the risk from the operation or use of the information system (IS) or the provision or use of common controls is acceptable .
Primary Responsibility:

- AO

Task R-5: Authorization Reporting

Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.
Primary Responsibility:

- AO or AODR

Monitor Security Controls

During the Monitor step, the goal is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization, in support of risk management decisions.
When a system is removed from operation, several risk management actions are required during the Monitor step. Organizations ensure that controls addressing system disposal are implemented. Examples include media sanitization, configuration management and control, component authenticity, and record retention.
Organizational tracking and management systems, including inventory systems, are updated to indicate the system that is being removed from service. Security and privacy posture reports reflect the security and privacy status of the system. Users and application owners hosted on the disposed system are notified as appropriate, and any control inheritance relationships are reviewed and assessed for impact.
The Monitor step also applies to system *elements* that are removed from operation. Organizations removing a system from operation update the inventory of information systems to reflect the removal. SOs and security personnel ensure that disposed systems comply with relevant federal laws, regulations, directives, policies, and standards.

Task M-1: System and Environment Changes

Analyze and determine the risk from the operation or use of the system or the provision of common controls.
Primary Responsibility:

- SO or CCP

- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Task M-2: Ongoing Assessments

Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring (ConMon) strategy.
Primary Responsibility:

- Control Assessor

Task M-3: Ongoing Risk Response

Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in POA&Ms.
Primary Responsibility:

- AO
- SO
- CCP

Task M-4: Authorization Package Updates

Update plans, assessment reports, and POA&Ms based on the results of the ConMon process.
Primary Responsibility:

- SO
- CCP

Task M-5: Security and Privacy Reporting

Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational ConMon strategy.
Primary Responsibility:

- SO
- CCP
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Task M-6: Ongoing Authorization

Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.
Primary Responsibility:

- AO

Task M-7: System Disposal

Implement a system disposal strategy and execute required actions when a system is removed from operation.
Primary Responsibility:

- SO

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
- ☐ Assess
- ☐ Monitor
- ☐ Authorize
- ☐ Categorize
- ☐ Implement

Review Activity 2

What activities occur when assessing 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 assessment plan (Security and Privacy Plans)
- ☐ Develop assessment reports (Security and Privacy Reports)
- ☐ Assessor selection
- ☐ Conduct control assessment
- ☐ Address deficiencies with remediation actions

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
- ☐ Develop authorization package
- ☐ Analyze and determine risk
- ☐ Implement risk response
- ☐ Make authorization decision
- ☐ Report the authorization decision

Review Activity 4

What activities occur when monitoring 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 system disposal
- ☐ Update authorization and authorization package
- ☐ Ensure ongoing assessment of control effectiveness
- ☐ Monitor system and environment changes
- ☐ Respond to ongoing risk
- ☐ Security and privacy reporting

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. Please use the Security Training, Education, and Professionalization Portal (STEPP) system from the Center for Development of Security Excellence to access the online exam.

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 SP 800-30 Guide for Conducting Risk Assessments *(correct response)*
- ☑ DODM 8530.01 Cybersecurity Activities Support to DOD Information Network Operations *(correct response)*
- ☑ DODI 8510.01 Risk Management Framework *(correct response)*
- ☑ DODI 8500.01 Cybersecurity (correct response)
- ☑ DODM 5200.01 DOD Information Security Program *(correct response)*

Feedback: *All of these are cybersecurity drivers.*

Review Activity 4

Which skills do security personnel need?

- ☐ Create cybersecurity training programs for all personnel.
- ☐ Develop new cybersecurity concepts.

- ☑ Identify fundamental cybersecurity concepts that are related to the protection of classified and controlled unclassified information. *(correct response)*
- ☑ Explain 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 explain 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 Framework process?

- ☐ 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 (correct response)
- ☑ Prepare (correct response)
- ☑ Categorize (correct response)
- ☑ Authorize (correct response)
- ☑ Assess (correct response)
- ☑ Select (correct response)
- ☑ Implement (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
- ☐ Monitor
- ☑ Select (correct response)
- ☐ Authorize
- ☐ Prepare
- ☑ Implement (correct response)
- ☐ Categorize

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

Review Activity 2

Which of the following are the activities that occur when performing the Select step of the RMF?

- ☑ Control Allocation *(correct response)*
- ☑ Plan Review and Approval *(correct response)*
- ☑ Control Tailoring *(correct response)*
- ☑ Control Selection *(correct response)*

Feedback: *These are all activities that occur during the Select step of RMF.*

Review Activity 3

What activities occur during implementation of security controls?

- ☐ Seek approvals from CIO
- ☐ Create appropriate training and communication plans
- ☑ Implement controls in the security and privacy plans *(correct response)*
- ☑ Document changes to planned control implementation *(correct response)*

Feedback: *The activities in the Implement step include implementing controls in the security and privacy plans, as well as documenting the changes to planned control implementation.*

Lesson 7 Review Activities

Review Activity 1

Which steps of the RMF are designed to evaluate risk?

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

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

Review Activity 2

What activities occur when assessing controls?

- ☐ Prepare the Plan of Action and Milestones (POA&M)
- ☐ Conduct final risk determination
- ☑ Develop assessment plan (Security and Privacy Plans) *(correct response)*
- ☑ Develop assessment reports (Security and Privacy Reports) *(correct response)*
- ☑ Assessor selection *(correct response)*
- ☑ Conduct control assessment *(correct response)*
- ☑ Address deficiencies with remediation actions *(correct response)*

Feedback: *When performing the Assess step, the activities include assessor selection, conducting the control assessment, developing assessment plans and assessment reports, and taking remediation actions.*

Review Activity 3

What activities occur when authorizing the system?

- ☐ Implement decommissioning strategy
- ☐ Develop, review, and approve Security Assessment Plan
- ☑ Develop authorization package *(correct response)*
- ☑ Analyze and determine risk *(correct response)*
- ☑ Implement risk response *(correct response)*
- ☑ Make authorization decision *(correct response)*
- ☑ Report the authorization decision *(correct response)*

Feedback: *The Authorize step includes these activities: authorization package, risk analysis and determination, risk response, authorization decision, and authorization reporting.*

Review Activity 4

What activities occur when monitoring controls?

- ☐ Prepare the Plan of Actions and Milestones (POA&M)
- ☐ Develop, review, and approve Security Assessment Plan
- ☑ Implement system disposal *(correct response)*
- ☑ Update authorization and authorization package *(correct response)*
- ☑ Ensure ongoing assessment of control effectiveness *(correct response)*
- ☑ Monitor system and environment changes *(correct response)*
- ☑ Respond to ongoing risk *(correct response)*
- ☑ Security and privacy reporting *(correct response)*

Feedback: *The Monitor step includes these activities: monitoring system and environment changes, ongoing assessment of control effectiveness, ongoing risk response, authorization package updates, security and privacy reporting, ongoing authorization, and system disposal.*