RMF Categorize Step

Student Guide

January 2023

Center for Development of Security Excellence

Table of Contents

Course Introduction

Introduction

Welcome to Risk Management Framework (RMF) Categorize Step

This course focuses on the categorize step, and by the end of the course, you will be able define the Categorize Step in the Risk Management Framework, or RMF.

The purpose of the Categorize Step is to inform organizational risk management processes and tasks by determining the adverse impact to the loss of Confidentiality, Integrity, and Availability of organizational systems, organizational operations and assets, individuals, other organizations, and the nation with respect and the information processed, stored, and transmitted by those systems.

Objectives

Before you begin, consider the following course learning objectives:

- Identify policies and guidelines for the Categorize Step in the Risk Management Framework (RMF)
- Identify the three tasks and associated inputs, outputs, roles and responsibilities in the Categorize Step

Lessons:

The course is divided into two lessons:

Lesson 1: Policies and Guidelines; and

Lesson 2: Tasks, Potential Inputs & Expected Outputs, Roles and Responsibilities.

Lesson 1: Introduction to Policies and Guidelines

Lesson Introduction

The RMF was developed as a result of a partnership between the National Institute of Standards and Technology, or NIST, the Department of Defense, or DOD, the Office of the Director of National Intelligence, or ODNI, and the Committee on National Security Systems.

In this lesson, you will learn the defining aspects of the categorize step, and the associated Policies and Guidelines.

NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View.

The purpose of **NIST Special Publication 800-39** is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations such as mission, functions, image, and reputation, organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems.

NIST SP 800-37 Revision 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. This document contains updates to the RMF, such as integration of privacy risk management processes and the incorporation of supply chain risk management processes.

Department of Defense Instruction, or DODI, 8510.01 Risk Management Framework, or RMF, DODI 8510.01 establishes the use of the RMF, an integrated, enterprise-wide decision structure for cybersecurity risk management that includes and integrates DOD Mission Areas, or MAs, in accordance with DODD 8115.01.

The CNSSI No. 1253: Security Categorization and Control Selection for National Security Systems, describes the categorization process and is a companion document to the NIST publications relevant to the Categorize Step.

The CNSS collaborates with NIST to ensure **NIST SP 800-53** contains security controls to meet the requirements of NSS and provides a common foundation for information security across the U.S. Federal Government.

This Instruction also provides NSS-specific information on developing and applying overlays for the national security community and parameter values for **NIST SP 800-53** security controls that are applicable to all.

NIST Special Publication 800-60 Volume 1 Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories contains the basic guidelines for mapping types of information and information systems to security categories.

The publication addresses the Federal Information Security Modernization Act, or FISMA, direction to develop guidelines recommending the types of information and information systems to be included in each category of potential security impact.

This guideline is intended to help agencies consistently map security impact levels to types of information and information systems.

The NIST SP 800-60 Volume 2 Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices, is intended as a reference resource rather than as a tutorial. This document describes information attributes that may result in variances from the provisional security impact level assignment. This is an important document in the Categorize Step because it describes how to establish a system security categorization.

Federal Information Processing Standards, or FIPS, Publication 199, **Standards for Security Categorization of Federal Information and information Systems.** This document is the second mandatory security standard. The Publication identifies the purpose of the Categorization Steps.

It requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.

The document provides guidance for the potential impact values assigned to the respective security objectives, which are the highest values from among the security categories that have been determined for each type of information resident on those information systems.

Federal Information Processing Standards, or FIPS, Publication 200, Minimum Security Requirements for Federal Information and Information Systems is the second mandatory security standard.

The Publication identifies the purpose of the Categorize Step by specifying the minimum-security requirements for federal information and information systems supporting the executive agencies of the Federal Government; and identifies the risk-based process for selecting the security controls necessary to satisfy the minimum-security requirement.

The CUI Registry. The CUI Registry is the government-wide online repository for federal-level guidance regarding CUI policy and practice

Review Activity

Knowledge Check 1

1. Select all that apply. Which documents discusses the purpose of the Categorization Step?
    - (a) SP 800-60 – Guide for Mapping Types of Information
    - (b) SP 800-18 – Guide for Developing Security Plans for Federal Information Systems
    - (c) FIPS 199 – Standards for Security Categorization of Federal Information Systems
    - (d) OMB FEA – Office of Management and Budget, Federal Enterprise Architecture

Lesson 1 Conclusion

Lesson Conclusion

You have completed this lesson. You should now be able to define Policy and Guidelines associated with the Categorize step.

Lesson 2: Tasks, Inputs, Outputs, Roles and Responsibilities

Introduction of Tasks

In this lesson, we will look at the Tasks, Inputs and Outputs, Roles and Responsibilities outlined in the Categorize Step. The Categorize Step includes three tasks that have an alpha designator of "**C"** preceding the task number.

Task C-1- System Description

Task C-2- Security Categorization

Task C-3- Security Categorization Review and Approval

Each task contains a set of potential inputs required to implement the tasks, and a set of expected outputs as a result.

The first categorize task to be discussed is Task C-1.

Task C-1: System Description

Task C-1 is the first of three tasks in the Categorize Step and provides:

A description of the system characteristics documented in the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for the information generated as part of the Software Development Life Cycle, or SDLC.

The level of detail in the security and privacy plans is determined by the organization and is commensurate with the Security Categorization and the security and privacy risk assessments of the system.

Information may be added to, or updated in, the system description as it becomes available during the system life cycle, during the execution of the RMF steps, and as any system characteristics change.

The System Registration information is updated with the system characterization information.

Task C-1 Potential Inputs

The Potential Inputs for Task C-1 include:

- System design and requirements documentation
- Authorization boundary information
- List of security and privacy requirements allocated to the system, system elements, and the environment of operation

- Physical or other processes controlled by system elements
- System element information
- System component inventory
- System element supply chain
- Information, including inventory and supplier information
- Security Categorization
- Data map of the information life cycle for information types processed, stored, and transmitted by the system
- Information on system use, users, and roles

Task C-1 Expected Outputs

The Expected Output of Task C-1 is the documented system description.

Task C-1 Roles and Responsibilities

The primary responsibility is carried out by the System Owner.

The system owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner is responsible for addressing the operational interests of the user community and for ensuring compliance with security requirements.

The supporting roles include the authorizing official or authorizing official designated representative; information owner or steward; system security officer; and system privacy officer.

Review Activity

Knowledge Check C-1

Try answering this question.

Information may be added to, or updated in, the System Description as it becomes available during the system life cycle

- True
- False

Task C-2: Security Categorization

Task C-2, Security Categorization is the second of three tasks in the Categorize Step.

A Security Categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed.

The Security Categorization determinations consider potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the loss of Confidentiality, Integrity, or Availability of information.

Security Categorization results are documented in the security, privacy, and Supply Change Risk Management, or SCRM, plans.

Security categorization information is documented in the System Security Plan or included as an attachment to the security plan.

Security categorization documentation can be cross-referenced in a privacy plan when the system processes Personally Identifiable Information, or PII.

Organizations have flexibility in conducting a Security Categorization:

FIPS 200 - describes a single impact level for a system based on the high-water mark concept or

CNSSI 1253 - describes three impact values that may vary for each of the security objectives of Confidentiality, Integrity, and Availability (for National Security Systems)

FIPS 199, Standards for Categorization of Federal Information publication establishes Security Categories for both information and information systems

FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (example: a loss of confidentiality, integrity, or availability)

The application of these definitions must take place within the context of each organization and the overall national interest

Potential Impact Levels

The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Details on LOW: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

(ii) (ii) result in minor damage to organizational assets;

(iii) (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

DETAILS ON MODERATE: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

(ii) (ii) result in significant damage to organizational assets;

(iii) (iii) result in significant financial loss; or

(iv) (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

DETAILS ON HIGH: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

(ii) result in major damage to organizational assets;

(iii) result in major financial loss; or

(iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries

Task C-2 Potential Inputs

To complete Task C-2, categorize the system and document the Security Categorization results. Many items are utilized in this process.

The potential inputs include:

- The Risk Management Strategy;
- Organizational Risk Tolerance;
- Authorization Boundary Information;
- Organization-and System-level risk assessment results

- Information types processed, stored, or transmitted by the system
- List of security and privacy requirements allocated to the system
- System Elements, and environment of operation
- Organizational authority or Purpose for operating the system
- Business impact analyses or criticality analyses
- Information about missions, business functions, and mission/business processes supported by the system

Task C-2 Expected Outputs

Task C-2 Expected Outputs are: Impact levels determined for each information type and for each security objective (Confidentiality, Integrity, and Availability) and security categorization based on high-water mark of information type impact levels**.**

Task C-2 Roles and Responsibilities

The Security Categorization process is carried out by the System Owner; and the Information Owner or Steward. Cooperation and collaboration between roles help to ensure that individual systems are categorized based on the Mission and Business Objectives of the organization.

The role of the System Owner and Information Owner or Steward consider the results from the security risk assessment as well as the privacy risk assessment when the system processes PII as a part of the security categorization decision

The decision is consistent with the risk management strategy.

The Primary Roles are of the System Owner and the Information Owner or Steward. We have described the System Owner roles and responsibilities previously

The Information Owner or Steward roles are responsible for establishing the rules for appropriate use and protection of the information and retains that responsibility even when the information is shared with or provided to other organizations

Information Owners or Steward provide input to System Owners regarding the security and privacy requirements and controls for the system where the information is processed, stored, or transmitted

The Supporting Roles support the Primary Roles for Task C-2

The Supporting Roles include the Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official or Authorizing Official Designated Representative; System Security Officer; and the System Privacy Officer.

Review Activity

Knowledge Check C-2

Try answering this question.

Select all that apply. Security Objectives include the following:

- Confidentiality
- Integrity
- Availability
- Deployability

Task C-3: Security Categorization Review and Approval

The Security Categorization results and decisions (completed in Task C-2) are reviewed by the authorizing official or a designated representative to ensure that the security category selected for the information system is consistent with the mission and business functions of the organization and the need to adequately protect those missions and functions.

For information systems that process PII, the Senior Agency Official for Privacy reviews and approves the Security Categorization results and decision prior to the authorizing official's review.

The authorizing official or designated representative reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with the categorization decisions for all other organizational systems.

The authorizing official collaborates with the senior accountable official for risk management or the risk executive (function) to ensure that the categorization decision for the system is consistent with the organizational risk management strategy and satisfies requirements for high value assets.

If the security categorization decision is not approved, the system owner initiates steps to repeat the categorization process and resubmits the adjusted results to the authorizing official or designated representative.

System registration information is subsequently updated with the approved security categorization information.

Task C-3 Potential Inputs

Task C-3 Potential Inputs include:

Impact levels determined for each information type and for each security objective (Confidentiality, Integrity, Availability); Security categorization based on high-water mark of information type impact levels; List of the high-value assets for the organization.

Task C-3 Expected Output

Task C-3 expected output is the approval of security categorization for the system.

Task C-3 Roles and Responsibilities

Primary Roles

The Primary Responsibility for Task C-3 is the Authorizing Official, or the AO, or the Authorizing Official Designated Representative, or AODR; Senior Agency Official for Privacy.

The AO is a senior official or executive with the authority to formally assume responsibility for operating a system, providing common controls inherited by organizational systems, or using a system, service, or application from an external provider.

The Authorizing officials collaborates with common control providers, system owners, Chief Information Officer, Senior Agency Information Security Officers, and other interested parties during the authorization process

The Senior Agency Official for Privacy is the senior official or executive with agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risk.

The role of Senior Agency Official for Privacy is an inherent U.S. Government function and is therefore assigned to Government personnel only.

The supporting roles for Task C-3 are the Senior Accountable Official for Risk Management or the Risk Executive (Function); the Chief Information Officer, and the Senior Agency Information Security Officer.

Review Activity

Knowledge Check C-3

Try answering this question.

The Authorizing Official (AO) formally assumes the risk for:

- The responsibility and accountability for operating a system
- The responsibility and accountability for identifying a system
- The responsibility and accountability for updating a system
- The responsibility and accountability for preparing a system

You have completed this lesson; you should now be able to define to:

- Select Step Tasks
- Potential Inputs and Expected Outputs
- Roles and Responsibilities associated with each Task

Course Conclusion

Conclusion

Congratulations, you have completed the RMF Categorize Step course.
You should now be able to identify:

- Policies and guidelines for the Categorize Step in the Risk Management Framework (RMF)
- The three tasks and associated inputs, outputs, roles, and responsibilities in the Categorize Step

For more information on the RMF Categorize Step, please visit the Resources link.

Course Credit

To receive credit for this course, you must take the course assessment.

To access the assessment:

Select Exit to return to the course page

Select Launch Exam to begin the online assessment

Appendix A: Answer Key

Lesson 1: Review Activity

Knowledge Check 1– Policies and Guidelines

1. Select all that apply. Which documents discusses the purpose of the Categorization Step?
   ☒ SP 800-60 – Guide for Mapping Types of Information
   ☐ (b) SP 800-18 – Guide for Developing Security Plans for Federal Information Systems
   ☒ (c) FIPS 199 – Standards for Security Categorization of Federal Information Systems
   ☐ (d) OMB FEA – Office of Management and Budget, Federal Enterprise Architecture

Correct Feedback: *SP 800-60 – Guide for Mapping Types of Information, and FIPS 199 – Standards for Security Categorization of Federal Information Systems discuss the purpose of the Select Step*.

Lesson 2: Review Activity

Knowledge Check C-1

2. Information may be added to, or updated in, the System Description as it becomes available during the system life cycle.
   ☒ True
   ☐ False

Correct Feedback: *Information may be added to, or updated in, the System Description as it becomes available during the system life cycle.*

Knowledge Check C-2

3. Select all that apply. Security Objectives include the following:
   ☒ Confidentiality
   ☒ Integrity
   ☒ Availability
   ☐ Deployability

Correct Feedback: Confidentiality, Integrity, and Availability are the three security objectives

Knowledge Check C-3

4. The Authorizing Official (AO) formally assumes the risk for:
   ☒ The responsibility and accountability for operating a system
   ☐ The responsibility and accountability for identifying a system

The responsibility and accountability for updating a system
The responsibility and accountability for preparing a system

Correct Feedback: The AO is a senior official or executive with the authority to formally assume responsibility for operating a system, providing common controls inherited by organizational systems, or using a system, service, or application from an external provider.