RMF Authorize Step

Student Guide

May 2023

Center for Development of Security Excellence

Table of Contents

Course Introduction

Introduction

Welcome to Risk management Framework, or RMF, Authorize Step.

This course focuses on the Authorize Step, and by the end of the course, you will be able to define the Authorize Step in the RMF.

The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk, including supply chain risk, to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system, or the use of common controls is acceptable.

Objectives

Before you begin, consider the following course learning objectives.

- Describe the purpose of the Authorize Step in the Risk Management Framework (RMF)
- Identify tasks, inputs and outputs, roles and responsibilities within the Authorize Step.

Lessons:

The course is divided into two lessons:

Lesson 1: RMF Authorize Step: Policies and Guidelines

Lesson 2: Authorize Step Tasks, Inputs & 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 Authorize step, and the associated policies and guidelines.

The purpose of **NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System** 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 contains updates to the RMF, such as the integration of privacy risk management processes and the incorporation of supply chain risk management processes.

NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments provides guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39.

This policy provides guidance for carrying out each of the steps in the Risk Assessment Process, such as preparing for the assessment, conducting the assessment, and communicating the results of the assessment.

DODI 8510.01, Risk Management Framework for DOD Systems establishes the use of the RMF, an integrated enterprise-wide decision structure for cybersecurity risk management that includes and integrates DOD mission areas (MAs) in accordance with DODD 8115.01, Information Technology Portfolio Management and DODI 8510.01

CNSSI 1253 Security Categorization and Control Selection for National Security Systems (NSS) describes the process of the categorization process.

The *CNSSI No. 1253* is a companion document to the NIST publications relevant to the Categorize Step.

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

This Instruction also provides National Security Systems 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 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: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, this document is a reference resource rather than a tutorial. This document discusses information attributes that may result in variances from the provisional security impact level assignment. This is an important document because it describes how to establish a system security categorization based on the systems' use, connectivity, and aggregate information content.

Federal Information Processing Standards (FIPS) Publication 199 Standards for Security Categorization of Federal Information and Information Systems. This document identifies the purpose of the Authorize step. 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.

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

FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems is the second of the mandatory security standards. This publication identifies the purpose of the Authorize steps.

It specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal Government.

It also identifies the risk-based process for selecting the Security Controls necessary to satisfy the minimum-security requirements.

Review Activity

Knowledge Check 1

The purpose of the Authorize Step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system, or the use of common controls is acceptable.

- ○ True
- ○ False

Lesson 1 Conclusion

Lesson Conclusion

You have completed this lesson. You should now be able to define policy and guidelines associated with the Authorize 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 Authorize Step. The Authorize Step includes five tasks, which have an alpha designator of **"R"** preceding the task number.

- R-1: Authorization Package
- R-2: Risk Analysis and Determination
- R-3: Risk Response
- R-4: Authorization Decision
- R-5: Authorization Reporting

Each task contains a set of inputs that are required to implement the tasks and a set of outputs as a result.

The first Authorized Task to be discussed is Task R-1

Task R-1: Authorization Package

Task R-1 is the first of five tasks in the Authorize Step. This task assembles the authorization package and submits the package to the authorizing official, or AO, for an authorization decision.

Authorization packages include:

- Security Plans
- Privacy Plans

- Security Assessment Reports
- Privacy Assessment Reports
- Plan on Action & Milestones
- Executive Summary

A Senior Agency Official for Privacy reviews the authorization package for systems that process Personally Identifiable Information, or PII.

The information in the authorization package is used by AOs to make informed, risk-based decisions**.**

The authorization package may be provided to the AO in ***hard copy, electronically, or may be generated using an automated security/privacy management and reporting tool.***

When an information system is under ongoing authorization, the authorization package is presented to the AO via automated reports.

The assessment reports presented to the AO include information about deficiencies in ***system-specific, hybrid, and common controls***.

Task R-1 Potential Inputs

Potential Inputs include:

- Security and privacy plans
- Security and privacy assessment reports
- Plan of action and milestones
- Supporting assessment evidence
- Other documentation as required.

Task R-1 Expected Outputs

The expected output for Task R-1 is an authorization package with an executive summary, which may be generated from a security or privacy management tool for submission to the AO.

Task R-1 Roles and Responsibilities

The primary responsibility for Task R-1 is carried out by ***the System Owner, Common Control Provider, and Senior Agency Official for Privacy.***

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.

The Common Control Provider is an individual, group, or organization that is responsible for the implementation, assessment, and monitoring of common controls.

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 R-1 include the:

- System Security Officer
- System Privacy Officer
- Senior Agency Information Security Officer
- Control Assessor.

Review Activity

Knowledge Check 2

Try answering this question.

When an information system is under ongoing authorization, the authorization package may be presented to the AO via automated reports.

○ True

○ False

Task R-2: Risk Analysis and Determination

Task R-2 is the second of the five tasks in the Authorize Step. The task description is to analyze and determines the risk from the operation or use of the system, or the provision of common controls.

The AO or designated representative, in collaboration with the senior agency information security officer and the senior agency official for privacy for information systems processing PII, analyzes the information in the authorization package provided by the control assessor, system owner, or common control provider, and finalizes the determination of risk.

The AO analyzes the information provided by the Senior Accountable Official for Risk Management or Risk Executive Function and Information provided by the System Owner or Common Control Provider in the authorization package when making a risk determination.

They also analyze the relevant security and privacy information provided by the automated security or privacy management and reporting tool to determine the current security and privacy posture of the system.

Risk assessments are employed to provide information that may influence the risk analysis and determination informed by the **NIST Internal Report 8062 "An Introduction to Privacy Engineering and Risk Management in Federal Systems, January 2017."**

When the system is operating under an ongoing authorization, the risk determination task is effectively unchanged.

Task R-2 Potential Inputs

Task R-2, inputs include:

- Authorization package
- Supporting assessment evidence or other documentation as required
- Information provided by the senior accountable official for risk management or risk executive function
- Organizational risk management strategy and risk tolerance
- Organization- and system-level risk assessment results.

Task R-2 Expected Outputs

The expected output for Task R-2 is:

- Risk determination.

Task R-2 Roles and Responsibilities

The primary responsibility for Task R-2 is carried out by the ***Authorizing Official (AO)*** or the ***Authorizing Official Designated Representative (AODR).***

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

The AODR is an organizational official who is empowered to act on behalf of the AO to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations.

This includes carrying out many of the activities related to the execution of the RMF. The only activity that ***cannot be*** delegated by the AO to the designated representative is the authorization decision and signing of the associated authorization decision document, i.e., the acceptance of risk.

The supporting roles for Task R-2 include the:

- Senior Accountable Official for Risk Management or Risk Executive Function
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy.

Review Activity

Knowledge Check 3

Try this question.

When the system is operating under an ongoing authorization, the risk determination task is effectively unchanged?

- True
- False

Task R-3: Risk Response

Task R-3 is the third of the five tasks in the Authorize Step. The task description is to identify and implement a preferred course of action in response to the risk determined.

After risk is analyzed and determined, organizations can respond to risk in a variety of ways, including

Acceptance of risk (Deficiencies found during assessment remain documented and monitored for changes to risk factors) and

Mitigation of risk (Planned mitigation actions are included and tracked in a Plan of Action and Milestones (POA&M)).

Existing risk assessment results and risk assessment techniques may be used to help determine the preferred course of action for the risk response.

Control reassessments determine the extent to which remediated controls 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.

Risk assessors update the assessment reports with the findings from the reassessment, but do not change the original assessment results.

Because the AO is the only person who can accept risk, they are responsible for reviewing the assessment reports and plans of action and milestones and determining whether the identified risks need to be mitigated prior to authorization.

Decisions on the most appropriate course of action for responding to risk may include some form of prioritization. Some risks may be of greater concern to organizations than others. In that case, more resources may need to be directed at addressing higher-priority risks versus lower-priority risks.

- Greater risk = more allocated resources
- Lower risk = fewer allocated resources

Prioritizing risk response does not necessarily mean that the lower-priority risks are ignored. Rather, it could mean that fewer resources are directed at addressing the lower-priority risks, or that the lower-priority risks are addressed later.

A key part of the risk-based decision process is the recognition that regardless of the risk response, there remains a degree of residual risk.

Organizations determine acceptable degrees of residual risk based on organizational risk tolerance.

Task R-3 Potential Inputs

Task R-3, potential inputs include:

- Authorization package
- Risk determination
- Organization- and system-level risk assessment results

Task R-3 Expected Outputs

The Expected Outputs for Task R-3 include:

- Risk responses for determined risks.

Task R-3 Roles and Responsibilities

The Primary Responsibility for the Task R-3 carried out by the AO or the AO- designated representative (AODR).

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

The AODR is an organizational official who is empowered to act on behalf of the authorizing official to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations.

This includes carrying out many of the activities related to the execution of the RMF. The ***only activity that cannot be*** delegated by the authorizing official to the designated representative is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk).

The supporting roles include the:

- Senior Accountable Official for Risk Management or Risk Executive Function
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy
- System Owner or Common Control Provider
- Information Owner or Steward
- Systems Security Engineer
- Privacy Engineer; System Security Officer
- System Privacy Officer.

Review Activity

Knowledge Check 4

Risk assessors update assessment reports and the original assessment results

- ○ True
- ○ False

Task R-4: Authorization Decision

This task is the fourth of the five tasks in the Authorization Step.

The task description is to determine if the risk from the operation, or use of the information system, or the provision or use of common controls is acceptable.

The explicit acceptance of risk is the responsibility of the AO and cannot be delegated to other officials within the organization.

The AO consults with the ***Senior Accountable Official*** for ***Risk Management*** or the ***Risk Executive Function*** prior to making the final authorization decision for the information system or the common controls.

The AO conveys the authorization decision to the ***system owner*** or ***common control provider***, and ***others, as appropriate.***

The AO considers many factors when deciding if the risk to the organization's operations including ***mission, functions, image, reputation, and assets, individuals, other organizations, or the Nation,*** is acceptable.

The authorization decisions for individual systems consider the current residual risk, organizational plans of action and milestones, and the risk tolerance of the organization.

When the system is operating under ongoing authorization, the AO continues to be responsible and accountable for explicitly understanding and accepting the risk of continuing to operate, or use the system, or continuing to provide common controls for inheritance.

For systems, the authorization decision indicates to the system owner whether the system is.

- Authorized to operate or authorized to use,
- Not authorized to operate or not authorized to use.

For common controls, the ***authorization decision indicates*** to the common control provider and to the system owners of inheriting systems whether ***the common controls*** are ***authorized to be provided*** or ***not authorized to be provided.***

The terms and conditions for the common control authorization provide

- A description of any specific limitations or restrictions placed on the operation of the system or
- The controls that must be followed by the system owner or common control provider.

The organization determines the level of formality for the process of communicating and acknowledging continued risk acceptance by the AO.

Task R-4 Potential Inputs

Task R-4 inputs, include:

Risk responses for determined risks.

Task R-4 Expected Outputs

Task R-4 expected outputs, include:

- Authorization to operate, authorization to use, common control authorization
- Denial of authorization to operate, denial of authorization to use, denial of common control authorization.

Task R-4 Roles and Responsibilities

The primary responsibility for Task R-4 is carried out by the Authorizing Official, or AO. The AO is a senior official or executive with the authority to

- Formally assume responsibility and accountability for operating a system
- Provide common controls inherited by organizational systems
- Use a system, service, or application from an external provider.

Supporting roles for Task R-4 include:

- 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 Designated Representative

Review Activity

Knowledge Check 5

Try answering this question.

Select all that apply. Prior to making the final authorization decision, the AO consults with the _____________ or ______________:

○ Senior Accountable Official for Risk Management
○ Risk Executive (Function)
○ Senior Agency Information Security Officer
○ Senior Agency Official for Privacy

Task R-5: Authorization Reporting

This is the fifth and last task of the Authorize step. The task description is to report the authorization decision and any deficiencies in control that represent significant security or privacy risk.

AOs report authorization decisions for systems and common controls to designated organizational officials so the individual risk decisions can be viewed in the context of organization-wide security and privacy risk to organizational operations and assets, individuals, other organizations, and the Nation.

The AO also reports exploitable deficiencies, i.e., vulnerabilities, in the system or controls noted during the assessment and continuous monitoring that represent significant security or privacy risk.

Authorization decisions may be tracked and reflected as part of the organization-wide system registration process at the organization's discretion.

Task R-5 Potential Inputs

Potential Inputs for Task R- 5 include.

- The Authorization decision.

Task R-5 Expected Outputs

Outputs from this step includes:

- A report indicating the authorization decision for a system or set of common controls and annotation of authorization status in the organizational system registry.

Task R-5 Roles and Responsibilities

The Primary Responsibility for Task R-5 carried out by the AO or the AO- designated representative (AODR).

The AO is a senior official or executive with the authority to:

- Formally assume responsibility and accountability for operating a system
- Provide common controls inherited by organizational systems
- Use a system, service, or application from an external provider.

The AODR is a designated representative is an organizational official who is ***empowered to act on behalf of the AO*** to ***coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations.***

This includes carrying out many of the activities related to the execution of the RMF. The only activity that ***cannot be delegated*** by the AO to the AODR is the ***authorization decision and signing of the associated authorization decision document, i.e., the acceptance of risk.***

Supporting roles for Task R-5 include:

- System Owner or Common Control Provider
- Information Owner or Steward
- System Security Officer
- System Privacy Officer
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy

Review Activity

Knowledge Check 6

Try answering this question.

Authorization decisions may be tracked and reflected as part of the organization-wide system registration process at the organization’s discretion.

- True

- ○ False

Lesson 2 Conclusion

Lesson Conclusion

You have completed the Authorize Step Roles and Responsibilities lesson.

You should now be able to define Authorize Step Tasks, Potential Inputs and Expected outputs, and Roles and Responsibilities associated with each task.

Course Conclusion

Conclusion

Congratulations on completing the RMF Authorize Step course. You should now be able to:

Course Learning Objectives:

- Describe the purpose of the Authorize Step in the Risk Management Framework (RMF)
- Identify tasks, inputs and outputs, roles and responsibilities within the Authorize Step.

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

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

Appendix A: Answer Key

Lesson 1: Review Activity

Knowledge Check 1– Policies and Guidelines

The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system, or the use of common controls is acceptable.

- **True**

- False

Feedback: *The purpose of the Authorize Step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system, or the use of common controls is acceptable.*

Lesson 2: Review Activity

Knowledge Check 2, Task R-1

When an information system is under ongoing authorization, the authorization package may be presented to the AO via automated reports.

☒ **True**
☐ False

Feedback: *When an information system is under ongoing authorization, the authorization package may be presented to the authorizing official via automated reports.*

Knowledge Check 3, Task R-2

When the system is operating under an ongoing authorization, the risk determination task is effectively unchanged.

☒ **True**
☐ False

Feedback: *When the system is operating under an ongoing authorization, the risk determination task is effectively unchanged.*

Knowledge Check 4, Task R-3

Risk assessors update assessment reports and the original assessment results.

☐ True
☒ **False**

Feedback: *Risk assessors update assessment reports but do not change original assessment results.*

Knowledge Check 5, Task R-4

Select all that apply.
Prior to making the final authorization decision, the AO consults with the _____________ or ______________:

☒ Senior Accountable Official for Risk Management
☒ Risk Executive (Function)
☐ Senior Agency Information Security Officer
☐ Senior Agency Official for Privacy

Feedback: *Prior to making the final authorization decision, the AO consults with the Senior Accountable Official for Risk Management or the Risk Executive (Function)*

Knowledge Check 6, Task R-5

Authorization decisions may be tracked and reflected as part of the organization-wide system registration process at the organization's discretion

☒ **True**
☐ False

Feedback: *Authorization decisions may be tracked and reflected as part of the organization-wide system registration process at the organization's discretion*