

# RMF Stage 5 - Authorizing Information Systems

Reading  
1h

✓ Status Incomplete

## Introduction

In this reading, you will learn about the fifth stage of the RMF, *Authorizing Information Systems*, also known as *Authorize*, as shown below:

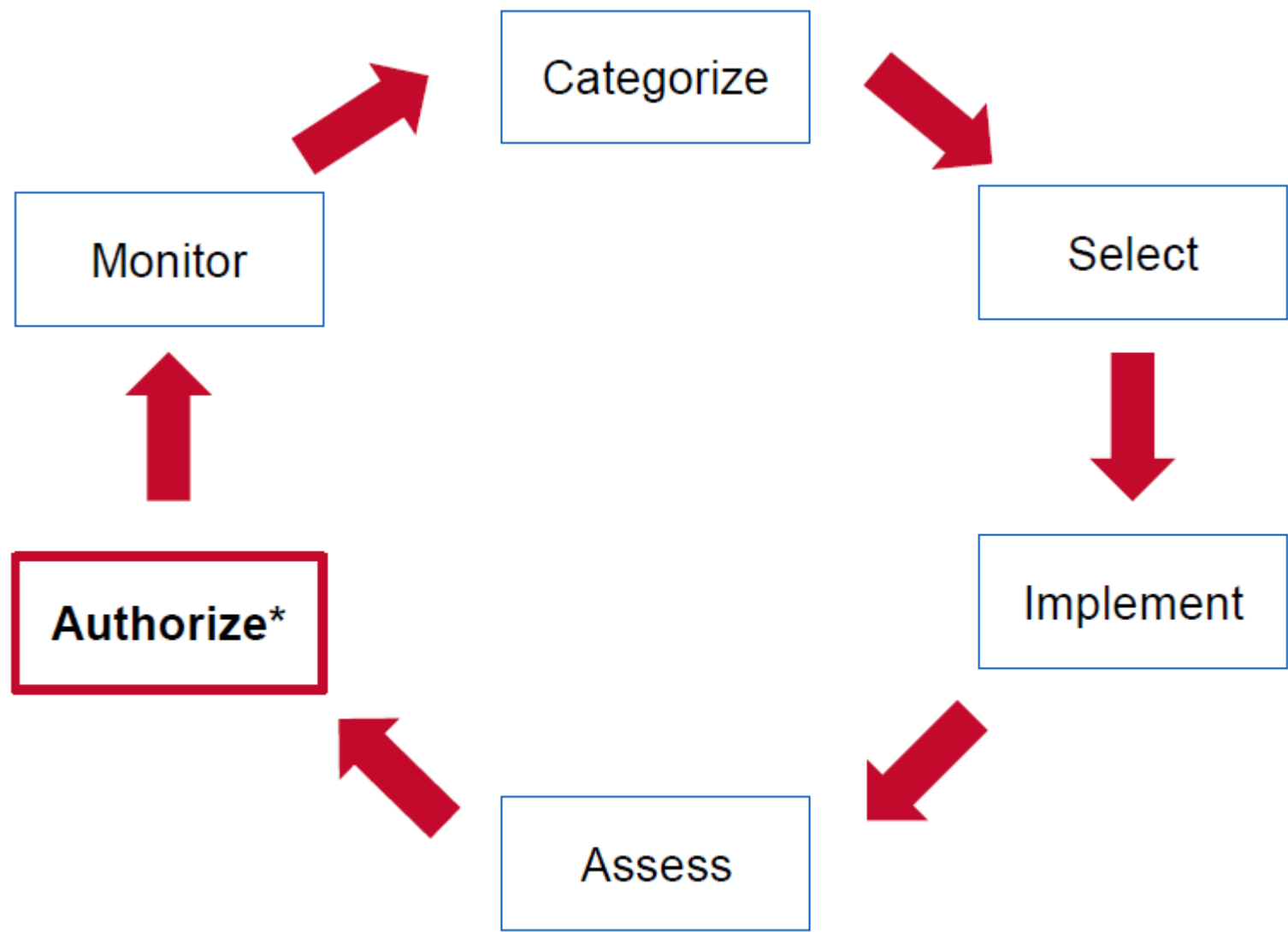


Figure 1: RMF – Authorize. Source: NIST SP 800-37

# Reading

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

**i** **What is the purpose of the Authorize Step?**

According to NIST, federal systems must be authorized before being promoted to production (i.e., becoming operational). The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official (authorizing official) to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation is acceptable based on the operation of a system or the use of common controls.

As with every RMF stage, the **Authorize** stage also includes a series of tasks:

1. Finalize POA&M
2. Assemble authorization package
3. Perform risk determination
4. Make a risk acceptance decision

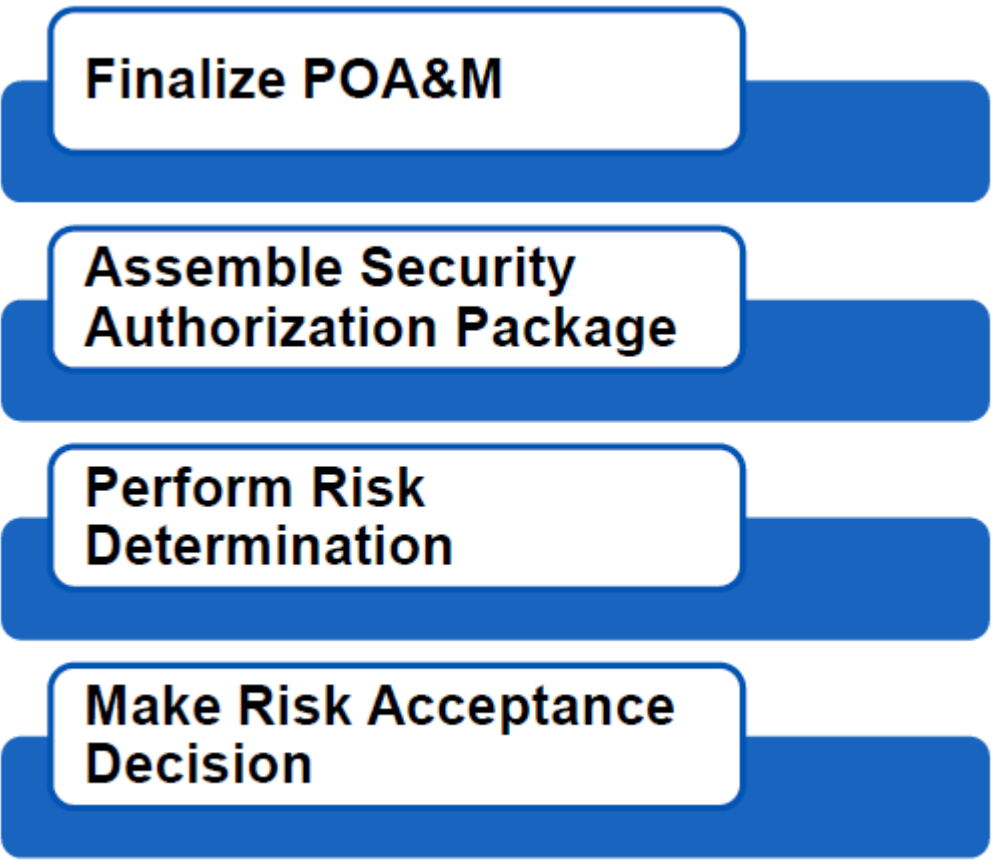


Figure 2: Key Tasks in RMF Authorize Stage (Source: NIST SP 800-37)

## Task 1: Finalize POA&M

The **POA&M** is compiled by ISO where further additions and adjustments are done by validators. It is almost always delegated to ISSO and includes the following:

- Description of deficiencies on a per-control basis
- Corrective action to be taken
- Resources required to implement
- Estimated completion date
- Mitigations reducing risk
- Estimate of residual risk

Some organizations document only non-compliant controls that must be corrected where their **SCA** has the final word on Risk Assessment of non-compliant or ineffective controls.

## Task 2: Assemble Authorization Package

Consider the following key points regarding the second task *Assemble Authorization Package*:

- Security authorization package must contain:
- Security plan
- Security assessment report
- POA&M
- If you are inheriting common controls from an Enclave, include the Authorization Package from Enclave. Also, Guest System inherits residual risk of Enclave which must be included in final Risk Assessment. Authorization Official (AO) must accept all sources of risk.
- Under NIST SP 800-53, when an organization is inheriting common controls from an Enclave, the Authorization Package from the Enclave should be included. This is because common controls are typically implemented in a shared environment, such as a data center or cloud computing environment. Therefore, it is important to understand how the controls are implemented and assessed in the Enclave, as this can impact the effectiveness of the controls in the organization.
- Additionally, when a Guest System inherits controls from an Enclave, it also inherits any residual risks associated with those controls. These residual risks must be included in the final Risk Assessment of the Guest System. The AO responsible for approving the Risk Assessment must accept all sources of risk, including those inherited from the Enclave.
- Authorization Package may be customized by AO to satisfy organizational needs, such as Risk Assessment briefing, architecture assessment, proposed operating conditions, etc.
- Under NIST SP 800-53, the Authorization Package is a collection of documents and artifacts that provide evidence to support the authorization decision. These documents typically include a security plan, Risk Assessment report, security assessment report, POA&M, and any other relevant documents that support the security posture of the system.
- The AO is responsible for approving the authorization decision, based on the evidence presented in the Authorization Package. However, the AO may customize the Authorization Package to satisfy the specific needs of the organization. For example, the AO may require a briefing on the Risk Assessment, an assessment of the system architecture, or proposed operating conditions.
- Customizing the Authorization Package allows the organization to tailor the evidence presented to the AO to better address the specific security concerns of the organization. This can help ensure that the authorization decision is based on a comprehensive understanding of the security posture of the system, as well as the specific needs and concerns of the organization.
- In summary, the Authorization Package is a collection of documents that provide evidence to support the authorization decision. The AO may customize the Authorization Package to satisfy the specific needs of the organization, such as Risk Assessment briefings, architecture assessments, proposed operating conditions, and other relevant documents. Customizing the Authorization Package allows the organization to better address the specific security concerns of the organization and ensure a comprehensive authorization decision.

## Task 3: Perform Risk Determination

This task has two sub-steps, estimating residual risk and finalizing system Risk Assessment, as explained below:

### Estimate Residual Risk

- SCA issues *Security Assessment Report (SAR)* which includes:
  - Residual risk from non-compliant or ineffective controls
  - List of deficiencies and remediation (POA&M)
- ISO may provide addendum to SAR. The ISO:
  - Rebuts specific control assessment findings
  - Provides clarifying information on system environment or operation
  - Describes remediation actions already underway and planned

### Finalize System Risk Assessment

Under Task 3, Performing Risk Determination in NIST SP 800-53, the Finalize System Risk Assessment step involves consolidating all sources of risk identified during the Risk Assessment process. Two sources of system risk that are specifically mentioned are:

1. **Non-compliant/ineffective controls:** each control that is determined to be non-compliant or ineffective contributes to the overall system risk. This means that if a control is not properly implemented or fails to provide the intended security function, it increases the likelihood and potential impact of a security event.
2. **Residual risk from common control providers:** common controls are controls that are implemented and maintained by a third-party organization, such as a cloud service provider or data center. When an organization utilizes common controls, they inherit residual risk associated with those controls. This residual risk must be assessed and included in the final system Risk Assessment.

In summary, the Finalize System Risk Assessment step involves consolidating all sources of risk identified during the Risk Assessment process, including non-compliant/ineffective controls and residual risk from common control providers. By considering all sources of risk, the organization can make informed decisions on how to mitigate and manage risks to the system.

## Task 4: Make a Risk Acceptance Decision – Basis for Authorization

Under Task 4, Make a Risk Acceptance Decision - Basis for Authorization in NIST SP 800-53, the AO makes an authorization decision based on the evidence presented in the Authorization Package. The following are the three authorization options available to the AO:

- **Authority To Operate (ATO):** the AO grants an ATO when the system meets the security requirements and is authorized to operate within its expected operating environment.
- **Interim Authority To Test (IATT):** the AO grants an IATT when the system is not fully compliant with security requirements but can be authorized to operate in a limited capacity for testing purposes.
- **Denial of Authority To Operate (DATO):** the AO denies authorization when the system does not meet the security requirements and is not authorized to operate.

In addition to the three authorization options, the AO may also refer the authorization decision to the CIO when the Risk Assessment exceeds the AO's risk threshold. This means that if the risks associated with the system are higher than the AO is authorized to accept, the decision is escalated to the CIO for authorization.

Finally, when two systems have interdependent security and each system has its own risks as well as shared risks, the AO may make a joint authorization decision. This involves coordinating with the other system's AO to ensure that the security controls and risks associated with both systems are taken into account before making an authorization decision.

In summary, the AO has three authorization options available: ATO, IATT, and DATO. If the risks associated with the system exceed the AO's risk threshold, the decision may be referred to the CIO. When two systems have interdependent security, the AO may make a joint authorization decision with the other system's AO.

The authorization options specified above have been explained in more detail below:

### ATO

Task 4 of this framework involves making a risk acceptance decision, which is the basis for authorization. The explanation given below refers to the concept of ATO, which is the official authorization to operate a system.

- ATO is issued by an AO: the ATO is granted by an AO who has the authority to make decisions regarding the security of the system. The AO is responsible for assessing the system's risk and determining whether it is acceptable to operate the system based on its security posture.
- System must comply with security posture described in the SSP: the SSP is a document that outlines the security controls and safeguards implemented in the system. The system must comply with the security posture described in the SSP, which includes the deployment, operation, and sustainment of the system.
- System must maintain an acceptable security posture: the system must maintain an acceptable security posture by implementing configuration management and vulnerability management. Configuration management involves maintaining the system's current state and ensuring that changes are authorized and documented. Vulnerability management involves identifying and mitigating vulnerabilities in the system.
- Type ATO: Type ATO authorizes the deployment of identical copies of a system. This eliminates duplicative effort and ensures that the operation, environment, and threats match the original system. This type of ATO is useful when multiple instances of a system are needed to support the mission.

## IATT

Under NIST SP 800-53, task 4 involves making a risk acceptance decision, which is the basis for authorization. An IATT is a type of temporary authorization that allows a system to undergo testing and evaluation before it is fully authorized for operation.

An IATT is typically granted when a system is undergoing significant changes or upgrades that affect its security posture. It allows the system to be tested in a controlled environment to determine its effectiveness in mitigating risk and meeting security requirements.

During the IATT period, the system is subject to continuous monitoring and evaluation. The results of the testing are used to identify any weaknesses or vulnerabilities that need to be addressed before the system can be fully authorized for operation.

Once the testing and evaluation are complete, the system may be granted an ATO if it meets the required security posture and has an acceptable level of risk. The IATT is then replaced by the ATO, which grants permission to operate the system.

## DATO


DATO is appropriate when risk outweighs benefits. Note, DATO is difficult to overcome and should never be a surprise. SCA is generally aware of AO risk tolerance and informally advises PM/SM to address significant security defects.

## Authority to Connect (ATC)

Interconnected systems, such as Enclave and other Guest Systems, share risk. Interconnections require ATC based on *ATO* (acceptance of risk) and *POA&M enumeration of non-compliant controls*.

In case of *POA&M enumeration of non-compliant controls*, authority is given to the IT security team to control and assess compliance with Cyber Security regulations by creating a POA&M that identifies non-compliant controls. The POA&M should include enumeration of each control, the severity of its non-compliance, and recommendations for how to address it. The IT security team is responsible for monitoring and reporting on the progress of any remediation efforts and updating the POA&M accordingly.

Enclave AO typically grants ATC; ATC may be granted to all instances of a system type. Also, ATC may be conditional (e.g., additional boundary defenses between guest and Enclave).

 ISO 27010, Information Security Management for Inter-Sector and Inter-Organizational Communications, defines the process for sharing sensitive information within a community of trust.

## Key Roles During the Authorize Stage

- **ISO** establishes operational significance of the system:
  - Basis for accepting risk
  - Establishes maximum acceptable risk
- **AO** makes authorization decision:
  - Weighs operational and security risk
  - Cannot exceed authorized risk threshold
  - As Enclave AO, grants ATC
- **CIO** makes authorization decisions for systems with residual risk that exceeds AO risk threshold; these systems typically have high benefit and high risk.

## Key Takeaways

- The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security to organizational operations and assets, individuals, etc. is acceptable based on the operation of a

system or the use of common controls.

- Key tasks in the RMF Authorize stage are: finalize POA&M, assemble Authorization Package, perform risk determination, and make a risk acceptance decision.

# Conclusion

In this reading, you learned about the fifth stage of the RMF (Authorize). Before you jump to the last and final stage of the RMF (Monitor), you will do an exercise as your next activity where you perform residual Risk Assessment.

# Further Readings

- Read pages 34-37 of the *Guide for [Applying the Risk Management Framework to Federal Information Systems](#)* prepared by NIST to get an in-depth understanding of the key tasks at the Authorize stage.
- Read [NIST RMF QSG: Authorize Step FAQs](#) to access frequently asked questions related to the RMF Assess stage.

✓ Mark Completed

←

Previous  
GRC Quiz 2

Next  
Conducting Residual Risk Assessment

→

## How well did this activity help you to understand the content?

Let us know how we're doing



## W05D1

Mon Jul 22

> Lectures (1)

✓ Work (8)

7 hrs

</> [Risk Management Methodology Document](#)

[RMF Stage 4 – Assessing Controls \(Part One\)](#)

[RMF Stage 4 – Assessing Controls \(Part Two\)](#)

? [GRC Quiz 2](#)

[RMF Stage 5 - Authorizing Information Systems](#)

</> [Conducting Residual Risk Assessment](#)

[RMF Stage 6 - Monitoring Security Controls](#)

[Writing Statement of Applicability \(SOA\)](#)

