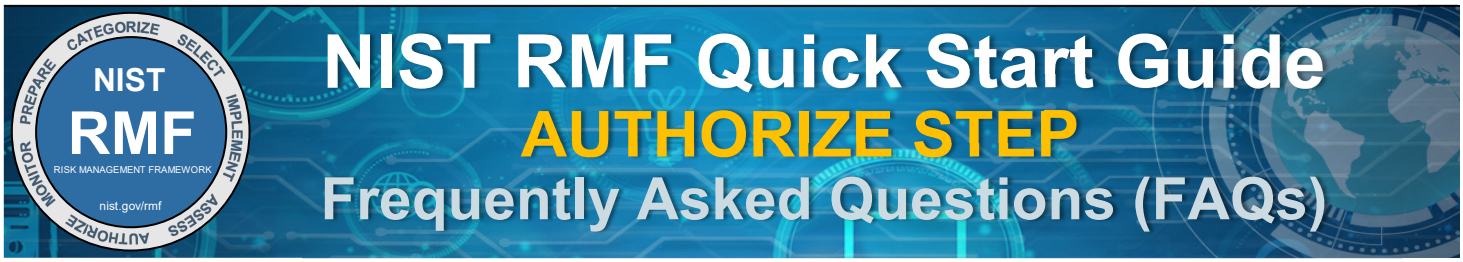
NIST RMF Quick Start Guide
AUTHORIZE STEP
Frequently Asked Questions (FAQs)

NIST Risk Management Framework (RMF) Authorize Step

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. The senior agency official for privacy is required to review authorization materials for systems that process personally identifiable information. Before a system is put into operation (or continues to operate), a valid authorization to operate is required.

Contents



General Authorize Step FAQs

1. What has been modified from NIST SP 800-37, Rev. 1, to NIST SP 800-37, Rev. 2, for the Authorize step?

The following modifications have been made from NIST SP 800-37, Revision 1 [SP 800-37r1], to NIST SP 800-37, Revision 2 [SP 800-37r2], in the Authorize step:

- The *Plan of Action and Milestones* moved to the Assess step (Task A-6) since it describes the actions that are planned to correct deficiencies in the controls identified during the assessment of the controls.
- The *Risk Determination* task was renamed *Risk Analysis and Determination* (Task R-2) to reflect that both a risk analysis and a risk determination are conducted.
- *Risk Response* (Task R-3), *Authorization Decision* (Task R-4), and *Authorization Reporting* (Task R-5) – previously combined as a single task in NIST SP 800-37, Rev. 1 – are now individual tasks in Rev. 2 (they are not new tasks) to specifically highlight these key authorization outcomes.
- Privacy elements and roles for systems processing personally identifiable information have been added as a direct response to Office of Management and Budget (OMB) Circular A-130 [OMB A130], which requires agencies to implement the Risk Management Framework and integrate privacy processes into the RMF process. In establishing requirements for security and privacy programs, the OMB Circular emphasizes the need for both programs to collaborate on shared objectives. [Back to Table of Contents]

2. What is the purpose of the Authorize step?

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. [Back to Table of Contents]

3. What happens during the risk analysis and determination task?

An essential task in the RMF Authorize step is the determination of risk since the decision to authorize (or not) a system to operate depends on the security and privacy posture of that system, as well as the risk from the operation and use of the system. This risk is determined using the authorizing official review and analysis of the information and materials in the authorization package, as well as organizational-level and system-level risk information provided by senior officials (e.g., senior agency information security officer, senior agency official for privacy, risk executive [function]), control assessors, system owners, and other stakeholders to the authorizing official. If necessary, further discussions between the authorizing official and those furnishing the information may take place to help the authorizing official fully understand the risks. During risk analysis and determination, the authorizing official also takes into consideration organizational risk tolerance, dependencies among systems and controls, mission and business requirements, criticality of the mission or business functions supported by the system, and the overall risk management strategy of the organization. If the system is under ongoing authorization, the authorizing official maintains the same risk analysis and determination process. What may change are the source of risk information and the platform through which it is communicated to the authorizing official (e.g., automated security and privacy management and reporting tool) when determining the current security and privacy posture of the system. [Back to Table of Contents]

4. What artifacts are in the authorization package?

The authorization package provides information on the security and privacy posture of the system or the common controls at or around the time a control assessment was performed. The authorization package includes security and privacy plans, security and privacy assessment reports, plans of action and milestones, and an optional executive summary. Organizations can leverage automated tools to assist them with keeping the authorization package contents up to date. [Back to Table of Contents]

5. Who is responsible for creating the authorization package?

The system owner or common control provider consolidates information and materials[1] for the authorization package and submits the package to the authorizing official or to the authorizing official designated representative for review. The common control provider and senior agency official for privacy also contribute information and materials[2] to the authorization package. The common control provider ensures that information about the common controls (i.e., controls inherited by the organizational system) is fully captured and addresses any outstanding plan of action and milestones. For systems that process personally identifiable information, the senior agency official for privacy reviews authorization packages to ensure compliance with applicable privacy requirements and to manage privacy risks prior to authorizing officials making risk determination and acceptance decisions. The senior agency official for privacy is also responsible for designating which privacy controls can be treated as common controls. The common control provider collects the necessary information and materials for the authorization package for common controls to be reviewed and approved by the authorizing official. [Back to Table of Contents]

[1] Documents and other supporting artifacts.
[2] Ibid.

6. What is the role of privacy in the authorization process?

The senior agency official for privacy has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risk. For systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information, the senior agency official for privacy reviews the authorization package prior to the authorizing official making risk determination and acceptance decisions. [Back to Table of Contents]

7. Can the authorization package be generated and submitted electronically?

An electronic (i.e., digital, non-print) version of the authorization package is recommended since it enables greater security (e.g., backup, access controls) and can facilitate faster transmission and delivery to intended recipients. These capabilities could be supported by automated security/privacy management and reporting tools, including governance, risk and compliance tools, and facilitating authorization and assessment efficiency. Electronic format is also preferred over print because the information (and supporting materials) contained in an authorization package changes over time. [Back to Table of Contents]

8. If the system is in ongoing authorization, how can an authorization package be submitted?

When a system is under an ongoing authorization, the authorization package is presented to the authorizing official via automated reports. Information presented to the authorizing official in assessment reports is generated in the format and with the frequency determined by the organization using information from the security and privacy continuous monitoring programs. [Back to Table of Contents]

9. Can the authorizing official designated representative do everything that the authorizing official does?

The authorizing official designated representative cannot approve an authorization package and accept risk. However, all other duties can be delegated by the authorizing official to the authorizing official designated representative. [Back to Table of Contents]

10. Can the system owner also be the authorizing official?

No, the system owner and the authorizing official are separate individuals, which eliminates the potential of a conflict of interest between the individual authorizing the system and the owner/manager of the system. [Back to Table of Contents]

11. Who determines if the risk is acceptable to an organization or not?

The authorizing official is the only person who can accept risk(s) upon review of the assessment reports and plans of action and milestones and after determining whether the identified risks need to be mitigated prior to authorization. The acceptance of risk reflects an organizational response to risk if the identified risk is within the organizational risk tolerance level. Risk acceptance, as with other risk decisions, is tied to the organizational risk management strategy and risk tolerance. Refer to NIST SP 800-30, *Guide for Conducting Risk Assessments* [SP 800-30], for risk assessment methodologies and guidance. NISTIR 8062 [IR 8062] introduces privacy risk management and a privacy risk model for privacy risk assessments. Organizations can use the NIST Privacy Risk Assessment Methodology (PRAM) tool to apply the risk model from NISTIR 8062 and analyze, assess, and prioritize privacy risks. [Back to Table of Contents]

12. How can risk be prioritized?

While risk can be quantified (e.g., as a product of impact and likelihood), the prioritization of risk is determined based on a variety of factors, such as asset criticality, available resources, and risk tolerance. Risks to high value assets could likely draw more resources for

mitigation. The prioritization of risks[3] should be performed in alignment with the organizational risk strategy. 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 their risk tolerance and their acceptable degrees of risk. [Back to Table of Contents]

13. How does an organization respond to identified risks?

Simply identifying and capturing risk information does not increase the security and privacy posture of a system or organization. An important aspect of risk management is the response to identified risks. Such a response includes mitigation of risks and acceptance of risks that cannot be fully mitigated. Plans of action and milestones help ensure that risks are tracked and mitigated as planned. For risks that are not or cannot be mitigated, organizations should look into implementing compensating controls to minimize the impact and likelihood of unmitigated risks. Such risks should also be recorded and monitored as part of the risk acceptance process. [Back to Table of Contents]

Authorize Step Fundamentals FAQs

14. How is the authorization decision made?

The authorization to operate is decided by the authorizing official based on a review of the security and privacy posture of the system to be authorized, the risks from the operation or use of the system, and input provided to the authorizing official by organizational officials. The authorization decision can only be made by the authorizing official (i.e., it cannot be delegated).

The security and privacy posture of the system is captured by artifacts in the authorization package that convey the most current information about the system and its environment of operation, including the effectiveness of the implemented controls (as assessed), the potential dependencies with other organizational systems and external systems, and the risk from these dependencies. Equipped with this information, knowledge of the organization, and the organization's risk management strategy and risk tolerance, the authorizing official analyzes security and privacy considerations and mission or business needs and determines if the risk to the organization's operations is acceptable. When deciding whether to authorize a system to operate, the authorizing official also reviews current residual risk and organizational plans of action and milestones. [Back to Table of Contents]

15. How is the authorization decision issued?

The authorization decision is communicated to the system owner and common control provider via the authorization package. The decision is also communicated to other officials as appropriate. Attached to the final decision on whether or not the system is authorized to operate are terms and conditions for operation. The terms and conditions describe limitations or restrictions that must be followed by the system owner or common control provider. Adherence to the terms and conditions is verified on an ongoing basis as part of the organization's continuous monitoring program. [Back to Table of Contents]

16. What is included with the authorization decision?

For systems, the authorization decision indicates to the system owner whether the system is authorized to operate, 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 the system owners of inheriting systems whether the common controls are authorized to be provided or not authorized to be provided. In addition to the authorizing official's final decision included in the authorization package, specific terms and conditions

[3] [SP 800-30] provides additional guidance on how to prioritize risk responses.

may accompany the authorization (or non-authorization) to operate. Adherence to the terms and conditions are verified by the authorizing official on an ongoing basis as part of continuous monitoring. [Back to Table of Contents]

17. If a system receives an authorization to operate, does it need to be reauthorized in the future?

Yes. Organizations may eliminate the authorization termination date if the system is operating under an ongoing authorization. For ongoing authorization, the authorization frequency is specified in lieu of an authorization termination date. [Back to Table of Contents]

18. Is the authorization decision transmitted to the system owner or common control provider?

The authorization decision is included with the authorization package and is transmitted to the system owner or common control provider. The organization ensures that the authorization decision is made available to organizational officials, such as system owners inheriting common controls, chief information officers, senior officials accountable for risk management or risk executive [function], senior agency information security officers, senior agency officials for privacy, and system security and privacy officers. [Back to Table of Contents]

19. What does the authorization decision mean to a system owner or common control provider?

The authorization decision indicates to the system owner or common control provider whether the system or common control is authorized to operate, authorized to use, not authorized to operate, or not authorized to use. For new systems, the authorization to operate approves the system "going live into production." For existing systems, the authorization to operate extends the current authorization. System owners and common control providers should review, acknowledge, and adhere to any terms and conditions set by the authorizing official included in the authorization to operate or use. If the system or common control provider is not authorized to use, then the system owner corrects the deficiencies identified and resubmits the package for approval. [Back to Table of Contents]

20. To whom does the authorizing official report authorization decisions?

In addition to communicating authorization decisions to system owners and common control providers, authorizing officials report system and common control authorizations to other organizational officials (e.g., the risk executive [function]) for their awareness and to support their individual risk decisions in the context of the organization. [Back to Table of Contents]

21. Can a system operate without an official authorization to operate decision?

No, an authorization decision and approved authorization package is completed and approved by the authorization official prior to a system being in operation. [Back to Table of Contents]

22. Is an organization required to report vulnerabilities?

Yes, organizations report exploitable deficiencies (i.e., vulnerabilities) in the system or controls noted during the assessment and continuous monitoring that represent significant security or privacy risk to the organization. For additional information about how an organization defines and quantifies significant security and privacy risk, see NIST SP 800-30 [SP 800-30], NIST SP 800-39 [SP 800-39], NISTIR 8062 [IR 8062], and the NIST Privacy Risk Assessment Methodology (PRAM). [Back to Table of Contents]

23. What are the different types of authorization?

The type of authorization that is issued to a system to operate depends on where the system is in the development life cycle, whether or not a robust organizational continuous monitoring program is in place, and what triggers an authorization (e.g., event-driven authorization). The following are the three types of authorizations:

- *Initial* – An initial authorization is a decision for a system to operate based on the initial review of the system or common controls after an assessment of system-level controls (including system-implemented hybrid controls) and inherited controls

described in the security and privacy plans. The initial authorization is the first authorization issued by the authorizing official for a system to operate.

- *Ongoing* – An ongoing authorization is a subsequent decision for a system to operate that is issued after a system is initially authorized to operate and according to the organization's continuous monitoring strategy. Ongoing authorizations can be time-driven or event-driven, require ongoing understanding and acceptance of security and privacy risk, and are only possible if the organization has established a robust continuous monitoring program.

- *Reauthorization* – A reauthorization is similar to an ongoing authorization in that it is a subsequent decision issued after a system is initially authorized to operate and can be time-driven or event-driven. The difference between a reauthorization and an ongoing authorization is the fact that reauthorizations are static, single point-in-time decisions. For reauthorizations, the authorizing official may opt to have a full review of the system or common controls or to customize the review targeting specific controls based on the motivation for the reauthorization. [Back to Table of Contents]

24. Can a system be given an interim authorization to operate?

No, a system cannot be given an interim authorization to operate. However, the authorizing official may approve a short-term authorization for a system be tested within the operational environment before controls are implemented or as they are implemented. This condition is set in the authorization termination date as part of the authorization decision. [Back to Table of Contents]

25. What are the types of authorization decisions that can be given by an authorizing official?

The following types of authorization decisions can be issued by the authorizing official:

- *Authorization to Operate* – The decision to authorize a system to operate is based on the review of the (contents of the) authorization package and the determination that the risk to organizational operations, assets, individuals, other organizations, and the Nation is acceptable. The authorization is accompanied by terms and conditions for meeting and maintaining authorization requirements and is valid for a pre-specified period of time. A time-driven authorization frequency is specified if a system is under ongoing authorization, though events may trigger a need to review the authorization to operate.

- *Common Control Authorization* – The decision to authorize common controls that can be made available for inheritance by organizational systems is based on the review of the (contents of the) authorization package submitted by the common control provider and the determination that the risk to operational operations, assets, individuals, other organizations, and the Nation is acceptable. The decision to reauthorize common controls can be time-driven or event-driven.

- *Authorization to Use* – The decision to authorize the use of an existing federal or nonfederal system currently and already authorized to operate by a federal entity is meant to promote reciprocity between systems with different authorization officials (i.e., both authorizing officials share the responsibility and authority for risk management) as well as to support the use of shared systems, services, or applications. The authorizing official issuing the authorization to use decision reviews the authorization package from the provider organization when determining risk from the use of the shared system, service, or application. The authorization to use decision may specify an authorization termination date and/or condition (e.g., event) that would trigger a review of the authorization.

- *Denial of Authorization* – An important aspect of authorization decisions is the determination of risk to organizational operations, assets, individuals, other organizations, and the Nation and whether the risk is acceptable. If the risk is not acceptable or when the risk is no longer acceptable (e.g., when there are deficiencies in controls or when there is a violation of policy and/or terms and conditions), then an authorization cannot be granted. In some cases, the authorization decision is rescinded. For previously authorized systems in operation, all activity is halted if a denial of authorization is issued. [Back to Table of Contents]

26. What steps can a system owner or common control provider take when a denial of authorization is issued?

The authorizing official or authorizing official designated representative works with the system owner or the common control provider to revise the plan of action and milestones to help ensure that measures are taken to correct the deficiencies that increase risk to an unacceptable level. [Back to Table of Contents]

27. Can an authorization be rescinded?

Yes, authorizing officials can rescind a previous authorization decision when assessment or monitoring information reflects an unacceptable increase in risk; when there is a violation of federal or organizational policies, directives, regulations, standards, or guidance; or when there is a violation of the terms and conditions of the authorization. When the deficiencies are reduced to an acceptable level of risk, the authorizing official can then authorize the system to operate. [Back to Table of Contents]

28. How can an organization leverage ongoing authorization?

There are two conditions that need to be met in order to leverage ongoing authorization:

1) The system or common control seeking ongoing authorization obtains an initial authorization to operate; and
2) A robust organizational continuous monitoring program is in place to monitor implemented controls.

Ongoing authorization is made possible by the organization's continuous monitoring program, as well as the organization's ability to guide and inform authorizing officials in their decision whether to authorize a system to operate or to authorize use of common controls. Authorizing officials rely on security and privacy information generated from the ongoing monitoring of controls and changes to systems and environments of operation. The information is generated and provided at a frequency stipulated by the organization and is defined by the organization's continuous monitoring strategy. Automation and state-of-practice tools, techniques, and procedures are utilized to provide authorizing officials with information that describes the security and privacy posture of the system to determine whether continued operation is acceptable. [Back to Table of Contents]

29. What are some event-driven triggers that might prompt a review of the authorization package?

Certain events can prompt an organizational reaction that can impact ongoing authorization and reauthorization. Examples of event-driven triggers include:

- A new threat, vulnerability, privacy risk, or impact information
- An increased number of findings or deficiencies from the continuous monitoring program
- New mission or business requirements
- Change in the authorizing official
- Significant[4] change in risk assessment findings
- Significant changes to the system, common controls, or the environments of operation (e.g., new or upgraded hardware or software, configuration changes, personally identifiable information processing modifications, service changes, location changes, requirement changes)
- Changes in the supply chain that affect security or privacy risks to operational systems
- Exceeding organizational thresholds [Back to Table of Contents]

[4] A significant change is defined as a change that is likely to substantively affect the security or privacy posture of a system.

30. What is the difference between *type* and *facility* authorizations?

Both *type* and *facility* authorizations are official authorization decisions intended to promote effective authorizations considering that certain systems share similar if not identical attributes that can be leveraged by other like systems once authorized. In *type* authorizations, the authorizing official may issue a type authorization to operate, such as to systems with common specifications (e.g., hardware, software), identical information processing, and identical control implementations deployed in multiple locations for use in specified environments of operation. In *facility* authorizations, the focus is on the environment of operation, such as physical environments (i.e., facilities) where a given system is located. If co-located systems share the same facility, a facility authorization can be leveraged since the implementation of controls such as physical and environmental protection controls, boundary protection controls, and contingency and incident response controls may be common and shared by multiple tenants. [Back to Table of Contents]

31. What is the difference between traditional and joint authorizations? Can a system have more than one authorizing official?

The difference between *traditional* and *joint* authorizations is the number of organizational officials in a senior leadership position serving as authorizing official with the responsibility and accountability for a system or common controls. In a traditional authorization, a single authorizing official is responsible and accountable for a system or common control. In a joint authorization, multiple organizational officials from the same or different organization share responsibility and accountability for the system and jointly accept security and privacy risks. The authorizing officials in a joint authorization have shared interest in authorizing a system and agree on terms and conditions for the joint authorization, including the process for determining and accepting risk. The joint authorization remains valid while there is agreement among the authorizing officials and while the authorization meets specific requirements. For more information, see control enhancements CA-6(1) AUTHORIZATION | JOINT AUTHORIZATION – INTRA-ORGANIZATION, and CA-6(2) AUTHORIZATION | JOINT AUTHORIZATION – INTER-ORGANIZATION [SP 800-53r5]. [Back to Table of Contents]

References

[IR 8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[OMB A130] Office of Management and Budget (2016) *Managing Information as a Strategic Resource*. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-37r1] Joint Task Force (2010) Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 1 [withdrawn]. https://doi.org/10.6028/NIST.SP.800-37r1

[SP 800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

[Back to Table of Contents]