RISE8

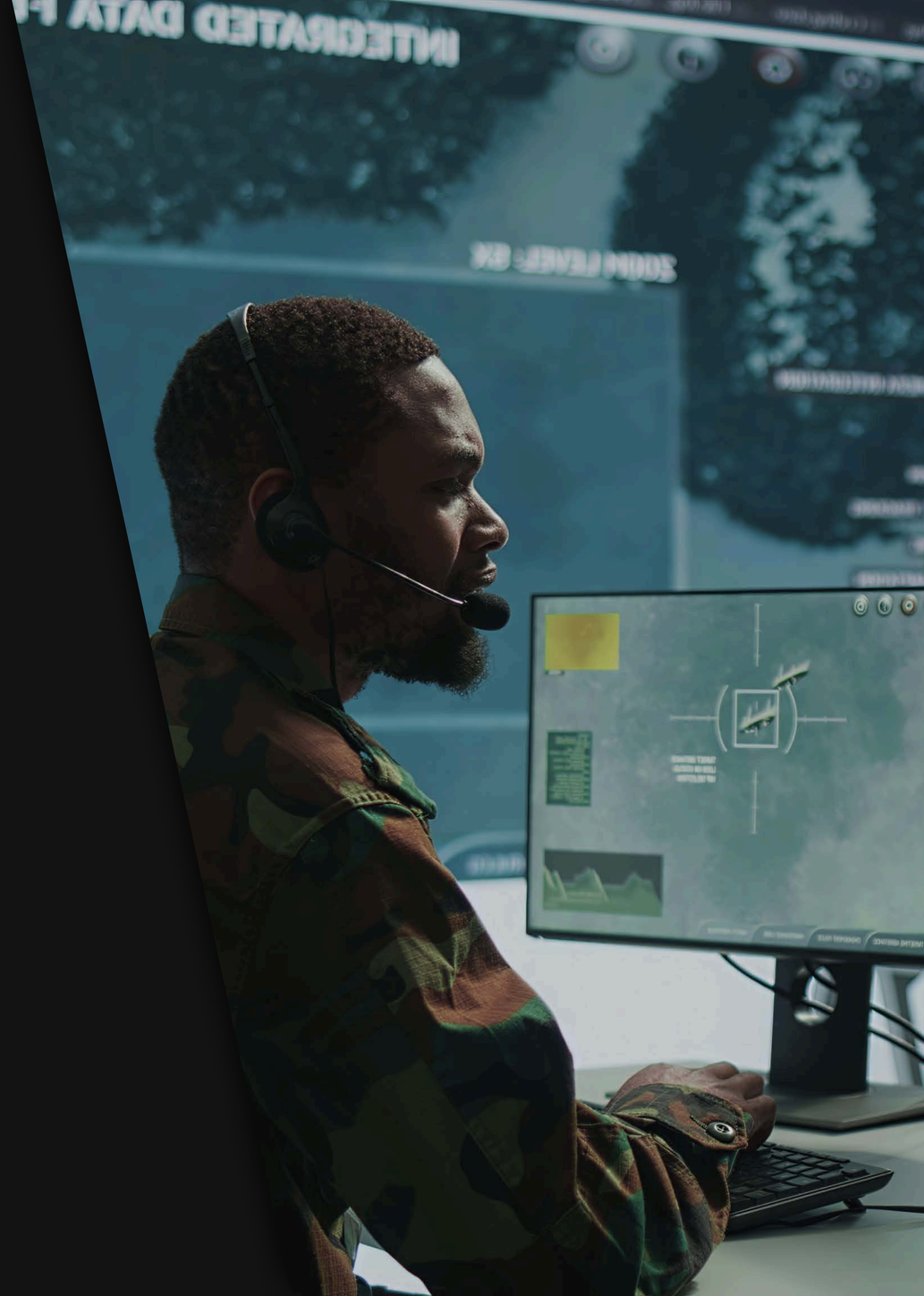
# Authorization to Operate Checklist (ATO)

**Learn about the process** of obtaining an authorization to operate, explore ATO resources, and learn about the next evolution of ATO: cATO.

# Obtaining an Authorization to Operate (ATO)

Obtaining an Authorization to Operate, or ATO, can be a complex and time-consuming process with delays and longer queue times resulting from limited capacity and skills deficits across government. Organizations lack sufficient information security analysts and authorizing officials (AO) to address the volume of systems and changes that require evaluation. In addition to setting aside money for their AO to hire dedicated, technically skilled assessors, organizations may also accelerate success with guides, checklists, and other free resources to achieve secure and compliant system authorization. Rise8 created this guide, with checklists and other free resources, to help you better understand the Risk Management Framework (RMF) process to acquire an ATO.

**We'll also explore continuous Authorization to Operate—ongoing authorization for continuous delivery after receiving an initial ATO.**

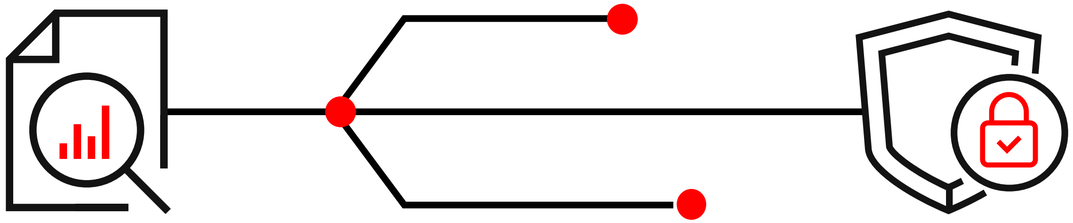


# What Is Authorization to Operate?

An ATO is a formal declaration that a system meets the necessary security and privacy standards for deployment on a specific network. This process involves a thorough evaluation of the system's security controls, risk management strategies, and overall security posture to ensure it can effectively protect sensitive data and maintain operational integrity without compromising the system or broader network.

Note: ATOs are often colloquially referred to as an “Authority to Operate.” The technical term is “Authorization to Operate.” This guide will occasionally use the colloquial term in addition to the technical phrase.

Are you wondering “What is Authorization to Operate NIST?” or “What is Authorization to Operate for Systems?” It’s all the same. Authorization to Operate is a product of the National Institute of Standards and Technology (NIST) RMF, so they are often referenced together. The RMF outlines a structured, but adaptable process with seven steps for managing risks associated with information systems: prepare, categorize, select, implement, assess, authorize, and monitor. Organizations may apply these steps in non-sequential order, as applicable to their software development lifecycles. ATOs are always for government information systems. They indicate that a system has passed a comprehensive security assessment and meets the required security standards to function within a specific operational environment.



# How Long Does Authorization to Operate Take?

The time required to obtain an ATO varies, but many in government identify waiting for an ATO and working through assessments as the longest step in developing and deploying software. Traditionally an ATO, granted during the seven-step RMF, requires a point-in-time check of security controls that can take months; the exercise repeats for major updates or when the authorization expires.

**Several factors contribute to process timeliness,** including the complexity of the system, the thoroughness of the preparation and documentation, the responsiveness of all stakeholders, and the availability of technically skilled assessors and highly competent system development teams.

## Here's a general outline of what to expect in each step of the RMF

01 **Prepare:** This involves identifying key roles, establishing a risk management strategy, conducting risk assessments, identifying common controls, and developing a monitoring strategy. This phase may take a few weeks to several months, depending on the organization's readiness and experience with the RMF.

02 **Categorize:** In this important step that ties the information system's security activities to the organization's mission/business priorities, organizations must identify information types, select provisional impact levels, then review and adjust or finalize impact levels, and assign a system security category and overall impact level.

03 **Control Selection:** Select appropriate baseline security controls based on risk assessments. Then add supplemental and compensating controls if necessary. This step typically takes a few weeks and is crucial for defining the security requirements. Organizations can expedite this with clear guidelines and previous experience.

04 **Implement Security Controls:** Implementing the selected security controls can take several months, depending on the complexity of the system and the number of controls to apply. This phase involves configuring and integrating security measures into the system while properly documenting how controls deploy.

05 **Assess Security Controls:** Conducting a thorough security assessment, including penetration testing and vulnerability scanning, can take a few weeks to a few months. The duration depends on the scope of the assessment and subsequent findings.

06 **Authorize System:** Compiling the Authorization Package (including the System Security Plan, Security Assessment Report, and Plan of Action & Milestones) and presenting it to the AO can take several weeks. The AO's review and decision-making process can add additional time, especially if there are significant risks that require further mitigation.

07 **Monitoring and Continuous Compliance:** While this phase occurs after the initial ATO is granted, it involves ongoing activities to ensure the system remains secure and compliant. This phase is continuous and involves regular updates and assessments.

The entire process from preparation to obtaining the ATO can range from six months to two years, with one year being a common duration. Factors such as the organization's familiarity with the RMF process, the complexity of the system, and the efficiency of the assessment and authorization process can significantly impact the timeline. **Once you've received your ATO, it's important to note that this authorization is generally issued for a limited period**—often three years—and once it expires, you will need to get reauthorized.

Checklist

# How Do I Get an ATO?

Obtaining an Authorization to Operate (ATO) involves a structured, but flexible process defined by the RMF. We are often asked, “What are the ATO process steps?” It’s important to remember that ATOs are granted during the seven-step RMF process.

Note: This checklist is a high-level overview of the seven-step RMF process—multiple steps in each of these sections must be completed. More information is available by visiting NIST or when working with an experienced partner like Rise8.

## Prepare

- Identify key risk management roles within your organization.
- Establish a risk management strategy and determine risk tolerance.
- Develop an organization-wide risk assessment and establish tailored control baselines.

## Categorize

- Determine the impact level of the system based on confidentiality, integrity, and availability.
- Use NIST’s FIPS 199 to help categorize the information and systems.

## Select Security Controls

- Choose a baseline set of security controls from NIST SP 800-53B based on the system’s categorization.
- Supplement these controls with additional ones if necessary to address specific risks.

## Implement Security Controls

- Apply the selected security controls to the system.
- Document how these controls are deployed and integrated into the system.

## Assess Security Controls

- Conduct a thorough evaluation of the implemented controls to ensure they are functioning correctly and effectively mitigating risks.
- This assessment typically involves penetration testing and vulnerability scanning.

## Authorize the System

- Compile an Authorization Package.
- Present this package to the AO for review.
- The AO will evaluate the risk and decide whether to grant the ATO based on the assessment results and the system's overall security posture.

## Monitor Security Controls

- Once the ATO is granted, continuously monitor the system to ensure ongoing security.
- Perform regular assessments, updates, and reporting to maintain compliance and address any emerging threats.

Resources like this Authorization to Operate checklist can help you create a structured approach to obtaining an ATO with the seven-step RMF process and ensuring comprehensive security for information systems. You can use this as an Authorization to Operate template, keeping in mind that this is a high-level overview.

We also hear a lot of people asking, "How can I get an ATO certification and accreditation?" Certification and accreditation (C&A) was part of the DoD Information Assurance Certification and Accreditation (DIACAP) program that RMF replaced in 2015 and is no longer used. The RMF is what you should be using today.

Checklist

# What Documents Are Needed for an ATO?

## 01 System Security Plan (SSP)

- **Overview:** Provides a comprehensive description of the system, including its purpose, scope, and architecture.
- **Contents:** Details roles and responsibilities, system categorization, implemented security controls, and their current status.
- **Purpose:** The SSP outlines how security measures are applied and maintained to protect the system.

## 02 Security Assessment Report (SAR)

- **Overview:** Summarizes the results of the independent security assessment.
- **Contents:** Includes findings from vulnerability scans, penetration tests, and control assessments with each control rated as Compliant, Non-compliant, or Not Applicable.
- **Purpose:** The SAR provides evidence of the system's security posture and highlights areas for improvement.

## 03 Plan of Action and Milestones (POA&M)

- **Overview:** Details the planned actions to address vulnerabilities and deficiencies identified in the SAR.
- **Contents:** Lists specific mitigation steps, responsible parties, resources required, and timelines.
- **Purpose:** The POA&M demonstrates the system owner's plan to address and mitigate identified risks.

## 04 Risk Assessment Report (RAR)

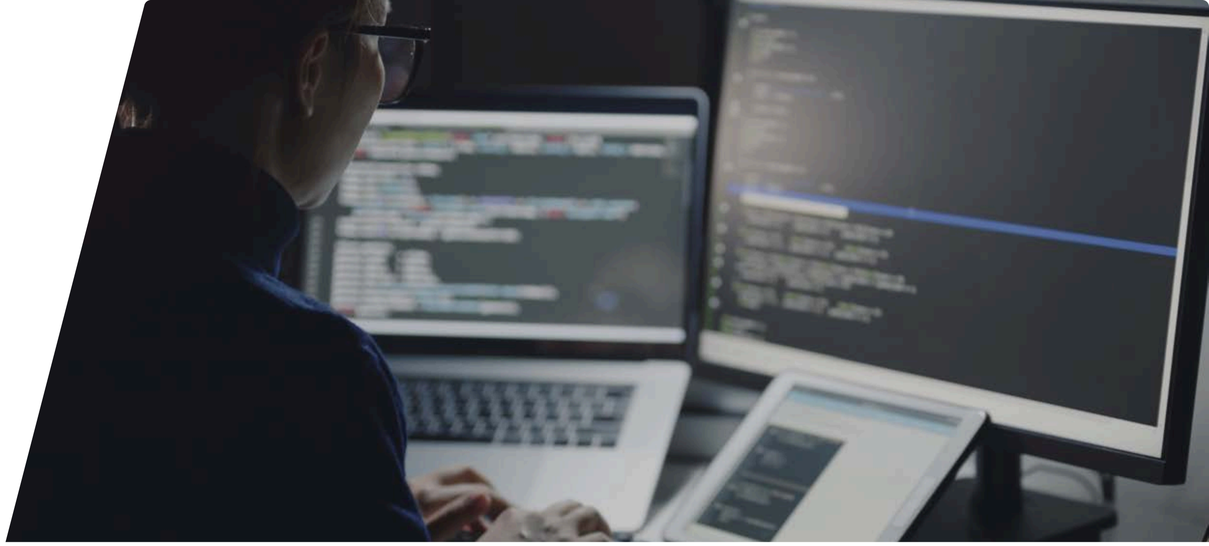
- **Overview:** Analyzes the risks associated with the system, categorizing them by impact and likelihood.
- **Contents:** Assigns risk levels (Very Low, Low, Moderate, High, Very High) to each finding, along with an overall risk posture for the system.
- **Purpose:** The RAR helps the AO understand the potential impacts and make informed decisions.

## 05 Authorization Package

- **Overview:** A compiled package that includes the SSP, SAR, POA&M, and any other relevant documentation.
- **Contents:** May also include contingency plans, incident response plans, configuration management plans, and privacy impact assessments.
- **Purpose:** The ATO package documents provide a complete view of the system's security status and risk management strategies, supporting the AO's decision-making process.

These documents collectively ensure a thorough evaluation of the system's security measures, identify potential risks, and outline plans to mitigate those risks. By providing detailed and structured documentation, the process of obtaining an ATO helps maintain a high level of security and compliance within government networks, ensuring that all aspects of the system's security are thoroughly reviewed and addressed.

# Is There an Alternative to the Traditional Way We Approach the Authorization To Operate (ATO) Process?



While there is no alternative to the RMF, the RMF is very flexible and encourages implementing the framework according to your needs and abilities. So yes, there are alternatives to the traditional way we approach the Authorization to Operate process. A popular alternative involves moving to an ongoing authorization tailored for continuous delivery, often referred to as continuous Authorization to Operate (cATO). Traditional ATOs can be time-consuming and often lead to delays in deploying critical systems due to their static, point-in-time assessments. In contrast, cATO offers a dynamic and ongoing approach to system authorization, better suited for today's fast-paced and continuously evolving cybersecurity landscape.

cATO is the uncodified term used to describe a specific subset of ongoing authorization tailored for continuous software delivery. cATO is designed to integrate continuous monitoring and agile methodologies, ensuring that security and compliance are maintained in real time as systems and software are developed and updated.

**This approach aligns with the RMF but shifts the focus from periodic reauthorization to ongoing assessment and authorization.**

# What Are the Benefits of cATO?

## The benefits of ongoing authorization include:

### 01 Real-Time Risk Management

- cATO requires continuous monitoring of the system's security posture, enabling real-time detection and mitigation of vulnerabilities.
- This proactive approach helps maintain a higher level of security and compliance, reducing the risks associated with new threats and vulnerabilities.

### 02 Agile and Efficient Deployment

- By adopting cATO, organizations can deploy software updates and new systems more quickly without waiting for lengthy reauthorization processes.
- This agility is crucial for government agencies and other organizations that need to respond rapidly to changing requirements and emerging threats.

### 03 Enhanced Flexibility and Responsiveness

- cATO provides a more flexible framework that allows for frequent updates and modifications, ensuring that systems remain secure and functional over time.
- This continuous process aligns better with modern DevOps practices, promoting a culture of ongoing improvement and adaptation.

Essentially, cATO represents a significant advancement over the traditional process for obtaining an ATO, providing a more responsive, efficient, and secure approach to system authorization, resulting in higher-quality software with reduced risk. By adopting cATO, organizations can better manage risks, deploy updates more swiftly, and maintain a higher standard of security in an ever-changing threat landscape.

# What Is an Example of Authorization to Operate vs cATO?

## Authorization to Operate Example

Imagine a government agency, the Environmental Protection Agency, tasked with developing a new system for monitoring air quality across the country. The system will collect data from thousands of sensors, analyze it, and provide real-time updates to policymakers and the public.

**Obtaining an ATO would look something like this**

01 **Preparation:** The agency begins by identifying key roles and establishing a risk management strategy. They categorize the system, select appropriate security controls, and document everything in a System Security Plan (SSP).

02 **Implementation and Assessment:** Over several months, the agency implements the security controls, and an independent assessment is conducted. A Security Assessment Report (SAR) is prepared, highlighting the effectiveness of the controls and identifying any vulnerabilities.

03 **Authorization Package:** The agency compiles an Authorization Package, including the SSP, SAR, and Plan of Action & Milestones (POA&M), and submits the package to the AO.

04 **Review and Decision:** The AO reviews the package, a process that can take weeks or even months. The AO may request additional information or modifications before granting the ATO.

05 **Operational Delays:** During this period, the system cannot be fully deployed. Any updates or changes to the system require a repeat of the entire process, causing further delays.

**Outcome:** While thorough, obtaining a traditional ATO results in significant delays. The system, intended to provide timely air quality data, cannot be deployed quickly enough to address emerging environmental concerns. Policymakers and the public are left waiting for critical information.

# Continuous Authorization to Operate (cATO) Example

Now, consider the same scenario, but the Environmental Protection Agency adopts a continuous Authorization to Operate approach, guided by Rise8's cATO Playbook.

## The process to achieve ongoing authorization would include

01 **Preparation and Integration:** The agency still begins with preparation and categorization. However, from the outset, they integrate continuous monitoring and agile methodologies. Security controls are selected and implemented with an emphasis on automation and real-time assessment.

02 **Ongoing Assessment:** Instead of a one-time, static assessment, the system undergoes continuous evaluation of frequent releases. Real-time monitoring tools detect and address vulnerabilities as they emerge. Security controls are regularly updated and tested.

03 **Real-Time Authorization:** With continuous monitoring in place, the AO can grant ongoing authorization based on current, real-time data. There's no need to wait for a periodic review cycle; the system is authorized to operate as long as it meets security standards.

04 **Rapid Deployment and Updates:** The system is deployed quickly, providing real-time air quality data to policymakers and the public. As new sensors are added or software updates are needed, these changes are seamlessly integrated and authorized without significant delays.

# Outcome

Achieving cATO enables the Environmental Protection Agency to deploy the air quality monitoring system swiftly and efficiently. Policymakers have immediate access to critical data, allowing them to make informed decisions to protect public health and the environment. The system remains secure and up-to-date, continuously adapting to new threats and requirements.

With a traditional ATO, the agency faced significant delays, impacting its ability to provide timely air quality data. With cATO, the same agency can deploy and update its system rapidly, maintaining high security standards and delivering essential information in real time. This example highlights the stark contrast between the two approaches and underscores the benefits of adopting a continuous, agile framework for system authorization.

**Rise8 is at the forefront of implementing cATO, leveraging the principles of the Risk Management Framework, Agile, and DevOps to streamline the authorization process, making it faster and more efficient while maintaining rigorous security standards.** With cATO, organizations can achieve continuous compliance and operational excellence, ensuring that their systems are always secure, up-to-date, and ready to move at the speed their users demand.

Download our comprehensive continuous authorization playbook to learn more about this process.