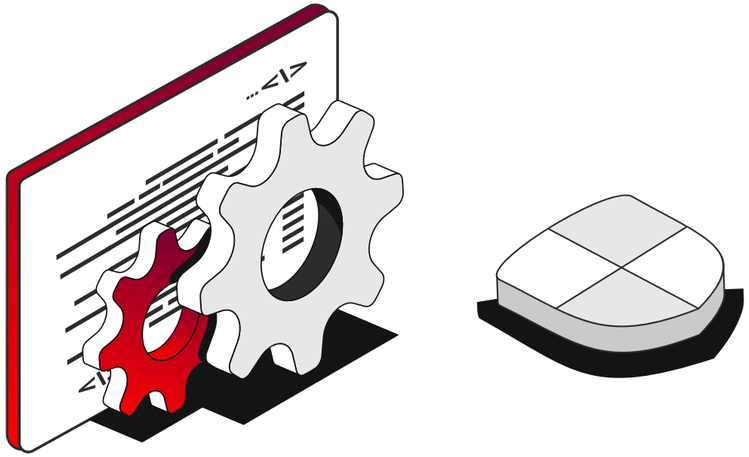
Adapt the NIST RMF for Continuous Delivery and Mission Impact

Move fast, stay compliant, and deliver software that meets the moment—**without delay.**

RISE8

Integrate NIST RMF with Agile and DevOps Methodologies to Drive Mission Impact

Despite the modern tools that have made software development a much simpler prospect than it was even a few years ago, it's still a process fraught with delays and security vulnerabilities. In government and military applications, there is an imperative to not only develop effective, secure software, but also deploy it at the speed users demand.



In this context, achieving authorization to operate (ATO)—a formal declaration that authorizes the deployment of a specific system on a network—is vital. Unfortunately, the traditional ATO is a point-in-time security controls check, required for initial deployment, major updates, and when the authorization expires. Software development across the federal government requires a more rapid, dynamic, and robust approach—continuous authority to operate (cATO). **Done correctly, cATO leverages an ongoing authorization tailored for the swift and continuous delivery of higher-quality, secure software. The Risk Management Framework (RMF) not only allows for this, but encourages it.**

This article highlights the fundamentals of cATO, including how to align RMF application with Agile and DevOps software development lifecycles without compromising compliance or sacrificing speed.

What Does ATO Stand for?

Within a government technology context, ATO stands for authorization to operate; it's best thought of as a formal declaration that a system meets the necessary government security and privacy standards for deployment as the Federal Information Security Modernization Act (FISMA) requires. It represents a formal commitment to managing security and privacy risks for federal government software, including the Department of Defense (DOD).

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.

Note: What Is continuous Authorization to Operate (cATO)?

Continuous authorization to operate (cATO) is an ongoing-authorization process for continuous delivery, after achieving initial authorization, that moves beyond the point-in-time nature of traditional ATOs. This methodology enhances mission-critical environments that require frequent and rapid deployment of software updates while maintaining high security.

What Is Continuous ATO Based On?

Initially, cATO was part of an initiative to streamline and expedite software approval processes, blending Agile and DevOps methodologies with the existing RMF. This innovative approach revolutionized traditional practices by emphasizing continuous assessment and improvement.

Today, the **Department of Defense (DoD)** describes cATO as a continuous risk determination and authorization by continuously assessing, monitoring, and managing risk. cATO allows organizations to build and release new system capabilities if they can continuously monitor them against the approved security controls. Organizations must meet three criteria to achieve cATO: continuous monitoring of security controls; active cyber defense measures; and the adoption of DevSecOps practices.

At times, this framework has devolved into an exercise of "authorizing the people and the process" rather than focusing on authorizing the information systems as the RMF requires. It's important to remember that cATO is about authorizing the system itself, albeit with the right people, policies/processes, and technologies as the inputs that result in secure, authorized outputs for a trustworthy and transparent environment.

What Is the Difference Between ATO and cATO?

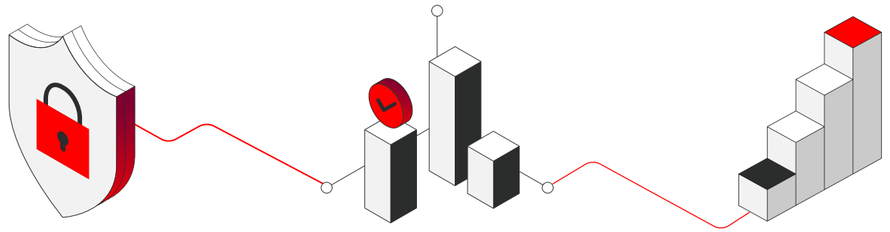
The best way to differentiate between a traditional Authorization to Operate (ATO) and continuous Authorization to Operate (cATO) is that ATO is a time-bound authorization after a point-in-time assessment. cATO is an uncodified term describing a specific subset of ongoing authorization tailored for continuous software delivery.

- **ATO** traditionally provides authorization for a set period—often three years—after which the organization's system must undergo a full reauthorization process. This process is resource-intensive, disruptive with the snapshot-in-time evaluation of the system's security posture, and provides neither speed nor adequate security to address changes in technology and emerging threats.
- By contrast, an **ongoing authorization tailored for continuous delivery (cATO)** represents a more dynamic and continuous approach to identifying, mitigating, and managing risk over time. Instead of requiring periodic reevaluation or renewal at set intervals, ATO compliance for an ongoing authorization requires truly continuous monitoring, implementation or remediation, and assessment to keep pace with the low lead times of continuous delivery found in high-performing DevOps organizations.

A 2022 DOD **memorandum** described current ATO processes as imperfect and insufficient in meeting modern challenges. Specifically, the current implementation "focuses on obtaining system authorizations (ATOs) but falls short in implementing continuous monitoring of risk once authorization has been reached." Additionally, "real-time or near real-time data analytics for reporting security events is essential to achieve the level of cybersecurity required to combat today's cyber threats and operate in contested spaces," bolstering the requirement for a transition from ATO to cATO "to accelerate innovation while outpacing expanding security threats." Because operations typically occur across a system of systems, the goal is to formalize and monitor system connections and enhance overall cybersecurity.

What Are the Benefits of Continuous ATO?

When organizations achieve continuous Authorization to Operate, they benefit in three distinct ways:



IMPROVED SECURITY POSTURE, LOWER RISK

Some of the most effective ways for organizations to improve their security posture and lower their risk exposure include:

- Rapidly assessing and reducing the number of security vulnerabilities or defects through effective threat analysis and best practices for secure coding.
- Continuously working to detect—and then remediate—application vulnerabilities effectively and quickly.
- Making up-to-date, reputable cybersecurity and vulnerability education available to development teams and other stakeholders.

INCREASED TRANSPARENCY, TRUST

When properly developed and implemented, cATO also increases transparency and trust within the organization, by:

- Ensuring all evidence artifacts—i.e. source code, documentation, and diagrams—are available throughout the software development lifecycle to support continuous monitoring and evaluation by cybersecurity assessors.
- Establishing and utilizing secure release pipelines to facilitate incremental automation of key risk assessment functions and practices.

Reduced Costs, Increased Delivery of Value With the Adaptable NIST RMF

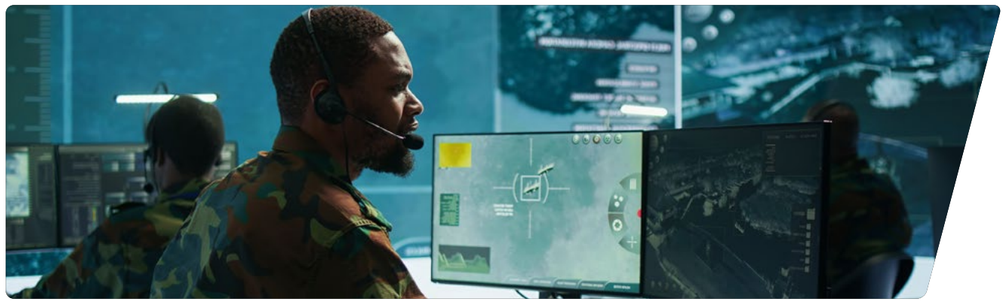
Organizations can reduce their costs and increase the delivery of value for their end users' needs by:

- Leveraging a secure cloud environment for software design, development, and delivery.
- Reducing the overall number of security defects and risks, including taking a proactive cybersecurity posture to quickly detect and mitigate new vulnerabilities as they emerge.
- Decreasing the time it takes to fully develop and deliver software solutions—from weeks, months, or even years to hours or days.
- Providing a level of adaptability and agility that enables developers to make more efficient system changes and updates.
- Ensuring compliance within complex regulatory environments.

The Essential Steps in the NIST RMF Process

As laid out in the framework's flexible and adaptable guidelines, the ATO RMF process consists of seven essential steps that organizations may apply in nonsequential order:

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



01 **Prepare:** Identify key risk management roles, develop a risk management strategy, conduct risk assessments, identify organizationally tailored and common controls, and establish a monitoring strategy.

02 **Categorize:** Analyze the impact of loss to categorize systems and the information they process, store, and transmit.

03 **Select:** Choose an initial set of controls and tailor them following the complete risk assessments.

04 **Implement:** Employ controls and describe how they apply within the system and its operating environment.

05 **Assess:** Determine whether the organization has effectively implemented controls and whether they produce the intended results regarding security and privacy requirements.

06 **Authorize:** Provide organizational accountability with a leadership determination on whether the system or controls have an acceptable level of risk to operate.

07 **Monitor:** Monitor the system and implement controls over time to mitigate risk and keep systems and information secure; document changes, conduct risk assessments and impact analyses, and report the security and privacy posture of the system.

RISE8

Check out the Rise8 cATO Playbook

You can find our playbook online at our **website**, or visit **this page** to download a copy.

Ready to Make Ship Happen?

WE'RE HERE TO ANSWER THE CALL

Get in touch

Or email us at **growth@rise8.us**