

# The New Age for Continuous ATO

## INSIDE:

ATO Reduces Cyber Risk .....	3
A Framework for Risk Management .....	6
Pentagon Activates Cyber Defenses with cATO .....	10

SPONSORED BY

**maximus**





# From the writer's desk



Kate Macri, Deputy Editor

## The Future of Cybersecurity Requires Continuous Verification

For years, federal agencies needed an authorization to operate (ATO) their IT systems, essentially a permission slip signing off on the cybersecurity risks associated with their IT infrastructure and applications. Then federal cyber leaders introduced the concept of continuous monitoring, suggesting risks must be constantly calculated, accepted and mitigated in order to operate certain aspects of IT infrastructure.

Now federal agencies are adopting continuous ATO, or cATO, a combination of these two concepts to constantly assess the risk posture of their IT systems as the rate of cybercrime skyrockets.

Constant vigilance is difficult, but federal agencies and industry are committed to shifting cybersecurity from passive to active, starting with a critical look at how they evaluate risk within the IT functions they use every day. ✿



# Table of Contents



Kate Macri,  
Deputy Editor



Sarah Sybert  
Staff Writer

## ARTICLE

### **NIST, HHS on Automating Data Collection for Cybersecurity**

Enabling data access, collection and protection can augment manual processes and keep systems secure.

BY SARAH SYBERT

## INFOGRAPHIC

### **Risk Management Framework**

Authorization underpins the system development lifecycle.

## PARTNER INTERVIEW

### **How cATO Supports Better Cybersecurity**

A continuous authorization to operate (cATO) can help federal agencies improve cybersecurity and software modernization efforts in a cloud environment.

**Tim Meyers, VP, Federal Cybersecurity, Maximus**

## ARTICLE

### **DOD Releases New Continuous ATO Initiative for 'Active' Cybersecurity**

The initiative will help defense leaders develop more aggressive cyber defenses.

BY KATE MACRI





## NIST, HHS on Automating Data Collection for Cybersecurity

Enabling data access, collection and protection can augment manual processes and keep systems secure.

BY SARAH SYBERT

The National Institute of Standards and Technology (NIST) and the Department of Health and Human Services (HHS) are improving data access and posture to mitigate cybersecurity risks, leaders said during an ATARC virtual event.

“One of the largest challenges is to ensure that you actually have, hands on, all of the data that you need to actually have the awareness of your environment, the kinds of security risks that you have in it and how you’re able to ensure that you can patch change configurations to mitigate risks in your environment,” Blair Heiserman, NIST’s CISO, said in describing the challenges his agency faces in the modern-day security operations center environment.

Bobby Miller, CISO at HHS’ Office of Inspector General, explained that one of the biggest challenges at his office is training the workforce to perform security analysis across different data sets, then transforming that data into actionable insights.

“Moving forward, particularly as we start talking more about extended



detection and response (XDR), I think behavioral analytics will become essential to provide that holistic view to security analysts — being able to look across devices, applications on your network — that’s going to be invaluable,” Miller said.

With the continual growth of data, XDR will enable agencies and organizations to improve incident response. XDR collects and automatically correlates data across multiple security layers, ultimately

enabling faster detection of threats and improved investigation and response times through security analysis.

For XDR to be effective, Heiserman said that organizations must be able to ingest different data sources across different locations, including cloud, containerized solutions, endpoints and more, to build out posture awareness. It all comes down to capturing the right data at the right time to distill proper mitigation measures and improve detection. Miller said that XDR should take a cross-organizational approach to ensure alignment of implementation and

# Blair Heiserman

## CISO, NIST



improve security.

“You need to have near real-time data about your environment. That is how you get to a continuous ATO state, where you are aware of the risks in your environment, so you can continue to authorize systems for use. But you also need telemetry data, and you need it combined with other data sets because you have a wealth of information hitting every individual endpoint, every application, and by being able to stitch the analysis across the data sets from each of those, it provides an awareness,” Heiserman said.

Telemetry is the automated communication processes from multiple data sources. Telemetry data is used to improve customer experiences, monitor security, application health, quality and performance. Agencies are looking to leverage this data to improve incident response time.

“Having that telemetry data is critical for your security analysts ... Having the ability to have data at your fingertips, when you need it is essential,” Miller said. “When you start talking about pulling these data sets together, being able to instantly respond to an incident and track it down, you have to have that data.”

By “stitching” data together, organizations will be able to recognize new or unexpected correlations across multiple technology solutions. This technique will provide organizations with a baseline to compare risk and expose malicious activity.

“Now, you’re starting to see things that previously you could feed it in, but you had to have someone go and look to pull out a thread from an incident. I think that’s the potential promise. As it all gets stitched together, it’s telling you that ‘this is one you should be concerned about’ and ‘this is not,’” Heiserman said.

Moving forward, NIST is emphasizing the importance of developing data standards to have a shared language. Data standards will help focus and prioritize the workforce and resources on the most important threats or vulnerabilities, as well as improve risk-based decision-making. (ctd.)



**“You need to have near real-time data about your environment. That is how you get to a continuous ATO state, where you are aware of the risks in your environment, so you can continue to authorize systems for use. But you also need telemetry data, and you need it combined with other data sets because you have a wealth of information hitting every individual endpoint, every application, and by being able to stitch the analysis across the data sets from each of those, it provides an awareness.”**

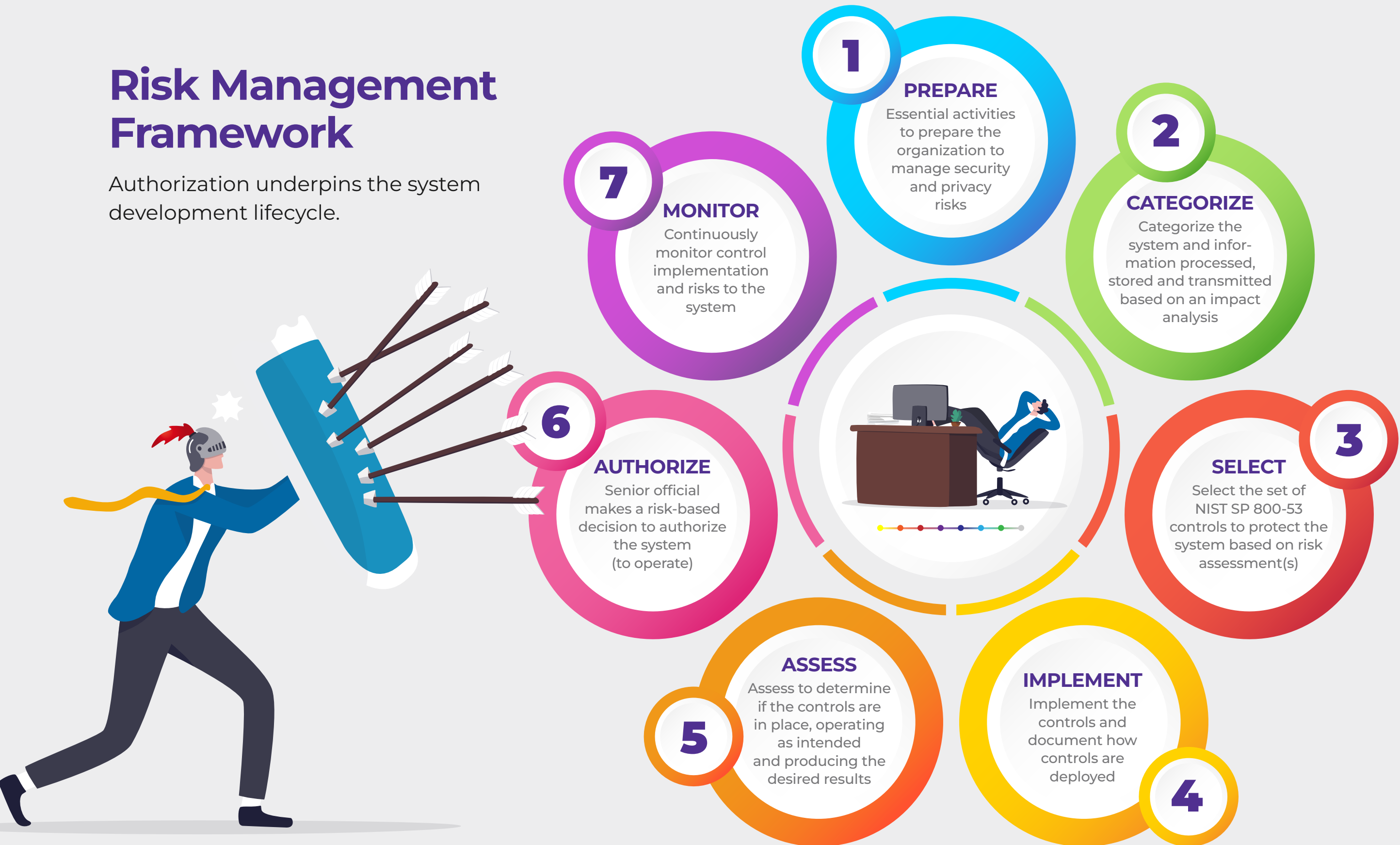
**Blair Heiserman, CISO, NIST**

“NIST is a standards organization, so obviously we’d love for people to abide by standards that makes integration easier ... so you’re speaking about the same vulnerability, the same exposure. It makes sure that everyone is talking at

the same level of criticality about something in their environment, which helps focus and prioritize,” Heiserman said. ✨

# Risk Management Framework

Authorization underpins the system development lifecycle.





# maximus


## How cATO Supports Better Cybersecurity

A continuous authorization to operate (cATO) can help federal agencies improve cybersecurity and software modernization efforts in a cloud environment.

---

**Tim Meyers, VP, Federal Cybersecurity, Maximus**

---

 **Why is continuous ATO (cATO) necessary for robust cybersecurity strategies and how does it aid agencies in meeting current cybersecurity directives?**

**Meyers** While each federal agency has a unique mission, they share a common purpose: to serve American citizens by providing reliable, secure and timely services. To do this, agencies require secure, scalable systems and applications to quickly and effectively deliver these services. DevSecOps is vital to that journey. But leveraging secure development methodologies is not enough, agencies face greater bottlenecks during the process of obtaining an Authorization to Operate (ATO). At Maximus, we believe that Continuous ATO (cATO) is essential to federal cybersecurity strategies. cATO automates the ATO process and deepens cybersecurity by establishing checkpoints throughout product lifecycle development. With cATO, agencies have more control, securing their “outside-in” strategies (i.e., web interface security) as well as their “inside-out” strategies with greater depth of segmentation. (ctd.)





**“cATO is a safety check: it ensures the security and safety of the product or program and keeps pace with development.”**

**—Tim Meyers,  
VP, Federal Cybersecurity,  
Maximus**

### **How does cATO support improved DevSecOps?**

**Meyers** With DevSecOps, you are accelerating the application development lifecycle. cATO takes this acceleration to another level, enabling the DevSecOps engine to move even faster. cATO is a safety check: it ensures the security and safety of the product or program keeps pace with development. When done properly, it allows developers to develop applications faster and security teams to identify security vulnerabilities and risks quicker while simultaneously assessing points of “go” or “no-go” all along the way. For example, we enabled a current customer to decrease their average Plan of Action Milestones (POAM) time-to-close by 93%. This is just one example of how cATO can truly accelerate the Software Development Life Cycle (SDLC).

### **What challenges do agencies face when enabling cATO capabilities?**

**Meyers** The biggest challenge for many agencies is shifting how they are currently developing applications. cATO requires agencies to expand beyond traditional application development methodologies, such as Waterfall, by bringing security to the forefront of the application development lifecycle rather than tacking it on at the end. For instance, we help our customers by integrating CI/CD (Continuous Integration/Continuous Delivery) pipelines with their DevSecOps. By doing this, we are creating the right environment of security tools that can correctly identify vulnerabilities at each stage.

### **How is industry prioritizing continuous ATO?**

**Meyers** I believe industry understands that government requires speed and agility to deliver enhanced services to citizens, and cATO is an enabler. At Maximus, we prioritize cATO because it allows agencies to keep pace with innovation while keeping security front-of-mind and liberating resources, time and budget to focus on what matters most: mission delivery. ✨



# Reinventing What's Possible in Cybersecurity

Our full-spectrum cybersecurity services deliver unrivaled protection and defense. From strategy, policy, and operations to implementation, we stay mission-focused.

**maximus**  
[maximus.com/cybersecurity](https://maximus.com/cybersecurity)





## DOD Releases New Continuous ATO Initiative for ‘Active’ Cybersecurity

The initiative will help defense leaders develop more aggressive cyber defenses.

BY KATE MACRI

The Defense Department launched a new cybersecurity initiative that will allow for continuous monitoring of cloud systems as part of a department-wide shift from passive to active cybersecurity practices.

The initiative calls for continuous authorization to operate (cATO), which DOD touts as an improvement upon its Risk Management Framework (RMF), which previously relied on one-time ATO sign-offs on systems or technologies.

Continuous authorization to operate allows DOD to engage in real-time monitoring of cyber risk. A cATO does not expire as long as the required real-time risk posture is maintained, according to a DOD memo signed by DOD CISO David McKeown.

Jason Weiss, DOD’s chief software officer who has since left the department, told GovCIO Media & Research in an email that the cATO memo intends to “build” off current DevSecOps initiatives throughout the agency.

“The memo represents a concerted effort to raise the bar beyond what an



existing paper document-oriented authorization to operate (ATO) requires,” Weiss said. “Different services have created different standards and understanding of what it takes to reach this level of maturity. This memo is the first step to rectify this problem by spelling out very specific ingredients that must be present, and it captures that not every system can or should qualify for a cATO.”

The initiative comes as federal cybersecurity continues to be a major point of reform for federal agencies and

follows a May 2021 executive order that calls for federal agencies to immediately begin deployment of zero trust architectures. In December 2021, DOD also created a new zero trust office within the Office of the CIO to spearhead zero trust deployment.

“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,” according to the memo. (ctd.)



# Jason Weiss

Former Chief Software  
Officer, DOD



The memo said authorizing officials must achieve three metrics to reach cATO:

- Continuous visibility and monitoring of “key cybersecurity activities” within the system they’re authorizing
- The ability to conduct active cyber defense in order to respond to cyber threats in real time
- The adoption and use of an approved DevSecOps reference design and embrace the department’s enterprise DevSecOps strategy

DOD believes cATO is key for apt cybersecurity because most IT and OT systems do not operate independently of each other, and bad actors are more likely to move laterally across systems and networks than in years past.

“The goal of a cATO is to formalize and monitor the connections across these systems of systems to deliver cyber resilient capabilities to warfighters at the speed of relevance,” according to the memo.

In practice, DOD expects authorizing officials to “feed” security controls into a dashboard view, “providing a real time and robust mechanism for AOs to view the environment.” This will allow authorizing officials to make better decisions regarding current cyber threats and allow defensive cyber operations to respond more quickly to threats based on “current system [cyber] posture.”

The memo also calls for DOD components to adopt an “active” cybersecurity mindset. Scanning and patching are no longer viable strategies for cybersecurity, and “systems must be able to show a real, or near real-time ability to deploy appropriate countermeasures to thwart cyber adversaries.”

As part of the cATO initiative, DOD also outlined requirements for securing the software supply chain. To reduce human error and adequately track software through a software bill of materials (SBOM), DOD components and military service branches must adopt an approved software platform and development pipelines, according to the memo. 🌟



**“Different services have created different standards and understanding of what it takes to reach this level of maturity. This memo is the first step to rectify this problem by spelling out very specific ingredients that must be present, and it captures that not every system can or should qualify for a cATO.”**

**—Jason Weiss, Former Chief Software Officer, DOD**