cATO Working Group

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) to begin its cATO Working Group, August 2024

During the initial cATO (Continual Authorization to Operate) working group, technology experts from government and industry discussed the challenges and opportunities with existing cATO processes in the Federal government.

Current cATO Landscape

"ATOs cost too much, take too long, and focus heavily on compliance versus security."

Current ATO processes often take up to 6 months or longer, despite ongoing efforts to shift left. Working group members concur the process must accelerate in order to meet the rapid fluidity of technology advancements and adversarial tactics. Challenges to accelerate the authorization process are plenty, but members point to culture as a top means of resistance to change.

Members also note that ATOs often result in compliance documentation, rather than meaningful security outcomes. While there are cases where the ATO process identifies significant security risks, too often the resources expended on ATO do not result in greater security outcomes.

The working group discussed the myriad challenges with accelerating authorizations and better orchestrating cATO throughout the enterprise.

Accelerating ATO

Members concur that the primary challenge of cATO is its time-consuming nature. Members discussed automation, changes to workplace and leadership culture, and better information sharing as potential ways to accelerate the ATO process.

Automation

"The focus is often on automation, but that's just one component of a successful OA [Ongoing Authorization] program."

Members acknowledge several opportunities that already exist to automate parts of the ATO process, such as the second version of FEDRAMP and OSCAL. Members recommend starting with a well defined life-cycle management strategy to identify the controls that can be automated and leverage existing capabilities to automate what is possible.

Data gathering and preparation is especially important to ready systems to be machine readable and capable of inheriting controls. Members believe that the technology already exists to integrate machine readable policies into OSCAL and add values that could measure the ability of a control.

Automation is also important to develop some consistency throughout the ATO process, especially as auditors with different skill sets and skill levels assess ATOs.

Culture of People and Processes

“The human aspect is something that shouldn't be tuned down. It still takes humans to build trust.”

Members agree that many of the challenges agencies experience with ATO are not driven by technology, rather the people and processes involved. Some members have witnessed significant resistance from system owners to go through the ATO process and focus on continuous monitoring.

One member noted that few people within the security community are trained to speak the language of business. Learning to articulate the value of implementing security controls and providing mission assurance to portfolio managers, chief privacy officers, and office of legal counsel could help move the process along more quickly.

Another member argued that the largest issues agencies experience aren’t with platforms and security baselines, but with the processes involved with continuously deploying and using technologies on an existing system.

Suppliers also consider ATO a burdensome process, especially smaller vendors and services offering smaller technology pilots. Many small vendors build valuable solutions, but don’t have the resources to hire experts to develop their own information security programs. Working group members mention they want to find a solution to support small vendors through the ATO process.

Members acknowledge that the agendas of executives often hinder plans to improve the ATO process in the long-term. Executives are often working to meet short-term regulatory guidelines, which results in personnel working in silos to meet ATO deadlines as quickly as possible.

Information Sharing

To bridge the gap between small vendors and the ATO process, and to accelerate the ATO process in general, members recommended improved information sharing. Some members believe that the only way to maintain security and compliance of systems is to open the process and remove silos. Although a significant cultural shift is required and some information must remain private, agencies could pull open source ATO information from a database and contribute back any changes they’ve made.

“No single vendor is able to handle security with how fast things are changing.”

On the other hand, the mechanics of opening processes and information to the public domain becomes very challenging. Starting at the statutory level, all system information becomes sensitive information and would have to go through the legal process for publicly disclosing sensitive information. Oftentimes, that creates more risk to the organization.

Orchestrating ATO

“Orchestration doesn’t necessarily mean automation, although it can. It’s taking a process and making sure the steps connect.”

The human element distinguishes ATO automation from orchestration. As one member said, “…orchestration gives a sense of someone there” to serve as checkpoints throughout the process.

Another member noted that while many aspects of the ATO process can be automated, agencies should first improve processes before considering automation. Orchestrating steps and workflows is the precursor to automation. Unfortunately, many agencies make the mistake of automating poor processes.

As agencies look to automate, they should first identify workflows and build automations around those workflows and the actual work being done. This helps to build in reminders and tasks to alert system owners to take specific action at the right time.

Security Controls

“ATO is really just the culmination of security control selection assessment and then ultimately risk management decisions.”

Working group members note that one of the most time consuming aspects of the ATO process is selecting security controls. Currently, the number of baseline controls are in the hundreds. One member recommends reducing the number of controls to the most critical, but that process is challenging in and of itself. Agencies should also examine whether the baseline controls provide value to the specific system, mission, or business line.

Risk Analysis & Metrics

“The ATO process doesn't do a good job of giving you a declaration of the security state of the information system.”

Evaluating and analyzing the risk level of a system is often missing during the ATO process. Members shared that agencies should declare the security state of their systems and be able to articulate the acceptable risk parameters of a given system. Knowing a system’s acceptable level of risk would enable agencies to more accurately choose controls. Taking a quantitative risk approach and centralized decision making can help determine risk, but ultimately agencies must rely on what’s prescribed in the FISMA law.

One member noted that Inspector General reports reveal the common denominators of risk across agencies. Most risk is due to a lack of common control inheritance from common control providers, a lack of management and oversight of system level or system specific control implementations, and issues with budget. Another member is addressing risk by incorporating security requirements from pre acquisition all the way through to deployment.

Final Thoughts from Working Group Members

- We're in this moment of micro services, large language learning models, and artificial intelligence, and it's moving so fast that we have to figure out how to orchestrate and automate [ATO] at the same time.
- I don't think there's one answer to such a big problem. It'll be a multiplicity of solutions that could bear on this big problem.
- We don't need to overcomplicate it. We've been doing configuration management forever, and cATO is just another flavor of configuration management. Automating the exchange of important ATO data will hopefully become easier with OSCAL or another standardized language.
- Security is the government's replacement word for quality management, which is why it gets overloaded. It's not security, it's the entire quality, confidentiality, integrity and availability of a system.
- Our authorization processes must align with our development processes. If nothing else is going to drive us to change, it should be because the development process has changed. The adversary moves at a much faster clip, which means whatever we're producing is obsolete.
- We're all trying to recreate the same exact thing. Agencies need to resolve this culture of fear and start sharing information.
- We need to come up with a way that protects our own contingency plans and incident response playbooks in such a way that the adversary is not able to obtain them, which has been disclosed in breaches in the past.
- We have other critical infrastructure sectors besides websites, so we need to develop a model that not just applies to simple systems like websites, but also the operational environments as well.
- We're using processes that are so old. Does it make sense to use these processes for ATO? Is there value in everything that we're collecting? Are we collecting it just to collect it? If it has no value, why are we doing it?

LEARN MORE AT:

[WEBSITE]