RIVA

Achieving Continuous Authority to Operate (cATO)

Austin O'Donoghue
Director of Cloud and Infrastructure

aodonoghue@rivasolutionsinc.com
www.rivasolutionsinc.com

Executive Summary

In an increasingly digital world, where threats to security evolve rapidly, it is critical for government agencies to maintain a robust, adaptable, and comprehensive cybersecurity strategy to protect the diverse set of products and solutions used to execute on mission. This paper explores the evolution and benefits of Continuous Authority to Operate (cATO), a solution that leverages real-time risk management and automated compliance monitoring to significantly improve an agency's security posture ensuring IT products and solutions move from ideation to production delivery rapidly and securely.

Traditional Authority to Operate (ATO) processes, characterized by periodic, point-in-time assessments, are increasingly inadequate to meet today's security and rapid development needs. This is especially true in the context of government operations where safeguarding sensitive public data and maintaining public trust is paramount. The limitations of traditional ATO can lead to substantial risks, including security breaches and non-compliance with federal mandates and regulations.

cATO, offers a comprehensive security framework that affords application development organizations a mechanism to assert their compliance with security controls and receive authorization to launch these workloads into production should the governing body assent. cATO is a great option for application development organizations that operate in a forward-looking, continuous delivery manner who continuously assert their security compliance and receive authority to operate their workloads.

This white paper presents a comprehensive guide to understanding and implementing cATO within government agencies. It explores the inherent challenges of traditional ATO, the solutions provided by cATO, the benefits realized, and guide to successful implementation. Through a detailed case study, this paper also highlights a successful implementation of cATO in a government agency, providing a real-world example of the transformational benefits cATO can bring.

Introduction

Government agencies, responsible for safeguarding a wealth of sensitive data, face the daunting task of maintaining a robust security posture while continuously adapting and deploying new products and solutions. This task is further complicated by stringent regulatory requirements designed to ensure data protection and public trust. For many years, Authority to Operate (ATO) processes, involving periodic security assessments and authorizations, have been employed by agencies to manage these risks.

However, the rapid pace of digital transformation and evolving threat landscape is revealing significant limitations in the traditional ATO approach. Hence, the need for a more dynamic, real-time approach has become more apparent than ever. Enter Continuous Authority to Operate (cATO) – a proactive approach that revolutionizes risk management by assessing, monitoring, and mitigating security risks in real-time, thereby providing agencies with the agility and responsiveness necessary to navigate an ever-evolving digital environment. This paper seeks to provide an in-depth look into the transformation from traditional ATO to cATO, highlighting the importance, benefits, and implementation steps of cATO within the specific context of government operations.

Table of Contents

The Challenge: Traditional ATO

The canonical ATO process involves a comprehensive assessment of security posture through the compliance with controls, standards, and regulations, and the analysis and validation of risks and compliance. Base line tests and evaluations are performed and documented. This process is often lengthy and onerous taking months and sometimes years to complete.

Here are three challenges to Traditional ATO:

With the fast-paced nature of digital transformation, changes occur at a rapid clip, outpacing the ability of traditional ATO processes to keep up. By the time one assessment is completed, the digital environment may have already evolved, leaving newly emerged vulnerabilities undetected. This exposes government agencies to potential threats between assessments, creating 'blind spots' that can be exploited by malicious actors.

Secondly, the traditional ATO process is often cumbersome and resource-intensive, involving manual and time-consuming tasks to review and authorize systems. This can lead to a backlog of systems awaiting approval, causing delays that hamper the agility and responsiveness of government agencies in deploying or updating systems.

Lastly, the traditional ATO's point-in-time approach struggles to align with the continuous nature of regulatory compliance requirements. Regulations like the Federal Information Security Management Act (FISMA) and the Federal Risk and Authorization Management Program (FedRAMP) mandate continuous monitoring and ongoing authorization, a demand that traditional ATO struggles to meet efficiently.

While the scope and scale of the ATO process is warranted as the data residing within government systems are often protected health, consumer, personally identifiable, or related to national security, a framework these security controls be complied with while avoiding bottlenecks of the delivery of value is critical for future oriented application development teams.

The Solution: Continuous Authority to Operate (cATO)

In response to the challenges and limitations posed by traditional ATO, the concept of Continuous Authority to Operate (cATO) has emerged as a transformative solution.

cATO is a strategy that shifts from point-in-time to real-time continuous monitoring of systems, providing an ongoing assessment of an agency's security risks and compliance posture. By leveraging advanced technologies such as automation, artificial intelligence, and machine learning, cATO effectively keeps pace with rapidly changing digital environments and evolving threats, addressing the inadequacies of the traditional ATO process. The continuous ATO process seeks not to replace security practices but to extend them, enabling the reuse of previous tests and documentation increments so that updates to the ATO can be as iterative as the software development and value delivery they support.

The three tenets of a continuous Authority to Operate are:

1. Baseline security compliance
2. Continuously monitor
3. Respond in real time

The continuous ATO process seeks not to supplant these security practices but to extend them, enabling the reuse of previous test and documentation increments so that updates to the ATO can be as iterative as the software development and value delivery they support.

The three tenets of a continuous Authority to Operate are:

1. Baseline security compliance
2. Continuously monitor
3. Respond in real time

The traditional ATO process falls well in line with tenet one. The innovation of a cATO is the continuous monitoring for incremental change, so that if a change has security impact, it can be reacted to accordingly.

cATO and Risk Management

A cATO mitigates risk in real time, obviating the need for many provisional ATOs or for delays in customer value delivery due to the length of the vetting process. The continuous monitoring of a cATO also allows the organization to react to the publication of new CVEs in real time, enabled by the programmatic and incremental nature of a cATO through tools such a SBOM analysis and machine-readable security controls.

cATO and Government Compliance

cATO is Continuous Compliance. A cATO practice enables organizations to assert, maintain, and document their compliance with any applicable FISMA, FEDRAMP, or NIST controls (among others).

The cATO process delivers these key security features using modern continuous integration, continuous deployment, and continuous monitoring practices.

During continuous integration, code quality scans, software composition analysis, dependency analysis, and peer review assure that the baseline security compliance levels dictated by the mission are met.

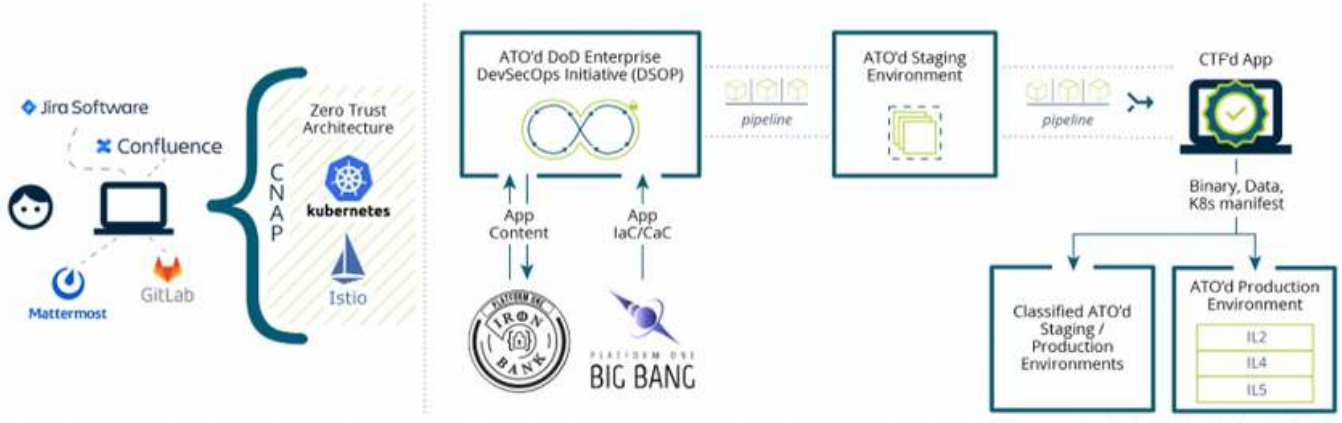
Continuous deployment of software packages in a security compliance manner involves deploying these software packages to secure supply change repositories after they have been satisfactorily scanned and vetted.

Continuous Monitoring identifies and enables your team to react in real time to any events that impact your security posture, reliability, usability, or other performance characteristics.

[Case Study] Successful cATO Implementation US Air Force Platform One

Rackner, a member of Team RIVA, contributed to the successful implementation of cATO at US Air Force's Platform One (P1) supporting P1's Authorizing Official who championed the creation, development, and acceptance of cATO as a practice. Prior to the adoption of cATO, the traditional DoD ATO process to accredit software was a mostly manual process taking over 8 months to complete.

To achieve a cATO, a system must embrace the DoD Enterprise DevSecOps Strategy, aligning to an approved DevSecOps Reference Design. This strategy creates a cultural change that implements the full and open agile collaboration of what have traditionally been separate disciplines. Incorporating development, security, and operations together closes gaps with baked in safeguards and monitoring functions that span the entire software supply chain. The DevSecOps Strategy supports a "Pathway to a Reference Design" whereby new architectures can be submitted for evaluation. Rackner was critical in driving DevSecOps adoption and cultural change necessary to achieve cATO on four P1 software factory components: Iron Bank, Big Bang, Cloud Narrative Access Point, and Party Bus.



DoD DevSecOps Reference Design

RIVA

Iron Bank

One of the Platform One (P1) components is called Iron Bank, which is the DoD Centralized Container Hardening Repository where applications (GOTS, COTS, open source) that conduct business with the federal government or DoD have their hardened application running on P1.

All Iron Bank containers are continuous scanned within their build pipelines, the scans from the build pipelines are provided in the Iron Bank console and scans are also centralized within the Vulnerability Assessment Tracker (VAT) where all compliance and vulnerability scans are being sent to.

Big Bang

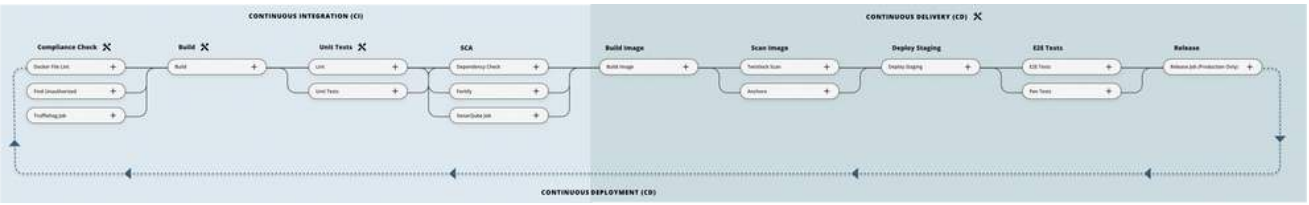
Another P1 service is the Big Bang Infrastructure. The Big Bang is a declarative, continuous delivery tool for deploying DoD hardened and approved packages into a Kubernetes cluster. Big Bang is a Helm Chart that is used to deploy a DevSecOps Platform on a Kubernetes Cluster. The DevSecOps Platform is composed of application packages which are bundled as helm charts that leverage Iron Bank hardened container images.

Cloud Native Access Point

The Cloud Native Access Point (CNAP) is how P1 enforces Comply2Connect security on Platform One, AppGate device inspection blocks any out of compliance endpoints, AppGate and the Palo Alto Firewall allow and deny rule configurations. This is accomplished in two pieces; a Palo Alto firewall and an AppGate (SDP VPN) controller. Users must connect to AppGate to access tools at IL-4 and IL-5, Role-based access control (RBAC), network micro-segmentation, and Layer 7 threat protection are implemented by CNAP.

Party Bus

Lastly, Party Bus is a cATO enabled DevSecOps service for government software programs looking for rapid development of approved, working mission applications to the warfighter.



Party Bus CI/CD

Platform One has assisted with bringing innovative technologies to the hands of the warfighter and is leading innovation efforts for larger enclaves like the advanced battle management system (ABMS) in the effort to create next generation command and control (C2) systems. While the transition to cATO may require considerable effort and a cultural shift, the benefits in terms of enhanced security, improved compliance, and increased efficiency make it a worthwhile pursuit for government agencies navigating an increasingly complex digital environment. Team RIVA and Racknar are excited to be a part of the journey.

Implementing cATO in a Government Agency

Transitioning to a cATO model may seem like a formidable task, but with a clear plan and the right strategies, government agencies can make the transition more manageable. Here are steps to consider when implementing cATO:

Conducting a Gap Analysis

Understanding the security posture of the organization through a careful and detailed gap analysis is the first step in implementing a cATO practice. Today this would involve analyzing your organization's Zero Trust maturity and identifying your trust perimeters, trust relationships, and micro-segmentation for evaluation. First, DevSecOps practitioners define the scope of the analysis with rigor. Then the appropriate security controls, standards, and best practices with which to comply are selected and documented. Along with selecting the controls to adhere to, risks are identified within applications and environments which may expose the organization to security risk. Once the scope, standards, and risks are understood, the task of identifying current gaps in security is set upon. The set of gaps is then prioritized, and an action plan is formulated to redress, minimize, or otherwise eliminate these security risks.

Define Requirements and Implement cATO

We prescribe the following ten steps towards definite your requirements and implementing cATO :

1. Identify your organization's specific security and compliance requirements
2. Develop an Implementation Plan
3. Conduct Staff Training
4. Integrate with Existing Systems
5. Configure Settings and Security Controls
6. Establish Continuous Monitoring Processes
7. Perform Initial Assessments and Remediation
8. Establish Risk Management Framework
9. Monitor, Assess, and Renew
10. Maintain Documentation and Reporting

Remember the implementation process may vary based on an agency's specific requirements and the chosen cATO tools. It is recommended to consult with experts or seek assistance from the tool vendors during the implementation to ensure a successful deployment.

Continuous Monitoring and Adjustments

Continuous monitoring and regular adjustments are crucial aspects of the Continuous Authority to Operate (cATO) strategy to ensure the ongoing effectiveness and relevance of the security measures in the face of evolving threats and changes in the organization's digital environment. Here are the key reasons why continuous monitoring and regular adjustments are important:

1. Evolving Threat Landscape
2. Timely Detection of Security Incidents
3. Proactive Risk Management
4. Compliance with Regulations and Standards
5. Changes in the Digital Environment
6. Adaptive Risk Management
7. Enhanced Incident Response Capabilities

Continuous monitoring and regular adjustments to the cATO strategy are vital for organizations to maintain a robust security posture, effectively manage risks, detect and respond to emerging threats, comply with regulations, and adapt to changes in the digital environment. By prioritizing these activities, organizations can stay ahead of potential security risks and safeguard their critical systems and data.

Benefits of cATO

The transition to cATO represents more than a change in security strategy for government agencies; it marks a significant shift towards proactive risk management and compliance. Here are four benefits of adopting cATO:

Cost Savings

By implementing cATO and continuous monitoring, organizations can identify and address security vulnerabilities in a proactive manner, reducing the likelihood of costly security incidents or breaches. When incidents do occur, a prompt response minimizes the financial impact associated with extended downtime, data loss, or system recovery. Timely identification and remediation of vulnerabilities through continuous monitoring can reduce the cost of remediation compared to addressing them after a breach or compliance violation.

Reduced Downtime

Through the implementation of continuous monitoring via robust tools and processes, organizations can proactively detect system abnormalities, performance degradations, and potential threats. This early detection helps prevent system failures and minimizes operational disruptions, thereby significantly reducing downtime.

Improved Compliance Rates

Continuous monitoring, through its proactive identification and remediation of compliance gaps, not only ensures that security controls remain effective and compliant with industry regulations but also assists organizations in maintaining a higher compliance level, thereby circumventing potential penalties or legal repercussions.

Enhanced Incident Response

With real-time visibility into security events provided by continuous monitoring, organizations can swiftly detect and react to incidents. By integrating a well-defined incident response plan into the cATO strategy, organizations can enhance their response capabilities, dramatically reduce detection and mitigation times, and limit the impact on business operations.

Conclusion

In the face of an ever-evolving digital landscape, government agencies are entrusted with the formidable task of safeguarding sensitive data, maintaining public trust, and adhering to strict regulatory mandates. The limitations of traditional Authority to Operate (ATO) processes, with their periodic assessments and approvals, are increasingly unable to cope with the rapid pace of digital transformation and the consequent cyber threats.

The Continuous Authority to Operate (cATO) model presents an innovative and essential solution. It not only redefines risk management by offering real-time, continuous monitoring of systems but also aligns with the ongoing nature of government regulatory requirements. Through automation, artificial intelligence, and machine learning, cATO empowers government agencies to keep pace with rapidly changing digital environments and evolving threats.

This white paper has sought to provide a comprehensive understanding of cATO and its transformative benefits for government agencies, illustrated through a real-world case study and implementation guide. With enhanced security, improved compliance, increased efficiency, and reinforced public trust, the compelling value proposition of cATO is clear.

The shift to cATO may represent a significant undertaking, requiring a cultural shift, an overhaul of procedures, and the adoption of new technologies. Yet, the remarkable benefits it offers make it an indispensable pursuit for government agencies aiming to maintain a robust cybersecurity posture in the digital age. As our digital landscape continues to evolve and expand, the need for proactive, dynamic, and continuous approaches to security and compliance, such as cATO, will only become more critical.

Austin O'Donoghue
Director of Cloud and Infrastructure

aodonoghue@rivasolutionsinc.com
www.rivasolutionsinc.com

RIVA