ATARC

WHITEPAPER

Zero Trust, Zero Delays: Enabling Continuous ATOs for Mission-Ready Software

Not for Attribution
(Chatham House Rules)

IN PARTNERSHIP WITH

Chainguard

Executive Summary

Federal agencies are under increasing pressure to deliver secure digital capabilities at speed. While cloud adoption, DevSecOps, and Zero Trust architectures have advanced significantly, the Authorization to Operate (ATO) process continues to lag behind modern software delivery.

This roundtable explored how agencies can transition from traditional, static ATO processes to continuous authorization models that better align with how software is built and deployed today. The discussion made clear that the limiting factor is no longer technology. The core challenge lies in how organizations approach risk, ownership, and compliance.

Participants described a future state in which security is embedded directly into development pipelines, platforms provide pre-authorized environments, and software can move into production in hours or days instead of months. Achieving that future requires a shift away from checklist-driven compliance toward a model where systems continuously demonstrate their security posture.

1. The Persistent ATO Challenge

Across government, ATO timelines remain a major barrier to mission delivery. Even in organizations that have embraced modern engineering practices, authorization processes are often slow, manual, and disconnected from how systems are actually built.

A common pattern continues to emerge. Agencies procure or develop software, deploy it into an environment, and only then begin to fully understand the security requirements needed to operate it. This leads to delays, rework, and frustration across both mission and security teams.

The ATO process, in many cases, has become less about ensuring security and more about producing documentation. As a result, it struggles to keep pace with iterative development and continuous deployment models.

2. Continuous Authorization as the New Model

Participants consistently pointed to continuous ATO as the direction forward. In this model, authorization is not a one-time event but an ongoing condition that is maintained through automation, monitoring, and engineering discipline.

Security controls are enforced within the development pipeline. Code is scanned, validated, and tested before it reaches production. Runtime environments are continuously monitored, and systems are regularly rebuilt to ensure integrity.

This approach shifts the focus from producing an authorization package to proving, in real time, that a system meets required security standards. Authorization becomes an outcome of the system's operation rather than a separate process.

3. Platform-Centric Approaches

A major theme of the discussion was the importance of platforms in enabling continuous ATO. Instead of requiring each program or system owner to build and secure their own environment, agencies can establish shared, pre-authorized platforms.

These platforms provide built-in security controls, identity management, logging, and monitoring. Mission owners deploy their applications into these environments and inherit much of the compliance posture.

This model simplifies the process for mission teams and reduces variability across systems. It also shifts responsibility toward platform providers, who are better positioned to implement and maintain consistent security controls.

4. DevSecOps Progress and Limitations

While DevSecOps has been widely adopted in principle, implementation remains uneven. Many organizations have tools and frameworks in place, but they are not always integrated with compliance processes.

Security often remains a downstream activity, separate from development workflows. As a result, the benefits of DevSecOps are not fully realized in the ATO process.

The most mature environments are those where development, security, and operations are tightly integrated. In these cases, security is part of the development lifecycle from the beginning, and compliance requirements are addressed continuously rather than at the end.

5. The Impact of Modern Architectures

Containerization and cloud-native architectures are enabling new approaches to authorization. These technologies allow systems to be rebuilt, redeployed, and validated quickly and consistently.

Instead of treating systems as static entities, organizations can adopt models where workloads are ephemeral and continuously refreshed. This supports a more dynamic approach to security, where validation happens repeatedly rather than once.

These capabilities align closely with Zero Trust principles, emphasizing continuous verification and minimizing reliance on long-lived trust assumptions.

6. Defining Requirements Up Front

One of the most consistent challenges discussed was the lack of clarity around requirements, particularly at the beginning of a project. Many mission owners do not fully understand the data they are handling or the associated security implications.

This lack of clarity leads to misalignment between stakeholders and delays later in the process. Security and compliance teams are often brought in after key decisions have already been made.

A more effective approach requires early collaboration across mission, security, and engineering teams. Clear understanding of data, risk, and system purpose must be established before development begins.

7. Organizational and Cultural Barriers

Technology alone will not solve the ATO challenge. Participants emphasized that cultural and organizational factors are often the biggest obstacles.

In many environments, compliance is treated as a separate function, and individuals focus on completing their portion of the process rather than ensuring overall system security. Risk decisions are fragmented, and accountability is unclear.

Moving to continuous ATO requires a different mindset. Leaders must prioritize mission outcomes and empower teams to adopt new approaches. This includes accepting new models of risk management and moving away from strictly checklist-based compliance.

8. Managing Complexity in Shared Environments

As agencies adopt platform-based approaches, new challenges arise around managing shared environments. These include ensuring proper data segmentation, maintaining visibility across systems, and enforcing consistent identity and access controls.

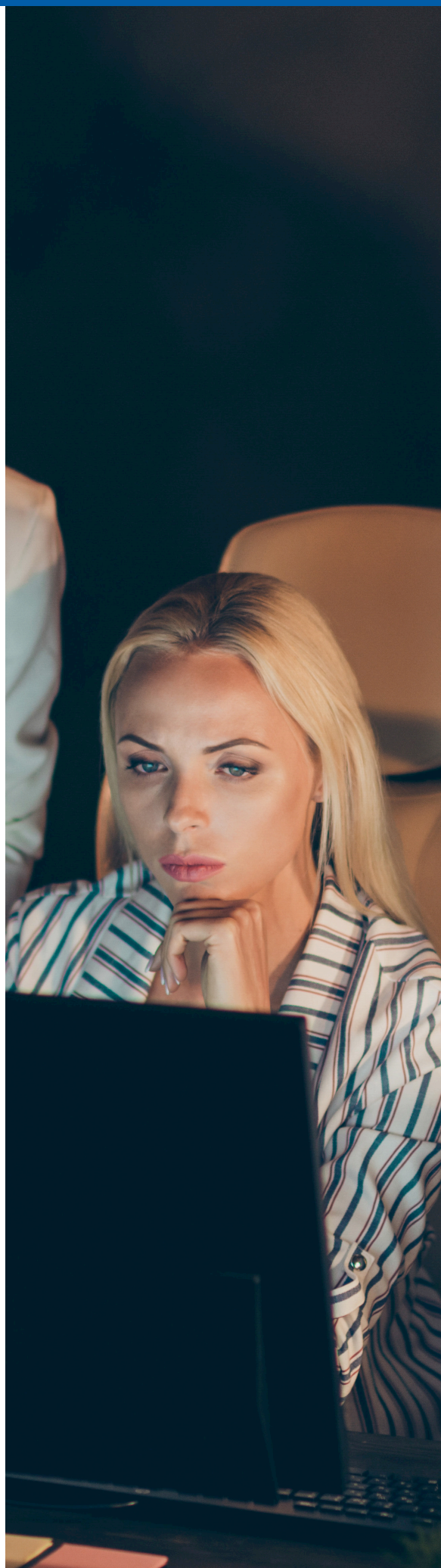
Modern cloud architectures provide tools to address these challenges, but they require careful design and governance. Agencies must balance the efficiency of shared platforms with the need to maintain isolation and accountability.

9. Integrating Privacy and Security

Privacy remains a critical component of the authorization process. Unlike many technical controls, privacy assessments are often qualitative and require a detailed understanding of how data is used and shared.

Integrating privacy into continuous ATO models requires earlier and more consistent engagement. Privacy considerations must be incorporated into system design and development, rather than addressed as a separate step.

This reinforces the need for a holistic approach, where security, privacy, and engineering are aligned from the outset.



10. CMMC and the Future of Vendor Readiness

A significant portion of the discussion focused on the growing role of the Cybersecurity Maturity Model Certification (CMMC) framework and its implications for both agencies and industry partners. Participants agreed that CMMC is no longer viewed as a future requirement or isolated compliance exercise. Instead, it is rapidly becoming a baseline expectation for organizations seeking to operate within the federal ecosystem, particularly in Department of Defense environments.

The discussion highlighted a persistent gap between government expectations and vendor preparedness. Participants expressed frustration that many vendors continue to approach federal cybersecurity requirements reactively, engaging with agencies before fully understanding the expectations associated with handling government data and operating within regulated environments. Several attendees noted that organizations entering the federal market must now arrive "cyber ready," with a clear understanding of applicable FAR, DFARS, NIST 800-171, and emerging CMMC requirements already embedded into their operations.

Participants emphasized that successful compliance is less about achieving perfection and more about demonstrating mature and repeatable risk management practices. Organizations are increasingly expected to maintain documented processes, continuous monitoring capabilities, and clear accountability structures. Known vulnerabilities, risk acceptance decisions, and remediation activities must be tracked and consistently managed rather than addressed informally or retroactively.

The group also discussed how acquisition practices are evolving alongside CMMC adoption. Agencies are increasingly incorporating cybersecurity certifications and compliance readiness into acquisition gate criteria. Rather than allowing broad participation from vendors with varying levels of maturity, agencies are beginning to establish clear go/no-go thresholds tied to certifications, control implementation, and security readiness. Participants noted that this approach reduces wasted effort for both government and industry while improving the quality of vendors entering the procurement process.

At the same time, attendees acknowledged that many organizations continue to struggle with unclear requirements, fragmented guidance, and limited internal expertise. Vendors often delay engaging auditors, compliance specialists, or security professionals until late in the process, creating unnecessary delays and confusion. Participants noted that government organizations also contribute to the problem through vague requirements, compressed procurement timelines, and inconsistent communication regarding expectations.

Automation and modern engineering practices were viewed as critical enablers for scaling CMMC compliance and accelerating authorization timelines. Participants described the growing use of AI-assisted pre-assessments, DevSecOps pipelines, automated control validation, and inheritable controls within shared platforms. These approaches allow organizations to identify compliance gaps earlier, continuously validate security posture, and reduce the manual burden associated with traditional authorization processes.

The conversation ultimately reinforced that CMMC is driving a broader cultural shift across government and industry. Compliance can no longer function as a standalone documentation exercise performed at the end of a project. Instead, cybersecurity readiness must become an integrated operational capability supported by leadership, engineering discipline, continuous validation, and close collaboration among mission owners, acquisition teams, security professionals, and industry partners.

11. Moving Forward

The federal government has the tools and knowledge needed to move beyond traditional ATO processes. The remaining challenge is adopting a model that aligns security with the speed and flexibility of modern software development.

Continuous authorization offers a path forward. By embedding security into systems, leveraging shared platforms, and focusing on real-time validation, agencies can reduce delays and improve mission outcomes.

The shift will not happen overnight. It will require sustained leadership, collaboration, and a willingness to change long-standing practices. But the direction is clear.

Security must evolve from a gatekeeping function into an integrated, continuous capability that enables, rather than delays, mission success.

Conclusion

The federal government has the tools and knowledge needed to move beyond traditional ATO processes. The remaining challenge is adopting a model that aligns security with the speed and flexibility of modern software development.

Continuous authorization offers a path forward. By embedding security into systems, leveraging shared platforms, and focusing on real-time validation, agencies can reduce delays and improve mission outcomes.
The shift will not happen overnight. It will require sustained leadership, collaboration, and a willingness to change long-standing practices. But the direction is clear.
Security must evolve from a gatekeeping function into an integrated, continuous capability that enables, rather than delays, mission success.