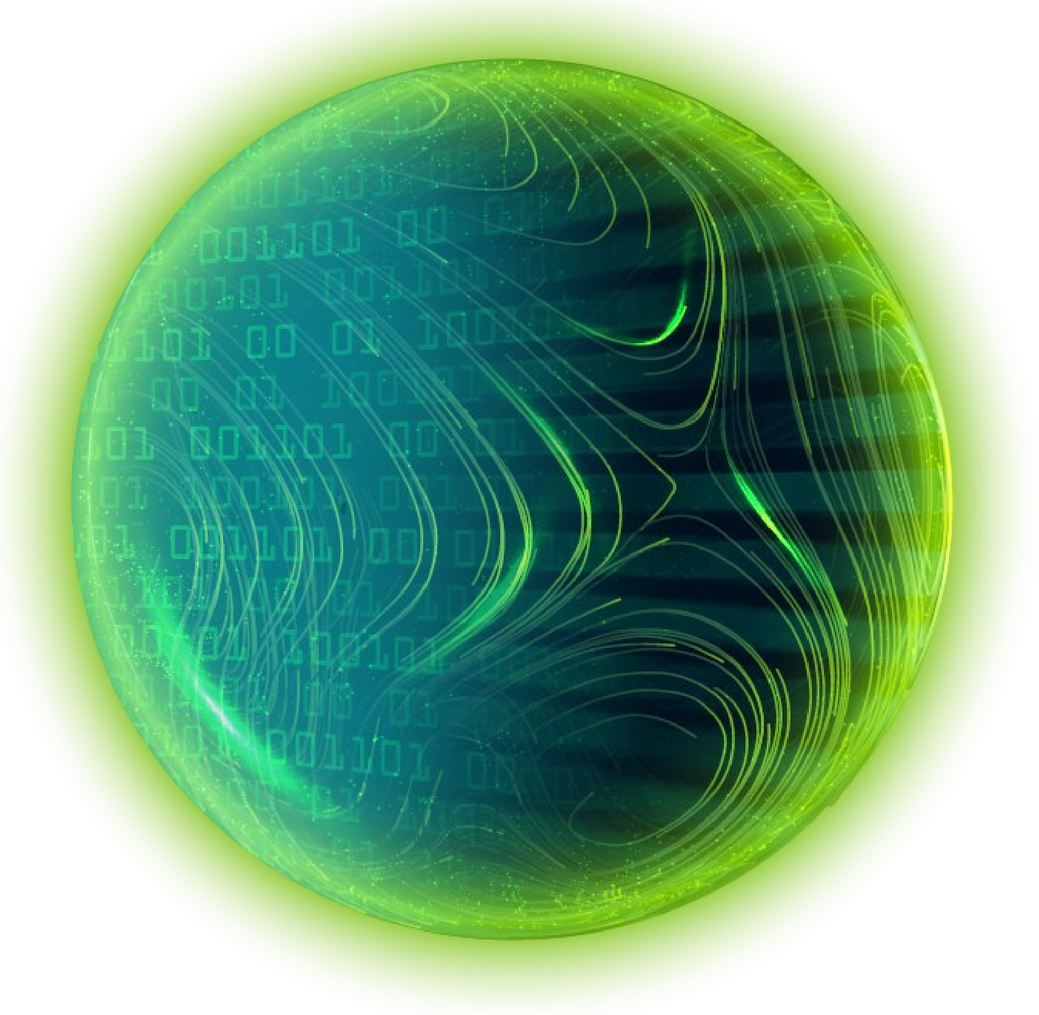
Deloitte.



Maturing cATO

Enabling Security & Compliance

MAKING AN IMPACT THAT MATTERS since 1845

Table of Contents

The Push Toward cATO

It is a classic problem: there is a capability that would greatly enhance your organization's ability to meet the mission, optimize processes, or simply make your life easier; but the Authority-to-Operate (ATO) process may take 6–18 months before you can use it. Managing risk is important, but there needs to be a way to deploy capabilities faster without sacrificing security.

At the same time, what about operations risk management in the "ever-evolving landscape of cybersecurity" as popular tech articles describe it? These articles contain a kernel of truth at their core: once deployed, your organization's risk management process needs to shift accordingly, accounting for changes in real time. There needs to be a way to move beyond point-in-time assessments, which may be outdated by the time they are complete, to a continuous evaluation of your risk posture.

Continuous ATOs (cATOs) (sometimes known as continuous authorization) can help you address both situations.[i] More than just a technical solution, cATOs represent a culture shift in how organizations look at risk, including revamping processes and training people. In this white paper, we will define risk, provide some examples of adopting cATOs, explain impacts for your organization, and show how Deloitte can help you get there.

What is Risk?

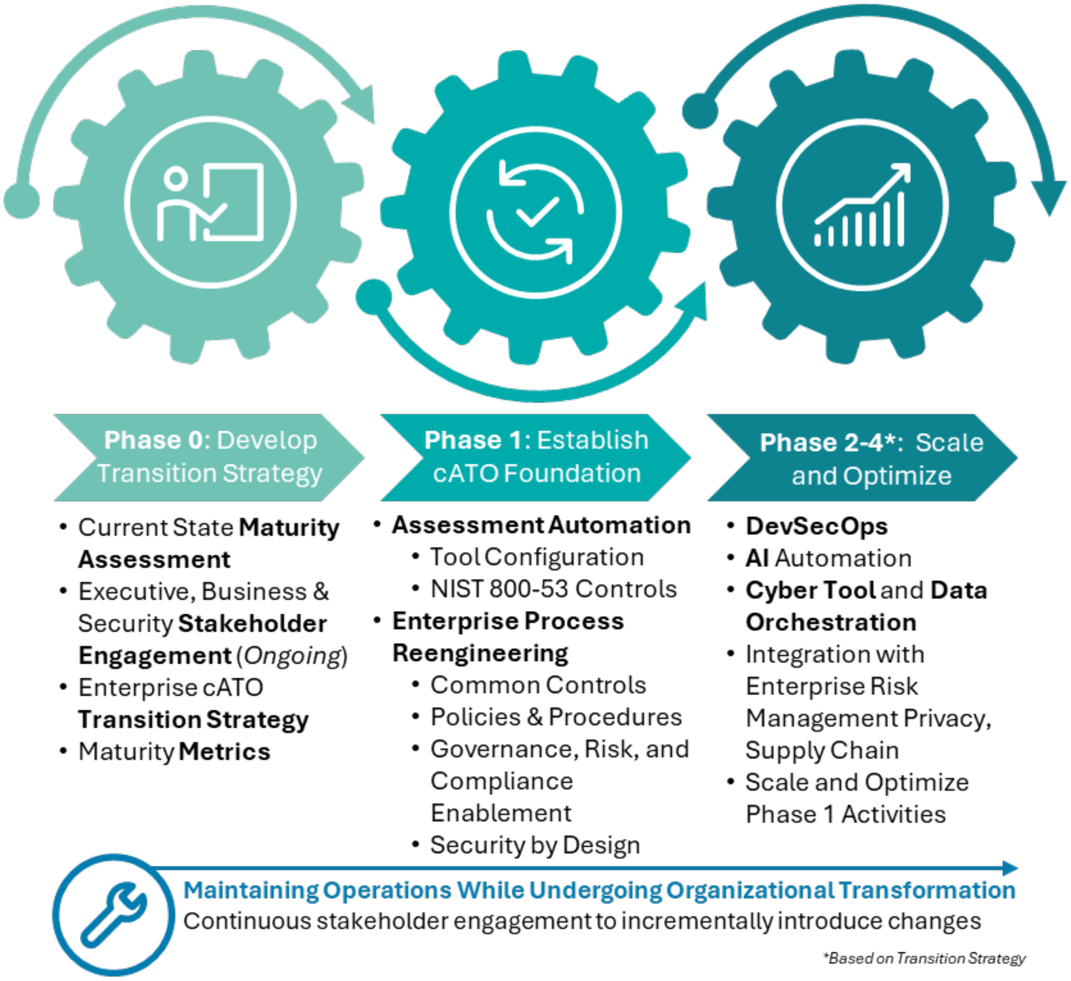
The Office of Management and Budget (OMB) Circular A-130 provides a foundational definition of risk for federal agencies: "a measure of the extent to which an entity is threatened by a potential circumstance or event." This measure typically depends on two factors: (i) the adverse impact or magnitude of harm that would arise if the circumstance or event occurs, and (ii) the likelihood of the event occurring. In other words, the federal government calculates risk as the product of impact and likelihood.

However, while A-130 offers a comprehensive definition, many agencies have operationalized risk management primarily through a compliance lens. This has led to a focus on point-in-time, "check-the-box" activities such as measuring risk by the number of Common Vulnerabilities and Exposures (CVEs) and the time taken to remediate them based on severity scores (Critical, High, Medium, Low). This approach often prioritizes time-to-remediation or third-party metrics (e.g., Common Vulnerability Scoring System or CVSS) rather than a broad assessment of risk grounded in both impact and likelihood. As a result, organizations may prioritize closing vulnerabilities quickly or incorrectly prioritizing lower risk vulnerabilities over critical ones instead of understanding which ones pose the greatest actual risk in the context of the environment in which they operate.

Adopting a cATO approach requires reframing risk management to align with the original intent of A-130: managing and minimizing risk on a continual basis, with decisions driven by real-time understanding of both impact and likelihood, not just compliance timelines. This reframing is imperative as regulatory requirements and emerging technologies drive new risk management decisions. For example, many organizations are hesitant to adopt Generative AI capabilities because of perceived uncertainty on how to secure and manage risk for those technologies. The proliferation of controls that need consideration, especially when risk delays the release of an official framework, further complicates adoption. cATO provides an avenue to address these challenges by aligning risk management strategies with operational goals, so that security measures are both effective and efficient.

Adopting a New Culture of cATO

As agencies move toward cATO, it is the people and processes utilizing these solutions that ultimately determine success. Part of this cultural shift is redefining risk, which enables people to look beyond compliance and whether a control is met or not at a point in time, as is the current state, without an understanding of the context behind that control. In a cATO approach, people and processes are instead focused more on leveraging data to continuously assess, understand, and maintain appropriate risk levels. This requires agencies to foster continuous learning and innovation for their people to understand risk, while building the necessary processes to support cATO. To help address these culture shifts, Deloitte developed a structured approach for transitioning to and maturing a cATO program.



Phase 0: Develop Transition Strategy

- Current State **Maturity Assessment**
- Executive, Business & Security **Stakeholder Engagement** (*Ongoing*)
- Enterprise cATO **Transition Strategy**
- Maturity **Metrics**

Phase 1: Establish cATO Foundation

- **Assessment Automation**
  - Tool Configuration
  - NIST 800-53 Controls
- **Enterprise Process Reengineering**
  - Common Controls
  - Policies & Procedures
  - Governance, Risk, and Compliance Enablement
  - Security by Design

Phase 2-4*: Scale and Optimize

- **DevSecOps**
- **AI** Automation
- **Cyber Tool** and **Data Orchestration**
- Integration with Enterprise Risk Management Privacy, Supply Chain
- Scale and Optimize Phase 1 Activities

Maintaining Operations While Undergoing Organizational Transformation
Continuous stakeholder engagement to incrementally introduce changes

**Based on Transition Strategy*

Figure 1. Deloitte's transitional approach to cATO implementation

Phase 0

Our cATO transition approach starts with Phase 0, which focuses on developing a transition strategy. Key activities in this phase include securing executive stakeholder commitment of necessary resources (such as funding, personnel, and time) to support the strategy, conducting a current state assessment, and identifying maturity metrics. The key outcomes of Phase 0 include:

- An approval from senior leadership based on these outcomes
- A cATO maturity assessment
- A documented transition strategy to cATO to include a cATO playbook that defines target metrics with effectiveness measures and clearly lays out a "definition of done" for transition

Senior leadership approval and support is critical as they facilitate involvement across the organization. Their influence promotes stakeholder alignment on the desired outcomes of the cATO program, making it easier to adopt new cATO processes, drive positive outcomes, and move away from outdated thinking. We help agencies accomplish this goal by presenting the maturity assessment and transition strategy to build confidence and commitment from senior leadership.

The cATO maturity assessment helps an organization understand the people, processes, and technologies that exist today in comparison to the desired outcome of a cATO. It also outlines how an organization can resolve any gaps including refining processes and training people. This would include processes for determining risk thresholds, automating assessment of risk, and DevSecOps—among others—as well as trainings that help illuminate the differences between traditional and continuous ATOs and provide clarity on the new processes. The maturity assessment serves as a guide for a transition strategy that establishes a timeline for initial transition and mature the cATO program.

The transition strategy is an awareness campaign that educates stakeholders on cATO and their role in the process. This clarification helps everyone understand their roles and how they impact others in the cATO process. Additionally, part of the transition strategy includes creating a cATO playbook containing information on specific roles and technologies involved, implementation steps, and required processes to be followed. To accelerate this process, Deloitte has built customizable transition strategies and playbooks including sample target metrics and key performance indicators (KPIs). By providing clear guidance and fostering a shared understanding, the transition strategy and cATO playbook enables agency personnel to make more effective and better-informed risk decisions through continuous evaluation.

Phase 1

In Phase 1, Deloitte collaborates with organizations to help them reengineer their enterprise processes to lay the groundwork for cATO. This involves helping establish foundational elements such as risk tolerance, standards, acceptance criteria, process documentation, and stakeholder training. Where the cATO playbook serves as a guide or reference—identifying the critical components and leading practices needed for cATO adoption—process reengineering is the actual work of designing, writing, and implementing the specific steps, workflows, and organizational changes that bring those playbook items to life within the unique context of each organization. In other words, the playbook outlines "what" needs to be done, while process reengineering is "how" those items are operationalized and embedded in daily practice. Using our experience driving cATO for our clients, Deloitte helps clients accelerate process engineering using roadmaps that define epics, user stories, and suggested sprints.

By the end of Phase 1, the organization has not only identified what is required for cATO (as described in the playbook) but has also established and approved the tailored roles, processes, and technologies necessary to perform automated and continuous risk assessments. The order of that list is important; too often, organizations focus on tools and technology, the landscape of which can shift rapidly and dramatically as evidenced by the impacts of Generative and agentic AI, but not on the desired outputs the technology should provide. Instead, we collaborate with clients to drive transformation through people and process changes that achieve desired outputs, not just technology, enabling ongoing risk management to become an integrated, repeatable part of the organization’s operations.

Phases 2 - 4

Phase 1 establishes the basis for cATO, while Phases 2 to 4 focus on implementing and scaling cATO across the organization. Phase 2 includes performing a pilot on a subset of resources, controls—or both—before moving to regular, full-scale operations in Phase 3. The pilot phase is important in that it gives an organization the opportunity to refine and adjust its processes before expanding to the rest of the organization. This is particularly significant given that cATO is foundationally reliant on DevSecOps, which integrates security into every stage of the development and operations lifecycle. This integration is essential for applying controls during build and then continuously monitoring those controls to contextualize them into an ongoing risk evaluation. Organizations unfamiliar with DevSecOps may require a longer transition time to fully adopt these practices. Phase 2 also helps identify potential training gaps and awareness campaigns needed for the broader implementation's success, while also providing some data on the effectiveness and success metrics established in previous phases.

After the pilot's adjustments, Phase 3 moves the organization to full-scale operations, where cATO processes are implemented across all applicable resources and controls. During this phase, stakeholders oversee consistent application of cATO practices, address any remaining challenges identified during the pilot, and begin collecting operational data. This data, which includes the KPIs and target metrics established in phase 0, inform ongoing process improvements and supports innovation efforts that will be further developed in Phase 4. The duration of Phase 3 can vary depending on organizational size, complexity, and readiness, but typically involves a period of sustained monitoring and refinement to facilitate successful adoption of cATO practices

Phase 4 incorporates innovations to make the cATO process more efficient by evaluating the collected KPIs and metrics to determine the success of the cATO implementation and identifying areas of improvement and efficiency. Some examples of potential KPI categories include:

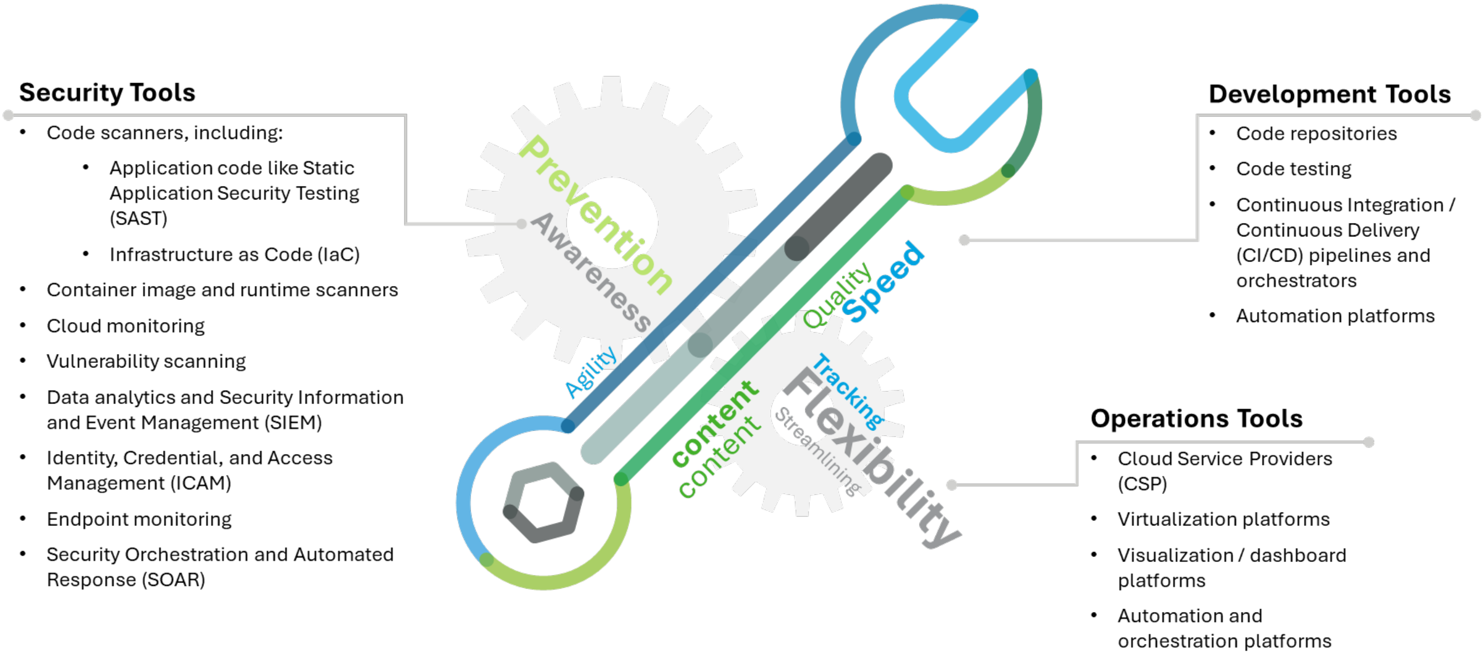
- **Risk Impact Metrics:** This includes the defined risk tolerance levels, potential impact of changes to those levels, time to address negative risk impacts, and what areas of the cATO lifecycle are introducing the most risks
- **Efficiency and Effectiveness Metrics:** These metrics determine how well people, processes, and technologies are working together to produce an accurate, ongoing risk assessment
- **Personnel Metrics:** This measures the effectiveness of cATO training and the effectiveness with which that training is applied

At the heart of cATO, people drive the organization's cultural change. Using our phased approach, Deloitte provides a way of supporting and informing an organization's people for successful adoption and implementation, while also enabling them to increase efficiency and optimization and be forward-leaning with innovation.

Technology-enabled cATO

In addition to the support of an organization's people, Deloitte guides clients on appropriate use of new and existing technologies for cATO implementation and maintenance. In some cases, organizations can leverage their existing tools while integrating new tools to address gaps between their previous static authorization practices and the new processes aligned with cATO. This balanced approach helps limit disruption, control costs, and enable a smoother transition to cATO processes.

The transition to cATO provides an opportunity to evaluate existing tools for future use in the cATO implementation. This evaluation is important because it helps align technology investments with the organization's established cATO metrics and outcomes and identifies any gaps that could impact success. This evaluation should not focus solely on traditional security tools as that view does not broadly consider the organization, but should also include technologies like the DevSecOps platforms, cloud and virtualized infrastructure, and IT service management platforms, among others. This allows organizations to gain a broad view of their enterprise and enables a better integrated cATO implementation, which should result in improved efficiency, scalability, and alignment with organizational goals. Tools like those below can be leveraged to broaden the scope beyond security



Security Tools

- Code scanners, including:
  - Application code like Static Application Security Testing (SAST)
  - Infrastructure as Code (IaC)
- Container image and runtime scanners
- Cloud monitoring
- Vulnerability scanning
- Data analytics and Security Information and Event Management (SIEM)
- Identity, Credential, and Access Management (ICAM)
- Endpoint monitoring
- Security Orchestration and Automated Response (SOAR)

Development Tools

- Code repositories
- Code testing
- Continuous Integration / Continuous Delivery (CI/CD) pipelines and orchestrators
- Automation platforms

Operations Tools

- Cloud Service Providers (CSP)
- Virtualization platforms
- Visualization / dashboard platforms
- Automation and orchestration platforms

Figure 2: Potential tools for cATO beyond security organized into categories.

Our approach does not focus on wholesale changes to security tools for the sake of change but to leverage—to the extent possible—the tools organizations are already using, then identify and address the gaps. Deloitte focuses on the tools within three primary areas:

- **DevSecOps Platform / Secure Software Supply Chain (SSSC)** – This area enables an everything-as-code (XaC) approach to build applications securely by design including application code, systems (such as virtual machines and containers), and infrastructure. Automated security testing is built in, including validating code libraries for security while using its testing data to automate controls assessments.
- **Continuous Monitoring (CONMON)** – This area aims to identify and proactively reduce risks before an adversary discovers them. Organizations can bolster this area by utilizing a centralized data lake where they can contextualize risk against threat intelligence and operational data, reducing the existing production attack surface profile.
- **Active Cyber Defense (ACD)** – This area covers the Security Operations Center (SOC) and identifying ongoing attacks, automated discovery of potential affected systems, and root cause. It is comprised of reactive security measures to reduce alert and event fatigue while focusing on security incidents by priority.

Especially when there is a myriad of disparate tools, it can be hard to understand how to gain the appropriate insights to support continuous risk assessment. However, one tool that is designed to help ease that pain point is a Cloud Native Application Protection Platform (CNAPP), which provides a suite of security solutions in a unified platform. CNAPPs typically feature Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP), and Cloud Infrastructure and Entitlement Management (CIEM) in one solution. In addition to these core features, CNAPPs increasingly include even more capabilities to bolster an organization's ability to manage risk including AI security, data secure posture management, and code-to-cloud tracing of vulnerabilities, among others. These capabilities are provided through a single platform, reducing the need to flip between multiple systems to understand what is happening from a risk perspective. It is unsurprising, then, that the DoD DevSecOps cATO Evaluation Criteria identifies CNAPP as a primary mechanism for evaluating a cATO for cloud environment(s).

Deloitte has an alliance with Wiz, an industry leading CNAPP provider, to help organizations move toward cATO. Wiz's unified platform supports all three core competencies of the cATO model through an integrated policy engine. The Wiz CNAPP provides:

- SSSC: Greater code security with automated software and AI Bill of Materials (SBOM and AI-BOM) and developer environment guardrails with integration directly into CI/CD pipelines and code repositories to build security into the development process, minimizing vulnerabilities from reaching production
- CONMON: Proactive threat reduction through automated risk assessment for cloud environments to quickly and accurately discover and prioritize toxic combinations of risk indicators for remediation activities, reducing time to detect and remediate vulnerabilities
- ACD: High-fidelity threat analysis, detection, and lateral impact visualization with reporting and linking to DevSecOps for remediation to reduce impact and blast radius of security incidents while accelerating fixes in code, systems, and infrastructure

Secure Software Supply Chain: Wiz Code

Deloitte leverages Wiz Code to help secure the software supply chain at the code level through two primary means: inventory analysis and DevSecOps deployment guardrails. Deloitte assists organizations during implementation of Wiz, guiding the setup and configuration so that telemetry information from deployed Virtual Machines (VMs), Kubernetes, and Docker containers, serverless applications, cloud storage containers, and other cloud objects is collected efficiently. From there, we leverage Wiz to present this data on demand to help build an SBOM. Additionally, we use this same visibility to assess the deployed AI services, technologies, and Software Development Kits (SDKs) creating an on-demand AI-BOM.

Within development workflows, we use Wiz Code to identify insecure dependencies, secrets, misconfigurations, and known vulnerabilities early in the development lifecycle, with checks built into Integrated Development Environments (IDEs), pull requests, Command-line Interface (CLI) workflows, and CI/CD pipelines. By scanning the organization's code against the same cloud, host, vulnerability, and other security rules and within the same platform, we can inject security directly into the development lifecycle, reducing time to deployment, and scaling modernized security for the cloud. This methodology is designed to reduce the security silos between the Application Security and Security Operations teams and developers.

To accelerate remediation of risks identified within their cloud environments, Deloitte uses Wiz's graph database enriched with an inventory of code repositories and developer identities. The inclusion of these data sources into the Wiz Security Graph—a core Wiz feature that goes beyond a simple database by mapping relationships between cloud resources, identities, configurations, code repositories, and vulnerabilities—correlates findings in code (e.g., CVEs. Known Exploited Vulnerabilities (KEVs), secrets, and IaC) with misconfigurations in version control and CI/CD, to provide a unified and detailed risk assessment. By connecting code-level findings to production risks in the Security Graph, Wiz enables faster remediation and stronger collaboration between Application Security; DevOps; and Governance Risk and Compliance teams.

This ability to incorporate cloud security directly within the software development lifecycle (SDLC) is known as "shifting security left". Deloitte guides organizations to be able to adopt shift-left practices, democratizing security so that every person across the organization becomes a stakeholder in the cybersecurity program. By empowering multiple groups to manage risk within their area of responsibility, Deloitte and Wiz together help clients embed security into daily operations and align with cATO objectives. This democratization also sets the foundation for a secure software supply chain that is not strictly isolated within DevOps but contains the necessary context for developers to understand how their code impacts the broader security posture of the production cloud environment. Using the Wiz Security Graph along with Deloitte's implementation supports the cATO objective of continuous, integrated assurance and helps reduce security delays by resolving risks proactively at their source.

Continuous Monitoring: Wiz Cloud

Deloitte uses Wiz Cloud to provide agentless, cloud-native visibility through direct application programming interface (API) integrations across multi-cloud environments. These integrations scan every cloud asset—including VMs, containers, serverless functions, managed services, and storage—and map them into a real-time security graph to connect findings across multi-cloud environments, correlating risk indicators such as vulnerabilities, misconfigurations, network exposure, secrets, malware, and policy deviations (e.g., Security Technical Implementation Guide or STIG noncompliance). The result is a contextual view of exposure and impact to facilitate automated, continuous risk assessments that align with the principles of NIST SP 800-37r2.

> "Assessment of security risk includes identification of threat sources and threat events affecting assets, whether and how the assets are vulnerable to the threats, the likelihood that an asset vulnerability will be exploited by a threat, and the impact (or consequence) of loss of the assets. As a key part of the risk assessment, assets are prioritized based on the adverse impact or consequence of asset loss" -NIST SP 800-37r2, p. 41[ii]

By providing insight across multiple cloud environments in real time, Deloitte's cATO approach—powered by Wiz's technology—assists organizations to operationalize the NIST risk management framework. This integrated approach allows for continuous identification, assessment, and prioritization of threats and vulnerabilities, enabling risk management to be proactive, broad, and aligned with NIST guidance. As a result, organizations can prioritize remediation based on organizational impact to achieve a unified, organization-wide view of risk that supports continuous authorization objectives.

Active Cyber Defense: Wiz Defend

Wiz Defend allows Deloitte to deliver active cyber defense capabilities as part of the Wiz platform. Deloitte assists organizations to assess their current cloud security posture and strategically align Wiz Defend's capabilities with business objectives and compliance requirements. The underlying Wiz graph database allows for higher-fidelity analysis than traditional relational databases and simple scan approaches to cybersecurity. Graph databases provide a more flexible schema, allowing for greater detection of dynamic changes and data relationships.

Deloitte uses Wiz to extend this visibility to runtime environments using Extended Berkeley Packet Filter (eBPF)-based sensors deployed across Kubernetes clusters, Linux hosts, and serverless workloads. These lightweight sensors monitor process activity, system calls, file access, and network behavior to detect malicious behavior in real time. This deeper level telemetry is implemented and connected across workload runtime signals, cloud activity, and audit logs, enabling teams to uncover lateral movement and attacker techniques that might otherwise go undetected. This high level of connection allows for the connection of seemingly unrelated events, detecting more sophisticated Advanced Persistent Threat (APT) attacks and malicious events.

Deloitte also helps organizations utilize Wiz Defend by integrating its threat detection events with existing SIEMs, customer relationship management (CRM) systems, messaging platforms, and other enterprise applications. As an example, Deloitte configures automated rules so alerts are routed to the right teams and provides ongoing tuning to reduce false positives and accelerate response times. Deloitte's use of Wiz Defend provides organizations with the agility to protect against threats, especially as those threats become more rapid and sophisticated.

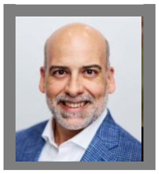
So Now What?

cATO offers a variety of benefits to an organization, but chief among those are speed of delivery and true risk management. Implementing and maturing cATO is a journey, and Deloitte can help you take the first steps:

- **Contact us**--Deloitte can help you perform a cATO maturity assessment, understand how to build a strategy to move to cATO, and implement new technologies like Wiz or adapt existing investments that can support true, ongoing risk assessment.
- **Schedule a demo**--Deloitte can provide a demo of Wiz in action so your organization can visualize the value and impact it can have along with a tailored cATO implementation.

Meet The Team

Dean Lee
Specialist Leader
Deloitte & Touche LLP
deanlee@deloitte.com



Mason Evans
Managing Director
Deloitte & Touche LLP
masevans@deloitte.com

[i] Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016).
[ii] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.