Aq Aquia

cATO+ and Federal Compliance Modernization

Accelerating Continuous Authority to Operate Through Compliance Documentation Automation

White paper

SEPTEMBER 2025

Authors:
Lloyd Evans, vice president of GRC, Aquia
AJ Yawn, director of GRC engineering, Aquia
Chris Hughes, co-founder and chief executive officer, Aquia

www.aquia.us | federal@aquia.us

Table of Contents

Executive Summary

The traditional authority to operate (ATO) process in both federal civilian (FedCiV) agencies and Department of Defense (DoD) environments presents significant challenges in software delivery, with authorization timelines typically ranging from 6-18 months. While continuous authority to operate (cATO) significantly streamlines those timelines, many implementations still struggle with the heavy documentation burdens. This white paper examines an enhanced approach — cATO+ — which builds upon standard cATO practices by adding crucial automation for compliance documentation and assessment.

This methodology has been successfully implemented across multiple government agencies, enabling them to redirect resources from compliance documentation to active risk reduction and mission-focused activities.

The documented results from agencies including the DoD, U.S. Patent and Trademark Office (USPTO), and Centers for Medicare and Medicaid Services (CMS) include: up to 74% reduction in compliance overhead, 30% decrease in authorization time, and 50% shorter onboarding times while maintaining strong security outcomes.

For government decision makers evaluating modernization investments, cATO+ offers a proven path to accelerate secure system deployment while reducing costs and improving security posture. This approach aligns with federal modernization initiatives, including:

- FedRAMP 20x, which aims to automate 80% of compliance requirements and reduce authorization timelines from years to weeks through machine-readable validation and industry-led automation.
- The DoD's Software Fast Track (SWFT) initiative, which aims to accelerate compliance timelines through automation, artificial intelligence (AI), and cloud-native services.

The methodology also supports broader agency transformation goals by enabling technical teams to focus on mission delivery rather than manual compliance tasks, ultimately improving both security outcomes and operational effectiveness.

The Challenge: Documentation Remains the Bottleneck in cATO

Across the DoD and FedCiv, there is a need to move at the speed of mission while ensuring systems comply with National Institute of Standards and Technology (NIST) and Federal Information Security Modernization Act (FISMA) requirements. While standard cATO implementations have improved upon traditional ATO processes, they often fall short in addressing the significant documentation burden that creates impediments to modern system development:

- Manual compliance documentation: Even in cATO environments, system security plans (SSPs), implementation statements, and assessment reports frequently require substantial manual effort.
- Documentation inheritance limitations: This introduces difficulties in efficiently reusing control implementations across systems.
- Compliance artifact generation: The manual creation of Open Security Controls Assessment Language (OSCAL)-based documentation can be time-intensive.
- Assessment documentation overhead: The associated documentation verification and validation processes can be labor-intensive.

These challenges persist even in organizations that have adopted basic cATO processes. A traditional security assessment still requires approximately 560 hours of manual effort from a team of four assessors, costing roughly $33,600 per assessment and creating operational bottlenecks that delay mission capabilities.

It isn’t that the need to document compliance adherence is inherently bad, but the way in which we do it as an industry hasn’t evolved in decades, despite advancements such as cloud, APIs, automation, and AI.

Operational Consolidation

The cATO+ methodology addresses current cATO challenges by adding crucial documentation automation components that integrate with existing tools to work alongside standard cATO components, such as infrastructure and continuous integration/continuous delivery (CI/CD) pipeline inheritance, and continuous monitoring and assessment.

Automated document generation

Custom, vetted automations for OSCAL-based system security plan (SSP) generation reduce SSP creation from weeks to seconds.

Control statements as a service

Pre-vetted implementation statements accelerate compliance documentation, with over 70% of implementation statements ready to go.

Automated assessment workflows

Manual assessment processes are transformed into automated verification procedures using native cloud services and event-driven architectures.

Document inheritance frameworks

Compliance artifacts are systematically reused across systems and environments.

Leverage Infrastructure as Code (IaC)

Pre-vetted IaC templates become the ATO baseline standards documented in OSCAL.

Why Federal GRC Needs an Engineering Mindset

Traditional GRC approaches break down in dynamic environments where infrastructure changes by the minute and compliance violations can cost millions and potentially compromise national security missions.

The most successful agencies in this new landscape share a common characteristic: they've moved beyond viewing compliance as a paperwork exercise and started treating it as an engineering discipline.

Read more on the blog

Documentation Aspect	Traditional cATO	cATO+ Approach
System Security Plan	Mostly manual with templates	Automated generation with OSCAL integration
Control Implementation Statements	Manual creation	"Control statements as a service" with 70%+ ready to use
Assessment Documentation	Manual validation	Automated assessment with continuous verification
Inheritance Documentation	Limited documentation reuse	Structured inheritance frameworks
Privacy Impact Analysis (PIA)	Performed manually post-ATO	Automated inclusion in early-stage system documentation
Privacy Threshold Analysis (PTA)	Conducted manually with policy input	Triggered automatically as part of the initial documentation flow
Business Impact Assessment (BIA)	Inconsistent or post-facto classification	Systematically classifies systems based on risk and business impact upfront
Control Coverage Review	Manual review of controls against standards	Log and output review with alerting for gaps using AI
Alignment	Manual checks for control alignment during deployment	Templated IaC ensures continuous deployment within assessed control boundaries

Comparison With Alternative Approaches

When evaluating cATO implementations, it's important to distinguish between approaches that simply rebrand traditional processes and those that introduce meaningful automation. The cATO+ approach differs from conventional implementations in several key ways:

Complete documentation automation

While standard cATO often focuses primarily on continuous monitoring and testing, cATO+ addresses the critical documentation gap that persists in most implementations.

Early cATO efforts focused on people and process over documentation, revealing challenges in reciprocity and inheritance. The "plus" in cATO+ fills this gap with custom, vetted automations for documentation generation and validation.

OSCAL integration

cATO+ leverages OSCAL to standardize and automate security documentation, enabling machine-readable compliance artifacts that can be systematically validated and updated.

Control statements as a service

The pre-vetted implementation statements library significantly accelerates documentation processes by providing ready-to-use, validated control implementation descriptions.

Customized documentation workflows

The approach adapts to specific organizational requirements, including:

- DoD-specific interpretations of NIST 800-53 controls
- Integration with specialized documentation systems like E-MASS
- Support for cloud-native, hybrid, and self-hosted infrastructure documentation requirements

While standard cATO addresses monitoring and security testing, the persistent documentation burden remains a critical bottleneck. By adding robust documentation automation, organizations can finally achieve the full potential of continuous authorization.

cATO+ Documentation Automation Tech Stack

The documentation automation capabilities of cATO+ are enabled by several key technologies.

1

OSCAL Implementation

Custom tooling leverages NIST's OSCAL to create machine-readable security documentation.

2

Automated Document Generation Pipeline

Integration with CI/CD workflows generates documentation artifacts based on actual system configurations.

3

Control Implementation Library

A database of pre-vetted control implementation statements is mapped to common cloud services and security tools.

4

Document-as-Code Principles

Software development practices are applied to compliance documentation, including version control, peer review, and automated testing.

5

Assessment Evidence Collection Framework

The gathering of evidence from security tools and mapping to control requirements is automated.

6

Document Inheritance Engine

The systematic reuse of control implementations across systems with appropriate context adaptation is leveraged.

These technologies work together to create a comprehensive documentation automation framework that addresses the full spectrum of compliance documentation needs throughout the system lifecycle.

Alignment With Federal Modernization and Industry Standards

The cATO+ approach supports the federal government's broader modernization initiatives, including DoD SWFT (software factory) and federal/DoD cATO/ongoing authorization (OA) programs. It also aligns with automation initiatives like FedRAMP 20x. These initiatives represent a fundamental shift toward automated, machine-readable compliance validation across all federal agencies and their partners.

The cATO+ methodology provides the technical foundation necessary to achieve federal modernization objectives through machine-readable documentation, industry framework integration, and continuous validation architecture.

Machine-Readable Documentation

- Custom OSCAL-based documentation generation produces machine-readable security artifacts
- Automated key security indicator (KSI) validation aligned with federal automation requirements and machine-readable validation expectations
- Automated generation of assessment packages that third parties can continuously validate

Key Technical Components

The cATO+ methodology is built upon the established principles of continuous monitoring, automated compliance verification, and real-time risk assessment that have been validated by NIST, the DoD, numerous FedCiv agencies, and industry research.

The approach is grounded in the scientifically proven concept that security control effectiveness can be quantitatively measured through continuous data collection and analysis, rather than point-in-time assessments.

This foundation is reinforced by formal security measurement frameworks, including NIST SP 800-55 and the DoD's Cybersecurity Maturity Model, which confirm that ongoing, automated control validation produces more accurate security posture assessments than traditional methods.

Industry Framework Integration

- Pre-built integrations with existing commercial security frameworks (e.g., System and Organization Controls 2 (SOC 2), ISO 27001, NIST Cybersecurity Framework)
- Automated mapping between commercial certifications and federal requirements
- Reduction of duplicate compliance efforts across multiple frameworks
- Leveraging existing organizational investments in security tooling and processes
- Automated evidence generation supporting federal automation goals

Continuous Validation Architecture

This approach is grounded in the scientifically proven concept that security control effectiveness can be quantitatively measured through continuous data collection and analysis, rather than point-in-time assessments.

It is reinforced by formal security measurement frameworks, including NIST SP 800-55 and the DoD's Cybersecurity Maturity Model, supporting federal goals of validating security through real-time data rather than periodic audits, in alignment with FedRAMP 20x.

Cloud-Native Security Integration

cATO+ reduces risk by increasing visibility through integrated security tool data within CI/CD pipelines and by monitoring cloud-native services that are already widely used across federal agencies and their industry partners:

- Integrated security tool data: Security telemetry connected within CI/CD pipelines
- Cloud-native security services monitoring: Utilizes services already deployed across federal agencies (e.g., AWS GuardDuty, CloudTrail, Config, SecurityHub, Azure Sentinel, etc.)
- Custom security workflows: Automated security checks providing real-time security impact analysis
- DevSecOps integration: Streamlined integration of static and dynamic code analysis, dependency checking, software bill of materials (SBOM) management, and container scanning

This foundation reduces the time to initial authorization from 6-18 months to just 6 weeks, while assessment periods are shortened from 1-3 month cycles to continuous, near-real-time feedback loops.

FedRAMP 20x Implementation

Where FedRAMP 20x establishes policy frameworks for cloud authorization automation, cATO+ provides a proven implementation methodology:

- Machine-readable assessment packages that FedRAMP 20x phase one requires
- Continuous reporting capabilities moving beyond point-in-time assessments
- Third-party assessment organization (3PAO) integration workflows aligned with FedRAMP 20x assessment expectations

Industry-Led Innovation Framework

Federal modernization initiatives place decision-making power into industry and agencies' hands, moving away from prescriptive security methods. The cATO+ approach embodies this philosophy by:

- Leveraging existing commercial investments: Building upon existing SOC 2, ISO 27001, and other commercial security frameworks that organizations have already implemented
- Providing flexible implementation patterns: Adapting to specific organizational requirements and existing toolchains
- Supporting direct agency-provider collaboration: Enabling streamlined collaboration between federal agencies and their industry partners

Addressing Government Efficiency Goals

The cATO+ approach aligns with broader federal efficiency objectives focused on automation and accelerated secure technology adoption.

✓

Cost reduction

Documented 74% reduction in compliance overhead while improving security outcomes

✓

Timeline acceleration

Authorization time reduction from 6-18 months to 6 weeks

✓

Resource optimization

Automating manual processes allows organizations to redirect resources from compliance documentation to mission-focused activities and active risk reduction

Preparing for Continuous Authorization

The cATO+ methodology provides a foundation that scales across all federal compliance requirements.

Organizations implementing cATO+ are positioned for participation in federal continuous authorization programs, with current readiness that demonstrates their commitment to advanced compliance practices. The comprehensive automation framework supports future scalability, enabling expansion across different impact levels and agency requirements as organizational needs evolve.

Early adoption of cATO+ creates a competitive advantage, as federal agencies increasingly expect automated, continuous compliance capabilities from their industry partners.

Additionally, organizations that embrace this methodology early are well-positioned for emerging federal automation programs, preparing them for expanded requirements as these programs mature across different impact levels.

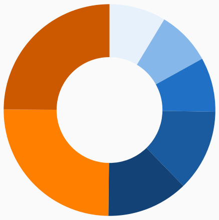
Implementation at Scale

By integrating with existing infrastructure already in place, cATO+ helps get mission-critical applications to the end user 70% faster.

Results and Performance Metrics

Assessment periods

Traditional ATO



1-3 month cycles

Aquia cATO+

Continuous, near-real-time

SSP Generation

From weeks to seconds

70% of implementation statements ready to go

Initial authorization

Traditional ATO

6-18 months

Aquia cATO+

6 weeks

Scaling Benefits

As cATO+ expands, federal agencies can anticipate the following benefits:

- Automation and inheritance for up to 70% of security controls
- Automation of 55% of control assessments
- Further reduction in time to authorization from months to weeks
- Enhanced continuous deployment capabilities dramatically improving mission responsiveness while maintaining superior security standards

Operational Impact

Current State

- ISSOs, developers, business owners, assessors, and authorization officials spend months navigating traditional ATO processes
- Significant deployment delays reduce operational effectiveness
- Manual assessment work creates bottlenecks and diverts technical resources from mission-focused activities

Future State, With cATO+ Implemented

- Teams focus on active risk reduction through robust vulnerability management, infrastructure security, and configuration management
- Developers deploy secure code to production in days rather than months
- Automated security checks integrate into workflows, providing immediate feedback on compliance issues
- Authorization officials make decisions based on continuous data rather than point-in-time snapshots
- Information System Security Officers (ISSOs), Information Systems Security Managers (ISSMs), and assessors are enabled to determine data-driven risks for systems through automated workflows supporting compliance, governance, and assessment

Conclusion

The cATO+ approach addresses the critical documentation challenges that persist in standard continuous ATO implementations. By adding robust documentation automation, organizations can overcome the final major hurdle in streamlining authorization processes.

The data from implementations across multiple federal agencies demonstrates that properly implemented cATO+ processes can significantly reduce compliance documentation overhead while improving security outcomes. Where standard cATO implementations often deliver incremental improvements, the addition of documentation automation can transform authorization timelines from months to weeks.

The key insight from successful implementations is that documentation should be a byproduct of good development and security practices, not a separate, manual effort. By making documentation automation a first-class component of the authorization process — the defining characteristic of cATO+ — organizations can finally realize the full promise of continuous authorization: delivering secure mission capabilities at the speed required by today's operational environment.

The key insight from successful implementations is that documentation should be a byproduct of good development and security practices, not a separate, manual effort.

Service Disabled Veteran Owned Small Business
SDVOSB
CVE

About Aquia

Aquia is a digital services firm specializing in cloud infrastructure, cybersecurity, and compliance automation. Since 2021, we've generated millions in cost savings for the federal government through cloud services and licensing optimization, and reduced authorization timelines by 74% through modernized security processes.

Named the Department of Health and Human Services' "2024 Service-Disabled, Veteran-Owned Small Business (SDVOSB) of the Year," we are committed to helping government mission owners maximize outcomes and challenge the status quo. Learn more at aquia.us or contact us at federal@aquia.us.

AWARDABLE
PLATFORM ONE

Aquia's cATO+ solution is awardable on the DoD's Platform One Marketplace, making it ready to be acquired quickly by DoD customers through flexible pathways. Learn more.

Trusted By

U.S. Department of Veterans Affairs
CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
uspto
U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF INSPECTOR GENERAL
CLOUD ONE FAST SECURE STREAMLINED
PLATFORM ONE DEPARTMENT OF DEFENSE
CDC
U.S. SECURITIES AND EXCHANGE COMMISSION MCMXXXIV
USDA
MARYLAND
U.S. AIR FORCE
U.S. DIGITAL SERVICE
Nava
leidos
OMNI FEDERAL
Skyward IT SOLUTIONS
noblis
coforma
KESSELRUN
DATALOCK CONSULTING GROUP
nuix
RegScale
Excella
BIGBEAR.AI
cantaloupe
VALLEY IT SOLUTIONS

AWARDABLE PLATFORM ONE
2025 ELEV8 GovCon HONOREE
Great Place To Work. Certified MAR 2024-MAR 2025 USA
builtin 2025 BEST PLACES TO WORK
Inc. Best Workplaces Honoree 2024
FORTUNE BEST SMALL WORKPLACES 2024
Google Cloud Partner
aws PARTNER Advanced Tier Services

- Public Sector
- Authority to Operate
- Security Services Competency