ATARC

cATO Working Group

Continuous Authorization to Operate (cATO) Implementation Playbook

Acknowledgements

ATARC would like to take this opportunity to recognize the following cATO Working Group members for their contributions:

Darren Death, EXIM, ATARC cATO Working Group Government Chair

Brian Hajost, SteelCloud, ATARC cATO Working Group Industry Chair

Trevor Bryant, CISA

Annette Mitchell, IRS

Oluyemisi (Yemmy) Omiteru, ICE/DHS

Hasan Yasar, Carnegie Mellon

Douglas L. Johnson Jr., ATARC cATO Working Group Member

Melissa Livesey, TVA

Dave Raley, USMC

Dave Rideout, US Army

Tom Volpe Jr., C2 Labs

Chetin Durak, Caveonix

Anton Hoffman, Caveonix

Jack Nelson, Caveonix

Chris Harr, Wiz

Bryan Rosensteel, Wiz

Claire Hackney-Carr, ATARC cATO Working Group Member

Introduction

In today's rapidly evolving cyber environment, obtaining an initial Authorization to Operate (ATO) under the Risk Management Framework (RMF) can take anywhere from 6 to 36 months. This lengthy process lends itself to hidden program costs for achieving and maintaining an ATO, leading to higher operating costs, sometimes in excess of $1.5 million per system. Given the complexity of information systems and the increasing need for rapid business service delivery, enhancements to ATO processes and the implementation of Continuous Authorization to Operate (cATO) are critically important to meet mission requirements. The overarching strategic objective of cATO is to make government cyber activities more efficient for all.

Current Situational Context

Security Product Teams must navigate major toil to gather key artifacts such as the System Security and Privacy Plan, Information Security Risk Assessment (ISRA), Contingency Plan (CP), Architecture Diagrams, and Vulnerability Scan reports. To collect data necessary for completion of these reports, static, point-in-time scans are leveraged. To keep these static reports as an accurate relection of these system undergoing the ATO process, it is often necessary to freeze all system updates, patching, and innovation, unless a critical security vulnerability arises. For many of these systems, the time required for ATO completion renders the authorized system as outdated once finally authorized. These processes can be streamlined using cATO to derive an overall system authorization, greatly reducing ATO timelines, while allowing for more agility in system design and speeding up innovative development for mission systems. Decision-makers in a Cyber security context must adjust traditional approaches for assessing systems, accounting for limited resources, and accelerating authorizations by leveraging Artificial Intelligence.

Desired Outcome

A modernized cATO product team integrates cyber artifacts automatically into all systems development and release activities, prioritizing automated cyber security gates over manual processes. Implementing a robust cATO system is not a one-size-fits-all approach for all organizations, but by following a crawl, walk, run approach, the objective of efficiently improving a time-consuming Risk Management Framework is achievable.

What is cATO?

The term cATO is used interchangeably with the term ongoing authorization (OA) which is part of the National Institute of Standards and Technology (NIST) RMF. NIST Special Publication 800-37 Revision 2 defines ongoing authorization as follows:

> *The process of maintaining authorization of an information system or organization's security posture through the continuous monitoring of security controls and risk-related information to determine if risks remain acceptable over time.*

The following are some additional characteristics of ongoing authorization/cATO:

- **Time-driven** and may also be **event driven**
- **Dependent on a robust Information Security Continuous Monitoring (ISCM) program** to provide near real-time system security-related information
- Considers/includes not only technology but **also people, processes, etc**.

Initial Conditions for cATO

Organizational Authorizing Officials (AOs) that are considering adopting a cATO approach should ensure that the following conditions are met:

- The AO has granted an initial ATO in accordance with the Risk Management Framework (RMF), and the system has entered the operational phase
- A robust ISCM program is in place that monitors all implemented controls:
  - at the appropriate frequencies
  - with the appropriate degree of rigor
  - In accordance with the organization's ISCM strategy and NIST guidance
- The AO is still responsible and accountable for understanding and accepting risk
- Security-related information supporting cATO should be made available to the AO on demand (ideally as a dashboard or report).
- Security-related information from manual monitoring is used when automated monitoring is not possible.

If these conditions are met, a termination date for the ATO does not have to be specifically stated as long as the ISCM program continues to provide the necessary security related information. AOs should leverage the security-related information gathered during monitoring to support cATO as opposed to a static, point-in-time assessment.

ISCM Strategy

ISCM which is also known as Continuous Monitoring (ConMon) is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

Organizations are responsible for defining their overarching ISCM strategy in accordance with NIST Special Publication 800-137. The ISCM strategy defines the assessment methods and frequencies for all implemented controls. A robust ISCM program must be implemented to support the overarching ISCM strategy. This program will consist of manual and automated assessments.

ADDITIONAL ISCM CONSIDERATIONS

- **Automated Security Assessments:** Implementing automated tools for continuous security assessments can help identify vulnerabilities and compliance issues in real time. These automated tools should, to the extent applicable for the system under ISCM, contain insight into the continuous integration/continuous delivery (CI/CD) pipeline as well as runtime events. These assessments elevate monitoring beyond point-in-time vulnerability enumeration and compliance benchmark reporting.
- **Risk-Based Prioritization:** Prioritize applications and programs based on their risk profile, ensuring that high-risk systems receive immediate attention and remediation. This prioritization extends to risk remediation, where the emphasis is reducing the impact to the confidentiality, integrity, and availability (CIA) of the agency over a prioritization of reducing the overall number of vulnerabilities present.
- **Integration with DevSecOps:** Embed security assessments within the DevSecOps pipeline to ensure that security is considered throughout the software development lifecycle. This integration should be implemented in a bi-directional manner, where security assessments within DevSecOps prevent the introduction of risks from being introduced into the production environment, and the automated security assessments include necessary insight into the CI/CD pipeline, to ensure swift remediation of identified risks, and reducing the reintroduction of these risks by resolving back within the source image and code repository.

Prioritizing Security Controls for ISCM

Security controls are essential for protecting core functionalities and ensuring the system's immediate operational security. Effective prioritization of security controls supports the development of the Information Security Continuous Monitoring (ISCM) strategy, aids in determining assessment frequencies, and guides the selection of target controls for automation.

DIAGNOSTIC QUESTIONS

- What are the minimum controls which can trickle down across different control panes: applications, operating systems, databases, containers, and network to effectively grant an ATO?
- Are those controls housed in a Source Control System to ensure version control, automation, and consistent repeatability when applied to other systems seeking a new ATO?
- Do we we have the ability to scope by projects, for example should we collect results from a development environment?

Prioritizing security controls for ISCM begins with categorizing the information system to select an appropriate control baseline from NIST Special Publication 800-53r5. To avoid overcategorization, each system should tailor and scope the baseline using the scoping guidance provided in NIST SP 800-53r5. Once a tailored set of controls is established, organizations can then effectively prioritize security controls for continuous monitoring. Selecting the right security controls for continuous monitoring requires a risk-informed, threat-driven, and mission-aligned approach. Below are key practices to guide the process:

1. **Start with a Tailored Baseline**

    - Begin by selecting a baseline of controls from NIST SP 800-53r5 and/or other applicable frameworks (e.g., ISO 27001, CIS Controls).
    - Tailor the baseline using:
        - System categorization (per NIST SP 800-60r1)
        - Scoping guidance (from NIST SP 800-53r5)
        - Inheritance from common or shared controls

2. **Incorporate Threat Intelligence Using Frameworks Like MITRE ATT&CK**

    - Use **MITRE ATT&CK, D3FEND**, STIGs, CIS Benchmarks and other threat frameworks to map real-world attack techniques to relevant security controls.
    - Prioritize controls that directly mitigate tactics and techniques used by adversaries targeting your environment.
    - Align control selection with high-risk TTPs (tactics, techniques, and procedures) to ensure coverage against known and emerging threats.
    - Leverage the ISCM to reduce automate discovery of potential attack blast radius and accelerate identification of kill chain events.

3. **Prioritize Based on Risk and Mission Impact**

   - Use results from risk assessments (e.g., ISRA) to identify high-impact areas with greatest impact to CIA.
   - Focus on protecting mission-essential functions, sensitive data, and critical infrastructure.
   - Engage business and security stakeholders to ensure prioritization aligns with organizational risk tolerance and operational needs.

4. **Emphasize Controls That Support Automation**

   - Prioritize controls that can be monitored continuously through automated tools (e.g., SIEM, CNAPP, GRC & vulnerability scanners).
   - Automation enhances real-time visibility, reduces human error, and supports scalability.

5. **Focus on Volatile and Frequently Changing Controls**

   - Monitor controls related to dynamic system components, such as:
     - Configuration management
     - Access control
     - Patch and vulnerability management
   - These controls typically require more frequent validation and have a higher risk of drift.

6. **Align with the ISCM Strategy and Resources**

   - Ensure selected controls align with the broader ISCM strategy:
     - Defined monitoring frequencies
     - Roles and responsibilities
     - Reporting, analysis, and escalation procedures
   - Consider staffing, tooling, and budget constraints.

cATO Framework

A cATO framework enables an organization to migrate systems into a cATO program and adopt a cATO cadence. The following are some key components of a cATO framework:

1. **cATO Pre-Requisites**

    a. Define ISCM Strategy
    b. Define Common Control Catalogs
    c. Define cATO entrance criteria
    d. Define cATO Metrics, Thresholds, and Triggers
    e. Develop cATO Dashboards and Reports

2. **Onboarding Systems into cATO**

    a. Onboarding Kickoff Meeting
    b. Complete Onboarding Checklist
    c. Onboarding Assessment Report
    d. Onboarding Approval Meeting
    e. Admission Letter

3. **Maintaining a cATO**

    a. Monitoring the Security Posture of the System
    b. Managing Event & Time Driven Triggers
    c. Conduct Periodic Risk Reviews
    d. Respond to Issues of Non-Compliance and with cATO Conditions
    e. Risk Mitigation Actions

4. **Managing Risks from Control Inheritance**

ISCM Metrics

A successful cATO program begins with a well-defined ISCM strategy that integrates technology, processes, procedures, operating environments, and personnel. This strategy must establish meaningful metrics that provide real-time visibility into the security posture of an information system.

Effective assessment of key security controls is essential for maintaining a cATO cadence. By defining core metrics as part of the automation process, organizations can enhance situational awareness, streamline risk management, and ensure continuous compliance.

The following are key recommended metrics to support a successful cATO program:

- Establish baseline metrics including:
    - **Mean Time to Patch (MTTP):** This metric tracks the average time it takes to apply patches to known vulnerabilities. Shorter MTTP indicates a faster response to security threats, which is critical for maintaining a secure system posture.
    - **Mean Time to Detect (MTTD):** This metric measures the average time taken to detect a security incident. Lower MTTD values signify a more proactive and effective monitoring system.
    - **Mean Time to Recovery (MTTR):** This metric assesses the average time required to recover from a security incident. Lower MTTR values indicate a more efficient and resilient recovery process.
    - **Mean Time Between Failures (MTBF):** This metric calculates the average time between system failures. Higher MTBF values reflect a more reliable and stable system.
    - **Vulnerability Density:** Measures the number of vulnerabilities detected per unit of code (e.g., per 1,000 lines of lines of code). Helps identify areas of the codebase that are more prone to vulnerabilities and require focused attention.
    - **Patch Compliance Rate:** The percentage of systems that are up-to-date with patches. Ensures that systems remain protected against known vulnerabilities.
    - **False Positive Rate (FPR):** The percentage of security alerts that are incorrectly identified as threats. Helps improve the accuracy of security monitoring tools and reduces the time spent investigating false alarms.
    - **Security Debt:** The cumulative count of unresolved security issues over time. Provides insight into the backlog of security issues that need to be addressed.
    - **Incident Response Time:** The time taken from the detection of a security incident to the initiation of a response. Measures the efficiency of the incident response process and helps identify areas for improvement.
    - **Compliance Drift:** The degree to which systems deviate from compliance standards over time. Ensures continuous adherence to compliance requirements and helps identify areas where additional controls are needed.
    - **User Privilege Levels:** Tracks the distribution and number of user accounts with elevated privileges. Ensures that only necessary personnel have access to sensitive information and reduces the risk of insider threats.
    - **Security Training and Awareness:** Measures the effectiveness of security training programs based on assessments and user feedback. Ensures that employees are aware of security policies and best practices, reducing the risk of human error.

ISCM Thresholds

Establishing thresholds for ISCM metrics is critical for maintaining a cATO. These thresholds define acceptable security baselines, trigger automated responses when deviations occur, and ensure real-time risk visibility. Without well-defined thresholds, organizations risk operational disruptions, compliance failures, and security blind spots that could undermine cATO efforts.

The following table outlines recommended risk thresholds for each of the listed ISCM metrics. These thresholds can serve as a baseline for organizations operating under a cATO model. Thresholds can vary by environment and risk tolerance, so these should be tailored based on business needs and maturity. The following thresholds can be leveraged to trigger an automated response when exceeded enabling timely risk mitigation and maintaining continuous compliance:

Metric	Recommended Risk Threshold for Alerting	Rationale
Mean Time to Patch (MTTP)	>30 days (High Risk), >90 days (Moderate Risk), >180days (Low Risk)	Faster patching reduces exposure to known vulnerabilities; align with CVSS severity and SLA policies.
Mean Time to Detect (MTTD)	>72 hours	Shorter detection times improve incident containment and reduce potential damage.
Mean Time to Recovery (MTTR)	>8 hours (High Systems), >24 hours (Moderate Systems)	Efficient recovery helps maintain availability and trust during and after incidents.
Mean Time Between Failures (MTBF)	<365 days	Higher MTBF reflects improved system stability and reliability.
Vulnerability Density	> 1 per 1,000 LOC (High Systems), > 5 per 1,000 LOC (Moderate Systems)	Helps identify insecure code areas; higher density indicates greater likelihood of exploit.
Patch Compliance Rate	< 90% (High Risk), < 75% (Moderate Risk)	High compliance reduces systemic vulnerability to known threats.
False Positive Rate (FPR)	> 10% (High Systems), > 25% (Moderate Systems)	Excessive false positives can overwhelm teams and mask real threats.
Security Debt	> 100 open issues (High Risk), > 250 open issues (Moderate Risk)	Indicates backlog in remediation; growing debt weakens overall security posture.
Incident Response Time	> 1 hour (High Systems), > 4 hours (Moderate Systems)	Quick initiation of response reduces dwell time and impact.
Compliance Drift	> 5% deviation from standard (High Systems), > 10% deviation (Moderate Systems)	Continuous alignment with policies and controls is essential for maintaining ATO.
User Privilege Levels	> 5% of users with elevated access (High Systems), > 10% (Moderate Systems)	Least privilege principle helps minimize insider threat and misuse.
Security Training & Awareness	< 85% completion or assessment score (High Systems), < 70% (Moderate Systems)	Poor training results in increased human error and susceptibility to phishing or social engineering.

cATO Reporting

To maintain a Continuous Authorization to Operate (cATO, organizations must provide real-time dashboards and automated reports that offer clear, actionable insights into the security state of an information system integrating results from both automated and manual assessments. These tools help AOs assess risk, ensure compliance, and make informed decisions regarding the system's security posture.

The following table outlines key recommendations for a cATO dashboard, designed to support continuous authorization by providing real-time visibility into system security. Each component addresses a specific need and collectively ensures that AOs have the actionable insights required to assess risk, ensure compliance, and maintain trust in agile, dynamic environments.

Dashboard Component	Purpose	Key Elements
Executive Summary View	Provide a high-level overview of system health.	System authorization status, overall risk rating, compliance score, key trends, last update timestamp
Real-Time Security Posture Metrics	Highlight the current security state using automated tools.	Open vulnerabilities, patch status, tool coverage, asset inventory accuracy, configuration compliance
Identification of critical toxic combination of risk	Tracks issues based on combination of risk elements which pose the greatest threat to the agency's CIA for data and systems	Consistent with the RMF to prioritize public exposure, risk to critical data and systems, risk of lateral spread with privilege elevation, known exploitable vulnerabilities (KEVs), etc.
Control Compliance and Assessment Status	Track control implementation and assessment progress.	Control coverage by NIST family, assessment frequency, manual vs. automated coverage, inheritance use
Risk and Threat Intelligence Integration	Provide a threat-informed view of system risk.	Mapped MITRE ATT&CK techniques, threat feeds, correlated threats, business impact analysis
Audit and Authorization Artifacts	Ensure transparency and traceability for auditors.	Links to SSP, ISRA, CP, POA&M, ATO letter, recent assessments, evidence repositories, assessment history
System Activity and Change Monitoring	Monitor changes that may affect system security.	Code deployments, infrastructure changes, IAM changes, configuration drift
POA&M Tracking and Remediation Workflow	Keep track of known issues and remediation progress.	Open POA&M items, severity, due dates, owners, remediation status, risk acceptance
Customizable Views and Role-Based Access	Provide tailored dashboard experiences for various stakeholders.	Filters by system/unit, views for AOs/ISSOs/engineers, export options
System-of-Systems or Portfolio View	Enable cross-system oversight for leadership.	cATO health by system, aggregate risk summaries, shared control effectiveness
Integration with ISCM and DevSecOps Pipelines	Enable real-time data ingestion and automation.	APIs for data ingestion, pipeline hooks for violations, GRC platform integration

Shifting Left Security Practices: Leveraging Software Factories in cATO

Software factories provide a structured, automated, and scalable approach to software development, which can be directly leveraged to enhance ISCM in a cATO framework. By integrating security controls into the software factory pipeline, organizations can achieve real-time visibility, continuous risk assessment, and automated compliance reporting.

Automating and orchestrating security practices through people, technology, and processes is essential. Shifting left means integrating security earlier in the development process to identify and mitigate vulnerabilities before they reach production. This is achieved by the following:

- Establish software factories adhering to DevSecOps NIST SP 800-208a standards.
- Create Policy Enforcement Points (PEPs) in DevSecOps pipelines to immediately remedy any high priority or critical issues.
- Create an environment where software can be tested in a secured, compliant, and patched environment that matches the production environment.
- Produce compliance artifacts throughout all DevSecOps phases.
- Develop automation plans for implementing, monitoring, and reporting on compliance and vulnerabilities once the software is in production.
- Produce and/or ingest Software Bill of Materials (SBOMs) into the ATO process.
- Produce and/or ingest Artificial Intelligence Software Bill of Materials (AI-BOMs) into the ATO process.
- Develop a plan for monitoring and addressing SBOM and AI-BOM software vulnerabilities once discovered.

ADDITIONAL CONSIDERATIONS

- **Security-as-Code:** Implement security policies and controls as code to ensure they are consistently applied across all environments.
- **Continuous Compliance:** Automate compliance checks and reporting to ensure continuous adherence to regulatory and organizational standards.
- **Collaboration and Training:** Foster collaboration between development, security, and operations teams. Provide training to ensure all team members are aware of security best practices and their roles in maintaining security.
- **Proactive Threat Hunting:** Implement proactive threat hunting techniques to identify potential threats and vulnerabilities before they can be exploited.
- **Incident Response Automation:** Automate incident response processes to ensure a swift and coordinated response to security incidents.

By embedding ISCM capabilities into software factories, organizations can achieve continuous security assurance, reduce manual compliance burdens, and accelerate secure software delivery. This approach enables a proactive security posture that aligns with cATO objectives, ensuring systems remain resilient, compliant, and continuously monitored in real time.

The Role of Supply Chain Risk Management (SCRM) in cATO

SCRM plays a critical role in ISCM and cATO by ensuring that third-party vendors, suppliers, and software components do not introduce security risks that could compromise an organization's cyber resilience. As organizations move toward automated, real-time security monitoring, securing the supply chain is a fundamental requirement to maintain a trusted and continuously authorized operating environment.

Organizations should:

Set up supply chain policies consistent with NIST SP 800-53r5. SCRM involves identifying, assessing, and mitigating risks associated with the supply chain to ensure the integrity, security, and resilience of the system.

SCRM CONSIDERATIONS

- **Supplier Assessment:** Regularly assess suppliers for their security posture, compliance with standards, and potential risks they may introduce to the supply chain.
- **Contractual Obligations:** Include security requirements and expectations in supplier contracts to ensure they are legally bound to adhere to the organization's security policies and standards.
- **Continuous Monitoring:** Implement continuous monitoring of the supply chain to identify and address potential risks in real time.
- **Incident Reporting and Response:** Establish clear incident reporting and response protocols with suppliers to ensure timely communication and resolution of security incidents.
- **Supply Chain Mapping:** Create a comprehensive map of the supply chain to identify critical components and potential points of failure.
- **Diversification:** Diversify suppliers to reduce reliance on a single source and mitigate the impact of potential supply chain disruptions from countries like China.

cATO in Contracts

To successfully implement cATO, organizations must embed security, compliance, and continuous monitoring requirements language into contracts with vendors, service providers, and internal teams. This ensures that all parties align with cATO principles, supporting real-time security visibility, automation, and compliance enforcement throughout the system lifecycle.

Below are recommended clauses to include in contracts with vendors, service providers, and internal teams to align with cATO objectives:

- The Contractor shall implement and maintain security and compliance controls in alignment with [NIST SP 800-53r5 / FedRAMP / DoD RMF / applicable framework] throughout the contract term. Controls must support automation, auditability, and integration with the Agency's continuous monitoring infrastructure.
- The Contractor shall provide continuous monitoring data, including but not limited to security event logs, vulnerability scan results, and configuration data, via API or secure interface, to the Agency's centralized monitoring platform. Monitoring must support automated ingestion and real-time alerting capabilities.
- The Contractor shall ensure all deployed tools and systems support automated compliance reporting and data sharing using machine-readable formats (e.g., OSCAL, JSON, or XML). Manual reporting shall not substitute for automated compliance data feeds unless it is explicitly authorized.
- The Contractor shall deliver and maintain up-to-date, machine-readable documentation for system architectures, security controls, and data flows. Changes to the system impacting the security posture must be documented and reported to the Authorizing Official prior to implementation.
- The Contractor shall design and operate services in alignment with the Agency's Continuous Authority to Operate (cATO) strategy, including the use of approved dashboards, automated evidence collection, and risk-based decision support tools.

References

Ongoing Authorization/cATO

- Risk Management Framework for Information Systems and Organizations
- Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

Software Bill of Materials (SBOM)

- Software Security in Supply Chains: Software Bill of Materials (SBOM) | NIST
- Subpart 504.70- Cyber-Supply Chain Risk Management
- Software Security in Supply Chains | NIST
- SBOM - Glossary | CSRC

Software Factory

- DoD Enterprise DevSecOps Reference Design v1.0_Public Release.pdf
- DoD Enterprise DevSecOps Fundamentals

Security as Code

- Security Considerations for Code Signing
- Security-Oriented Code Review - Glossary | CSRC