White Paper

cATO Working Group Concept Paper

ATARC cATO Working Group

October 2024

ATARC
Advanced Technology Academic Research Center

Table of Contents

***Disclaimer**: This document was prepared by the members of the ATARC cATO Working Group in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with and shall not be used for advertisement or product endorsement purposes.*

Typically, obtaining an initial Authorization to Operate (ATO) under the Risk Management Framework (RMF) can take anywhere from 6 to 36 months. 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 stakeholders.

This paper outlines the purpose of the cATO working group and the specific work streams it comprises. The primary objective of this group is to enhance the ATO/cATO process in order to lessen the overall impact on the critical triple constraints—scope, time, and cost—faced by programs or projects seeking an ATO for implementation in any operational setting.

cATO Working Group Guiding Principles

- Save money, time and make an agency's security program better
- Reduce toil
- Most important thing we can do!
    - Provide a useful deliverable, provide actionable guidance that is implementable today.
    - As much as possible: Prototype, Pilot, Template.
- Level set the *misery index*
    - Provide best advice based on skills, budgets, and programs.
    - Our assumption should not be large budgets and a deep bench of skilled individuals.
    - Additionally, we should not assume that budgets will continue to grow for cybersecurity and that they may begin to decline.
- Prefer objective vs subjective data when possible.
- Prefer tests (technically verifiable) vs interviews when providing actionable guidance.
    - Publish these tests when possible.

Workstream 1 - Tiering of Security Controls

To efficiently manage the deployment and continuous improvement of security controls within the Authorization to Operate (ATO) process, a tiered or prioritized strategy is adopted. This approach organizes the implementation and enhancement of security measures into distinct levels, each targeting different security requirements of the system. It begins with the most critical security elements and gradually tackles more strategic and long-term goals. This tiered system ensures that vital controls are implemented quickly and effectively. Later tiers expand on the initial security foundations, promoting a robust development of the system’s overall security posture as it matures. For instance, the requirements of control families can be phased in as illustrated below, allowing each program to determine which phase is most crucial:

1		Control 1
2		Control 2
3		Control 3
4		Control 4

Tier 1: Immediate Implementation and Maturity - Tier 1 focuses on deploying and fully maturing critical controls that are essential from day one. These controls protect core functionalities and are crucial for the system's immediate operational security.

5		Control 5
6		Control 6
7		Control 7
8		Control 8
9		Control 9
10		Control 10

Tier 2: Gradual Maturation - Tier 2 controls are important but can be matured over time as the system evolves and additional layers of security become necessary. This phase allows for a more flexible implementation schedule.

11		Control 11
12		Control 12
13		Control 13
14		Control 14
15		Control 15
16		Control 16
17		Control 17
18		Control 18
19		Control 19

Tier 3: Long-term Strategic Implementation - The controls in Tier 3 are focused on broader program management activities that support the security infrastructure indirectly. These controls can be aligned with the long-term strategic goals of the organization.

This framework seeks to add more agility to the cATO processes such that Product Owners of systems can accrue evidence[1] to satisfy the controls needed as they progress through the RMF framework and the SELC/SDLC.

Workstream 2 – Integration of NIST SPs 800-160 and 800-37

To expedite the ATO process, it is essential to integrate security engineering principles from NIST Special Publication 800-160. This guidance underscores the significance of embedding security at the initial stages of system development (shift left). Implementing these principles early in the system lifecycle enables organizations to methodically address potential vulnerabilities and security requirements throughout the Systems Engineering Life Cycle (SELC) / Systems Development Life Cycle (SDLC). This proactive strategy not only embeds security into the system from the outset but also diminishes the repetitive back-and-forth that often characterizes the ATO process, typically occurring towards the project's completion.

To optimize these advantages, cybersecurity assessors should evaluate security controls during their development instead of waiting until the end of the project. This approach allows cybersecurity assessment activities to run simultaneously with other project tasks, streamlining the entire process. Conducting these assessments in parallel not only improves project timelines but also helps to shorten the traditional 6-to-36-month timeline typically required to secure an ATO at the conclusion of the project. This method not only accelerates the authorization process but also promotes a more secure system deployment from the outset.

Workstream 3 – Barriers and Successes Related to ATOs / cATO

Organizational barriers, whether related to people, processes, or technology, and exacerbated by internal and external pressures, can significantly slow the ATO process. This workstream will provide steps designed to identify and remove these barriers and deficiencies. By providing a roadmap that can be adapted to the culture of various agencies, the aim is to overcome stagnation and enhance process efficiency. Additionally, this workstream will offer practical, actionable guidance to mitigate these challenges and will share successful strategies that have been implemented in other organizations.

[1] https://csrc.nist.gov/glossary/term/evidence

Workstream 4 – Tools and Technology Enablement for cATO

Having the appropriate tools and technology, equipped with necessary security features and user-friendly interfaces, is crucial for accelerating cATO efforts. A vital component for cATO tools is the ability to interoperate—processing, consolidating, and presenting data from various sources to provide real-time insights that empower decision-makers to issue cATO authorization ratings. cATO teams must carefully assess which technologies will effectively facilitate the orchestration of cATO activities.