ATO as Code

Enabling Cybersecurity Modernization Through Risk Management Framework Compliance Automation

Cybersecurity Community of Interest

Date Released: March 26, 2024

Synopsis
This ATO-as-Code report issues a call to action for a unified approach for modernizing the Authorization to Operate (ATO) process or Risk Management Framework (RMF) implementation.

https://www.actiac.org/documents/ato-code
Agenda

> Welcome

> Project Overview

> Project Goals

> Whitepaper / Next Phase
<ato-as-code />: Project Overview

The ATO as Code Project within the Cybersecurity COI seeks to leverage a collaborative partnership between industry and agencies to help reduce the time and cost of ATOs and improve security by making it easier to perform continuous monitoring.

The ATO as Code project is an open solution accelerator that brings together:

> technologies
> a&a processes
> business metrics

Mission Assurance
In order to maximize the impact of the project and to tap into the wide variety of skillsets within the volunteer group, the following workstreams are proposed:

the “tech” > developers and “coders” who can develop and implement OSCAL models and produce workable artifacts and automation pipelines

the “process” > information assurance & rmf experts who can guide the process integration steps for adopting and incorporating machine readable artifacts into the ATO process

the “business impact” > program and business experts who can help quantify how to evaluate and present business value of faster ATOs and continuous monitoring.
The **Compliance Automation Process Maturity Model (CA PMM)** is intended to define a basic model to help organizations safely and rapidly adopt and scale OSCAL. The CA PMM does not prescribe a specific approach to build a fast, high-performing, and security-focused organization, but instead defines the basic principles to measure an organization’s process towards that goal. The CA PPM identifies 5 levels of maturity as defined in the sections below.
<ato-as-code />: Critical Factors

**DATA**

Make access to cybersecurity compliance and risk information easy by creating a common standard for how that data is collected and curated to provide insights into risk posture that expedite decision making. Provide agencies with the data to allow them to make intelligent policy decisions on the right fit of policy for the enterprise.

**TECHNOLOGY**

Automate the compliance process by leveraging the new data standard to rapidly build an ATO package, identify gaps in requirements, and recommend a risk decision. Technology should also improve information sharing between all stakeholders involved in the ATO and decision-making process. By automating the federal compliance process, we can then utilize it for advanced IT security analytics and real-time risk analysis, etc.

**MISSION**

Have a cohesive policy, inclusive of the OSCAL standard, that the rest of the enterprise can leverage and use automation to get additional levels of fidelity into the effectiveness of policy in relation to cybersecurity. Get to mission delivery faster by establishing these standards around IT delivery.
ATO as Code

Enabling Cybersecurity Modernization Through Risk Management Framework Compliance Automation

Cybersecurity Community of Interest

Date Released: March 26, 2024

Synopsis

This ATO-as-Code report issues a call to action for a unified approach for modernizing the Authorization to Operate (ATO) process or Risk Management Framework (RMF) implementation.
Thank you for attending!