ACT-IAC  
ATO-AS-CODE

Problem Statement

Version 1.0  
July 26, 2023

# **INTRODUCTION**

The American Council for Technology Industry Advisory Council (ACT-IAC) has formed a working group to expedite the application of automation to increase the efficiency of the compliance process and the effectiveness of cybersecurity risk management. The US Federal Government, IT security professionals, and other practitioners involved in the cybersecurity lifecycle are required to adhere to the FISMA guidelines. New technologies enable us to automate many currently manual aspects of this process and refocus professionals’ time on proactively protecting and securing IT and critical infrastructure.

# **OBJECTIVE**

The Federal Information Security Management Act of 2002 (FISMA) harmonized previous legislation (Government Information Security Reform Act, the Computer Security Act of 1987, the Clinger-Cohen Act, and the Paperwork Reduction Act of 1980). In 2014, FISMA was updated, focusing on risk management, continuous monitoring, proactive cybersecurity and it encouraged agencies to stay-up-to-date on best practices and emerging threats. It is estimated that since 2002, Federal agencies have spent well over $100 billion to safeguard their IT systems. On paper, FISMA fosters accountability and empowers both agencies and the Office of Management and Budget (OMB) to govern, execute and enforce the necessary components for implementing a cybersecurity program. Nevertheless, compliance has been slow due to persistent execution and responsibility ambiguities, along with funding constraints, since its inception. Compounding the lack of funding with the fact that FISMA has long been viewed as uninspiring, tedious, “unsexy” work with no connection to substantive policy goals.

With the increase in security related work, we have to modernize how we “answer the mail” on the various FISMA requirements. It is our mission to make the compliance process better for IT professionals and their teams that are required to adhere to these guidelines. By reducing manual processes through automation, cybersecurity and IT professionals can focus more on risk management as opposed to the current manual/paper-based processes that *support* risk management. It is also necessary to identify where data can improve transparency throughout the customer journey. Data exchange and governance is also vital for the program to integrate with a network of CIOs, CISOs, CFOs, and CDOs.

# **CRITICAL SUCCESS FACTORS**

The ATO-as-Code working group recognizes that a standardized approach to communicating cybersecurity risk data is a prerequisite to begin automating and modernizing the ATO process. The driving force behind this project or the critical success factors are:

**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.

# **BUSINESS REQUIREMENTS**

To achieve these three critical success factors, the ATO-as-Code Working Group will need to address the following business requirements which include:

* Use of innovative analytics to enable real-time risk assessment.
* Collect and analyze quantitative and qualitative data from multiple sources to shape the product roadmap for both internal and external users.
* Lead and facilitate modern agile and devops practices for the capabilities developed for this effort.

**This working group is until the end of December and follow-on actions will be determined at that time.**