ALPHA OMEGA
INTEGRATION
CREATING NEW POSSIBILITIES

A2O^{TM}
A platform for automating your ATO process

Achieving Continuous ATO with Intelligent Automation

Introduction

An Authorization to Operate (ATO) is a fundamental step to meeting security compliance before approving a software application and then continuously monitor the application during the life of the system. However, our experience suggests that, on average, an ATO can take anywhere between 6 – 18 months to complete. This length of time can stifle change, make applications stale, and limit the pace of modernization or transformation.

Alpha Omega Integration's (AOI) project experience and industry research suggests that the current ATO process which covers 17 control families and over 400 controls for a high baseline control system is very manual leading to prolonged timelines, delays in rolling out innovations that create business value, and increases system risk to an agency.

At AOI, we have been helping our clients reduce the time to ATO by combining our cybersecurity , intelligent automation and agile competencies. As a result, our customers have benefitted through reduction of time and cost associated with ATOs; achieved consistency in results and continuous compliance and monitoring; decreased system risk to the agency; and accelerated time to achieving and maintaining ATOs.

Our Approach

Our experience suggests — as evidenced by the results our clients have achieved — a multi-disciplinary pragmatic approach is required to reduce the time it takes to complete a system going through ATO, or for re-certifying a system. As a result, we have built A2O™ to address the lifecycle of the ATO process from gathering and evaluating the necessary controls based on the system's security profile, to identifying exceptions in security posture and monitor controls. Built on and in collaboration with the industry leading automation vendor UiPath, A2O™ takes a continuous automation approach to ATO by automating collection of data from manual controls , executing the controls, identifying gaps, and increasing observability and transparency, through technical and operational dashboards.

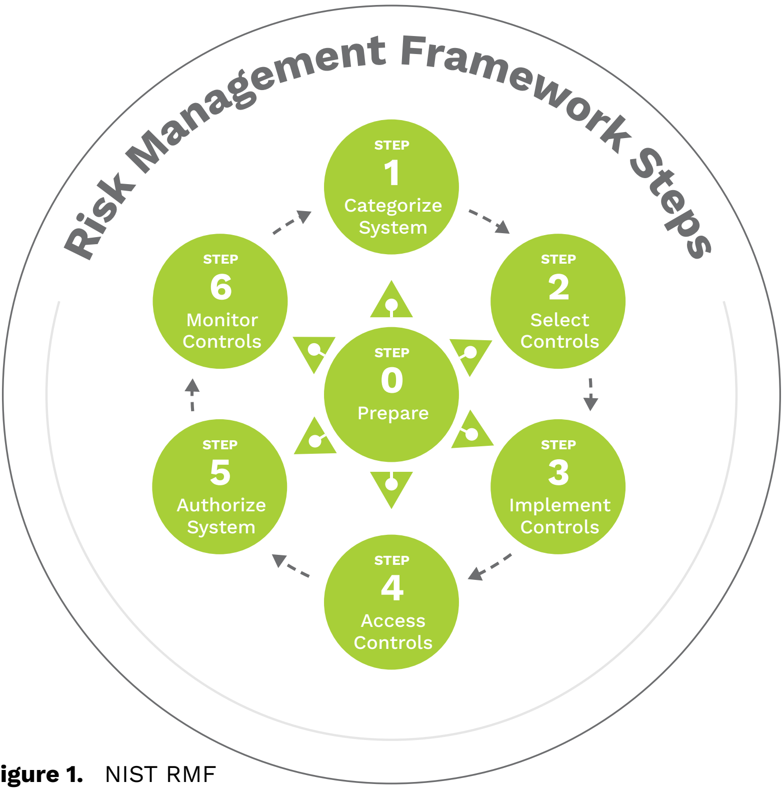


Figure 1. NIST RMF

The NIST Risk Management Framework (RMF) provides a flexible, holistic, and repeatable 7-step process (Fig. 1) to manage security and privacy risk and links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of the Federal Information Security Modernization Act (FISMA). A2O™ used the RMF as a guide to discover the greatest value for automation in the ATO process.

Our Approach

From evaluating the 7 steps within the RMF, the development of the A2O^{TM} platform focuses on steps 2, 3 and 6. Based on our experience, these are the steps that take most of the time, require a high degree of co-ordination, and potentially affect the effectiveness of the process. In this current state of our solution we chose to exclude the assessment of the system (Step 4) and the authorization of the system (Step 5), to ensure independence, and provide the data. However, based on the scope of engagement, the A2O^{TM} platform can be extended to support these needs.. Figure 2 illustrates our approach.

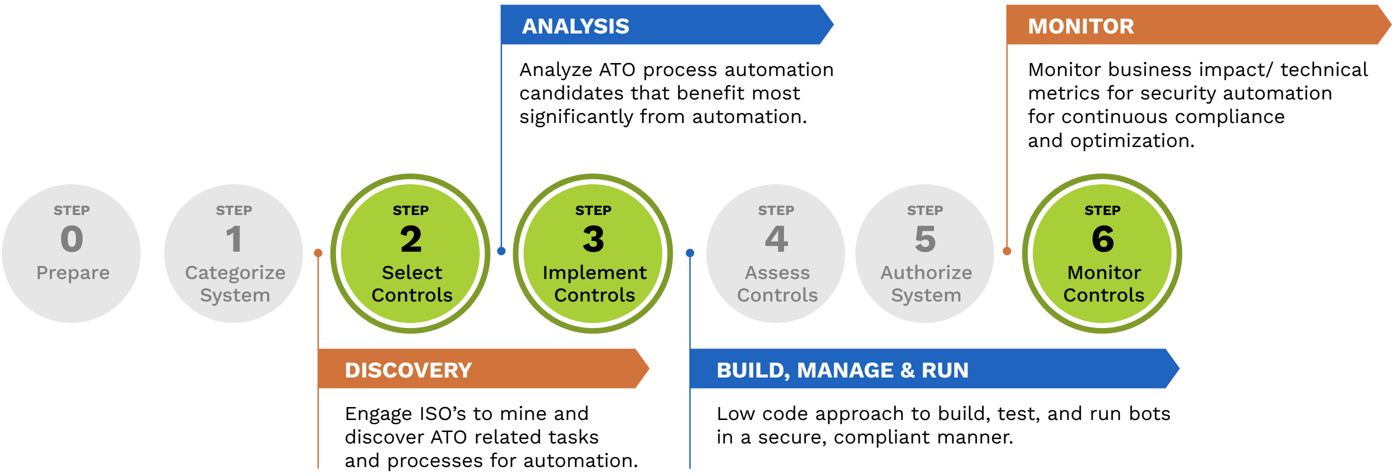

ANALYSIS
Analyze ATO process automation candidates that benefit most significantly from automation.
MONITOR
Monitor business impact/ technical metrics for security automation for continuous compliance and optimization.
STEP 0 Prepare
STEP 1 Categorize System
STEP 2 Select Controls
STEP 3 Implement Controls
STEP 4 Assess Controls
STEP 5 Authorize System
STEP 6 Monitor Controls
DISCOVERY
Engage ISO's to mine and discover ATO related tasks and processes for automation.
BUILD, MANAGE & RUN
Low code approach to build, test, and run bots in a secure, compliant manner.

Figure 2. A2O's Intelligent Automation Steps mapped to RMF Steps

Automating steps 2, 3 and 6 provides the most significant benefit for the ATO and continuous monitoring efforts. The A2O^{TM} platform focuses on steps 2, 3 and 6 through the following:

Discovery — We achieve this by data mining the tasks and processes that are carried out by ISOs and/or others involved in the ATO process. This provides us a baseline for how the ATO process is achieved, what are the typical steps, and the variations around each step.

Analysis — The discovery leads to understanding the standardization opportunities in ATO process and data along with identifying the candidates/steps for automation, while being able to forecast the benefits.

Build, Manage & Run — Once socialized and agreed upon within an agency, a series of bots automate activities from data collection, aggregation, and analysis to identify exceptions in security posture. These bots can be run individually as an assistant to ISOs or can be run end-to-end across the span of steps 2, 3 &6 of the ATO process.

Monitor — Once the bots are run as part of the ATO process, the A2O^{TM} platform monitors the process both at a technical and operational level to ensure business performance and optimization.

A2O™ in Action – USE CASES

Our client at the Navy's future Naval Networking Environment (NNE), operates one of the largest combined networks in the world, providing: secure end-to-end IT services to more than 400,000 hardware devices and 800,000 users at over 1,600 Continental United States (CONUS) sites, end-to-end IT services to nearly 30,000 hardware devices and 45,000+ users across 82 other locations. Further, it is interoperable with and leverages other Department of Defense (DoD) net-centric enterprise services.

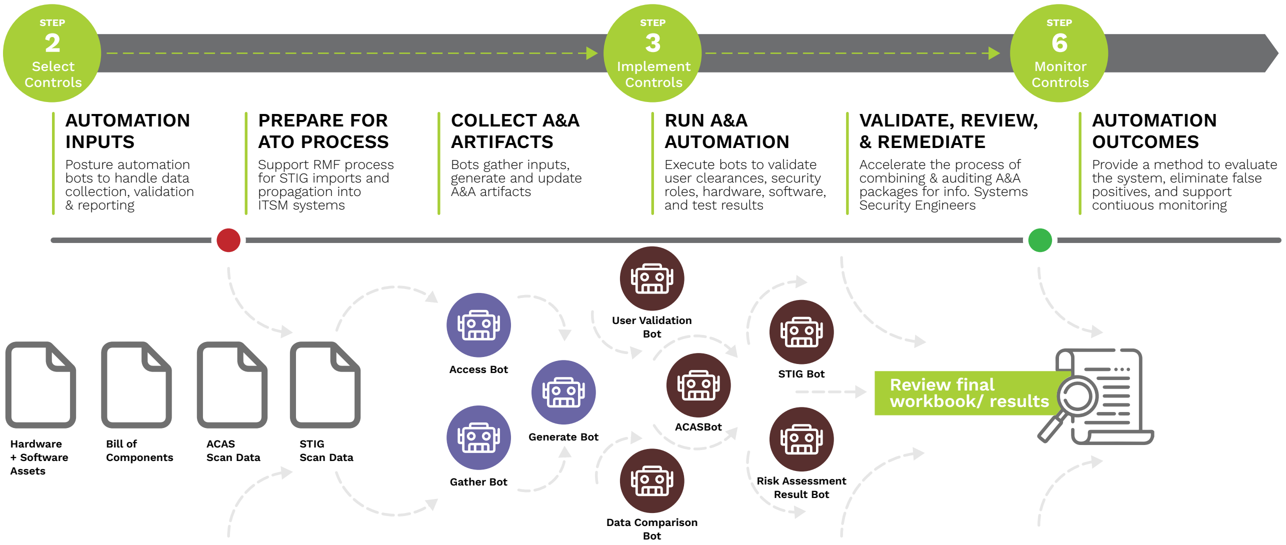
Their Authorization and accreditation (A&A) process was highly manual and labor-intensive involving multiple sources of data spread across many source systems that require Information Systems Engineers to go through the following steps:

1. Collect the data and establish a baseline workbook
2. Update the workbooks with ACAS and STIG scan data
3. Validate, analyze, publish results
4. Take remedial action

The planning, execution and governance of the A&A process was spread across a team of security engineers who had to co-ordinate and deliver the results to support the agency and contract requirements. As a result, the team faced challenges such as successful process and results co-ordination, accuracy of results, and time required to carry out the A&A process.

To meet the Navy's needs while addressing the challenges faced by the engineering team in delivering results, we developed the following intelligent automation approach and solution:

- At a high level we automated the entire A&A process (Figure 3) from data collection to validation to publishing exceptions and outcomes. The automation, which is a series of UiPath bots (both individual and aggregate), augments the information systems engineering team to implement steps 2, 3 & 6 of the RMF process from data collection to resolving vulnerabilities while taking technical actions to secure network and infrastructure.
- The scope of the data processed by the bots included:
  - Hardware and software assets
  - List of IT components from the bill of materials,
  - IT environment designs including but not limited to host, ports, protocols and network connection details.
  - ACAS data — includes ports, protocols, and vulnerabilities in the environment.
  - STIG data — includes ports, protocols, and vulnerabilities in the environment.



AUTOMATION INPUTS
Posture automation bots to handle data collection, validation & reporting

PREPARE FOR ATO PROCESS
Support RMF process for STIG imports and propagation into ITSM systems

COLLECT A&A ARTIFACTS
Bots gather inputs, generate and update A&A artifacts

RUN A&A AUTOMATION
Execute bots to validate user clearances, security roles, hardware, software, and test results

VALIDATE, REVIEW, & REMEDIATE
Accelerate the process of combining & auditing A&A packages for info. Systems Security Engineers

AUTOMATION OUTCOMES
Provide a method to evaluate the system, eliminate false positives, and support contiuous monitoring

Figure 3. A2O deployed at Navy

By deploying A2OTM the Navy realized the following benefits:

RMF process for STIG imports and propagation was reduced by **90%**

ISO time required to combine and audit A&A packages reduced by **90%**

Processing and validation defects with A&A reduced by **80%**

A&A Process standardized and streamlined to improve effectiveness

Key Stakeholders and Risk Management

A2O^{TM} addresses key stakeholders in the development lifecycle such as assurance stakeholders. This helps AOI ensure that proper security and internal controls are considered during the intelligent automation development life cycle. The A2O^{TM} team includes the System Owner, RPA Development Team, and Assurance Stakeholders with the following responsibilities: Systems Security, Information Security, Privacy, IT Risk Management, Internal Compliance, and Internal Control.

While implementing an Intelligent Automation solution brings operational effectiveness and efficiency to an organization, it also mitigates new risks introduced to the existing business system environment. The A2O^{TM} solution mitigates the risk by proactively identifying, assessing, and managing the risks with appropriate controls.

The AOI team pays attention to the tailoring controls over the following risk areas while implementing the solution for a specific engagement:

- Program Management
- Risk and Governance
- Access Controls
- Configuration Management
- Segregation of Duties

A2O^{TM} solution provides support for audit response activities, and can provide the following types of evidence in support of compliance activities:

- Privacy Impact Analysis
- RPA Security Plan (e.g., RPA Standards, Naming Conventions)
- High-Risk Control Considerations
- Interconnection Security Agreements (ISA)
- Memorandums of Understanding

Our A2O^{TM} solution team will work with client key assurance stakeholders to manage the risks associated with control selection and testing and the development of the evidence that supports control activities.

A2O^{TM} Benefits

With A2O^{TM} agencies can automate data collection and manual activities related to controls of the ATO process, reuse collected data to create documents required for assessments and audits, and promote collaboration, simplicity, transparency, consistency and traceability.

By implementing A2O^{TM} agencies can:

- Reduce time and cost associated with ATOs
- Promote consistency in results and continuous compliance and monitoring
- Decrease the system risk to agency
- Accelerate time to achieving and maintaining ATO
- Drive innovation and change
- Increase compliance scores with automated evidence
- Become agile

Authors

Navin Maganti

Navin Maganti is the Vice President, Intelligent Automation at Alpha Omega Integration responsible for capabilities from strategy through execution across technologies such as RPA, Process Intelligence, Machine Learning and Artificial Intelligence. Navin holds a MSBA from Temple University, as well as a Bachelor's in Electrical Engineering from Pune University in India

Raju Gupta

Raju Gupta is an Information Assurance Engineer with over 14 years of IT and Cybersecurity Security experience. He has proven expertise with Risk Management Framework (RMF), Cybersecurity Security Framework (CSF), Privacy Act, NIST 800-53 controls, U.S. Federal Risk and Authorization Management Program (FedRAMP). He has successfully supported multiple federal agencies, such Department of Homeland Security (DHS -FEMA and Law Enforcement Agency), Department of Defense (DoD), Department of State (DoS), Federal Deposit Insurance Corporation (FDIC) in implementation of Cybersecurity, Governance, Risk, Compliance and ATO solutions. Raju holds the following certifications (CISA, CGEIT, CRISC, CEH, CNDA, and CPDSE) and has a MS in Computer System Management from University of Maryland University College.

About AOI

Alpha Omega was created with a passion to serve our nation by providing unparalleled value in government contracting. Whether it's intelligent automation, custom agile software development, cloud solutions, or infrastructure security, our customer-first approach ensures we address your challenges with an innovative approach designed for your mission.

Contact

HQ
8150 Leesburg Pike, Suite 1010
Vienna, VA 22182

Email
info@alphaomegaintegration.com

Phone
(703) 637-7300

Fax
(703) 637-7309