Thank you to our Sponsors

WIFI: Public

Introduction, SAO and ATO on AWS overview

ATO on AWS

AWS and APN Go to Market (GTM) Campaign Workshop

Tim Sandage

What is ATO on AWS?

“ATO on AWS” is the formal title and marketing catchphrase for the AWS World Wide Public Sector (WWPS) program that will help customers, partners and independent software vendors (ISVs) significantly accelerate the process and reduce costs of obtaining an authorization to operate (ATO) under required compliance frameworks, such as FedRAMP, PCI-DSS, DFARS, DoD SRG, CJIS, HIPPA, and others.

The program includes support, guidance, and reusable artifacts such as AWS and partner solutions and pre-built templates that customers can use to build and optimize DevOps, SecOps, Continuous Integration/Continuous Delivery (CI/CD), and Continuous Risk Treatment (CRT) using proven techniques from AWS Security Automation and Orchestration (SAO) methodologies

ato authority to operate on aws

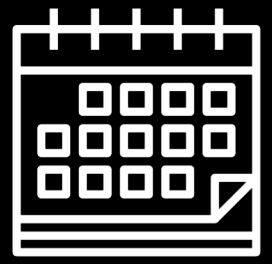
Breaking Down ATO on AWS

ATO on AWS is a partner-driven process that includes training, tools, pre-built CloudFormation templates, control implementation details, and pre-built artifacts.

Additionally, customers are able to access direct engagement and guidance from AWS compliance specialists and support from expert AWS consulting and technology partners who are a part of our Security Automation and Orchestration (SAO) initiative.

ato authority to operate on aws

Why ATO on AWS?



Time Consuming

Avg. 18-24 months

Complex

(e.g. 325 controls)

FedRAMP Moderate

Expensive

>$300-$800K

Avg. Security Assessment

Uncertain costs

TCO >$1m

ato authority to operate on aws

“ATO on AWS” campaign

Consists of multiple types of resources that will help accelerate the process for participating ISVs, including:

- **Training:** best practices for meeting compliance requirements for solutions on AWS, and maintaining a compliant environment effectively and efficiently over time.

- **Guidance, templates, tools, and partner solutions:** reusable artifacts, tools, and pre-built templates that ISVs can use to build and optimize DevOps, SecOps, Continuous Integration/Continuous Delivery (CI/CD), and Continuous Risk Treatment (CRT) using proven techniques from AWS Security Automation and Orchestration (SAO). Additionally, we have partnered with multiple solution providers who provide products and tools that help simplify and accelerate compliance authorization and management.

- **Direct engagement:** Qualified AWS compliance specialists will provide mentorship, oversight, and support through the process, from planning to authorization. We also have expert consulting partners trained in SAO who can be contracted to manage and support the process and resources.

- **Joint partner programs:** we will be supporting our leading AWS partners in the development and delivery of programs that add value to **“ATO on AWS”** by providing more options to unique capabilities to ISVs.

ato authority to operate on aws

“ATO on AWS” Campaign continued…

- **Qualified Managed Service Providers for Compliant Workloads:** We are working with our top managed service providers (MSP) to help them build and support environments that meet specific compliance standards. These MSPs will be good options for ISVs who prefer to minimize and simplify their area of responsibility by offloading hosting and compliance management.

- **Visibility and marketing:** Once ISVs achieve their ATO, we will jointly develop and execute a marketing and visibility plan to raise awareness and educate customers about the solution. Solutions will be published and marketed on the “ATO on AWS” landing page, and have the option of publication of a written or video case study/testimonial. This will also include formal “ATO on AWS” APN designations for the solutions that can be used by the ISV in their marketing artifacts and materials, as well as more specific derivatives, such as “**FedRAMP on AWS,” “SRG on AWS,” “CJIS on AWS,” etc.**

ato authority to operate on aws

Tenets for the ATO on AWS campaign

The following *Tenets* will guide the ATO program development:

- Automation – Leverage **"Infrastructure as Code"** concepts to construct, implement and run secure workloads through the use AWS services and partner innovation capabilities resulting in secure customer workload deployments capabilities globally.

- Certification - Optimize security processes to ensure they provide sufficient security value and continually reduce security and compliance effort through computerization.

- Validation – Enable continually test and monitor (e.g. Continuous Risk Treatments) of security configurations in AWS customer accounts to ensure their comprehensive operational effectiveness.

- Empowerment - Embolden informed decision-making and drive change through accurate cautious monitoring and actionable security metrics, which illustrates security in the cloud, is in advance of security on-premises

ato authority to operate on aws

aws

Existing Program Integration

- **AWS Security Automation and Orchestration (SAO)** ***methodology*** enables AWS customers to constrain, publish and track continuous risk treatments (CRT*), and configurations through the assimilation of DevOps routines (e.g. **continuous integration** (**CI**) and **continuous delivery** (**CD**)) into a “Type Accredited” secure AWS architecture which is designed to converge across common security frameworks (e.g. FedRAMP, DoD CC SRG, PCI-DSS, IRS 1075, etc.) through the use of security as code practices.

- **Security by Design (SbD)** - Is a security assurance approach, which enables customers to formalize AWS account design, automate security controls, and streamline auditing. This program will produce security automation based on secure leading practice configurations across all layers in an AWS customer accounts.

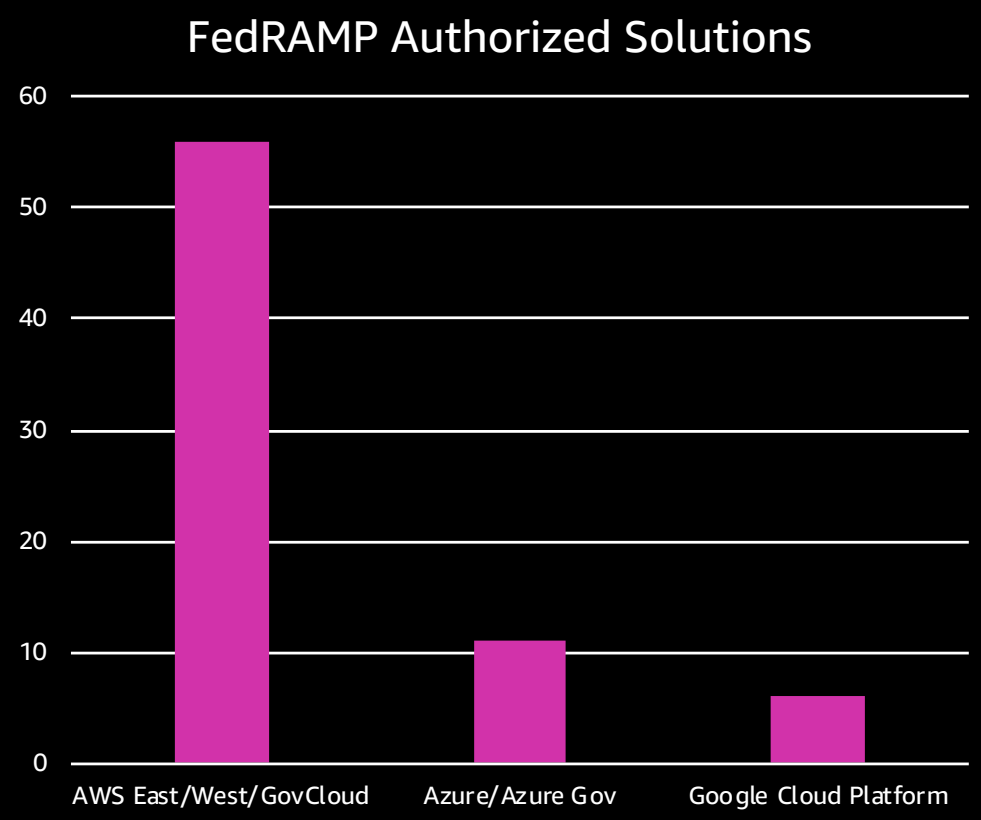
- **Modernizing Technology Governance (MTG)** – Is a four-step process for automating governance workflows to construct, implement and run secure workloads through directed, trustworthy and ratified governance automations in AWS.

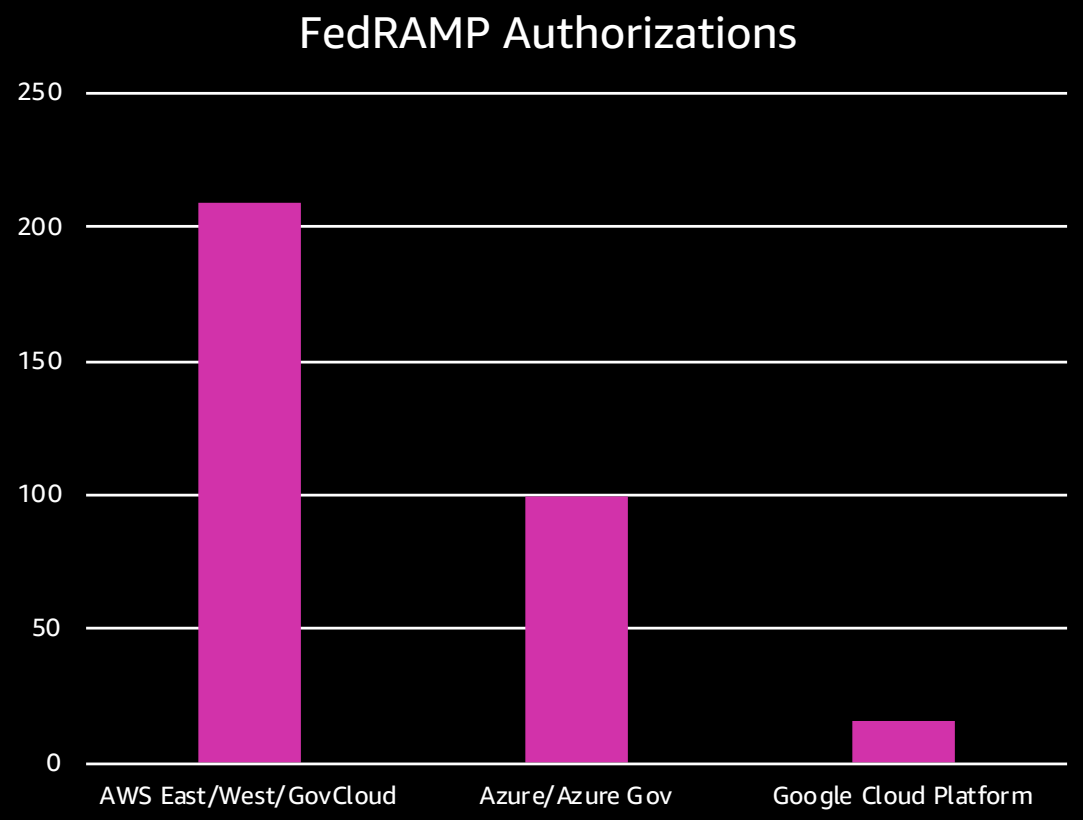
- **SbD Partners** – An underpinning of this project are partners which can empower, augment and advance SbD- MTG practices through amplified security capabilities and replication through advocacy and evangelizing our program globally.

ato authority to operate on aws

aws

Example of AWS ATO Leadership - FedRAMP





ato authority to operate on aws

2018 FedRAMP ATO's on AWS

ato authority to operate on aws

SAO Elevator Pitch?

"AWS SAO is an extensive set of, out-of-the-box integration and an API-first architecture which enables interoperability with any organization's existing security stack. Integrations for new and custom applications can also be easily developed using common scripting languages and a RESTful API.

AWS SAO makes it easy for AWS Customers to transition to an automated security capability to ensure that they can maintain their accreditations, certifications and compliance reports of their workload intact, all while deploying agile oriented software development and release management practices. This effort accelerates both AWS adoption, and customer value, by streamlining the accreditation process, and providing a defined workload migration and modernization platform.

AWS SAO reduces the effort of deployment, security configuring, and audit collection within an AWS customer account. The result of our combined AWS and Amazon Partner Network members efforts will create certified continuous configuration automation (CCA) solutions from both DevOps partners (e.g., Chef, Puppet, Ansible etc.) and Security partners (e.g. Splunk, CloudCheckr, CIS, etc.) to build an end to end automation capability for regulated and auditable workloads."

ato authority to operate on aws

aws

Key Benefits of AWS SAO

- ***Fast Track*** - A secure and swift automated deployment for regulated workloads in AWS

- ***Increased velocity*** **to market** – For AWS customer to achieve an Authority to Operate (ATO) **(current average is 18 – 24 months)**

- ***Assimilate*** - *SecOPS* and *DevOPS* practices into a **Governance as Code** (GaC) cycle for secure operations and orchestration, to keep accreditation baselines in place, as our customers look to become more agile in their adoption of AWS.

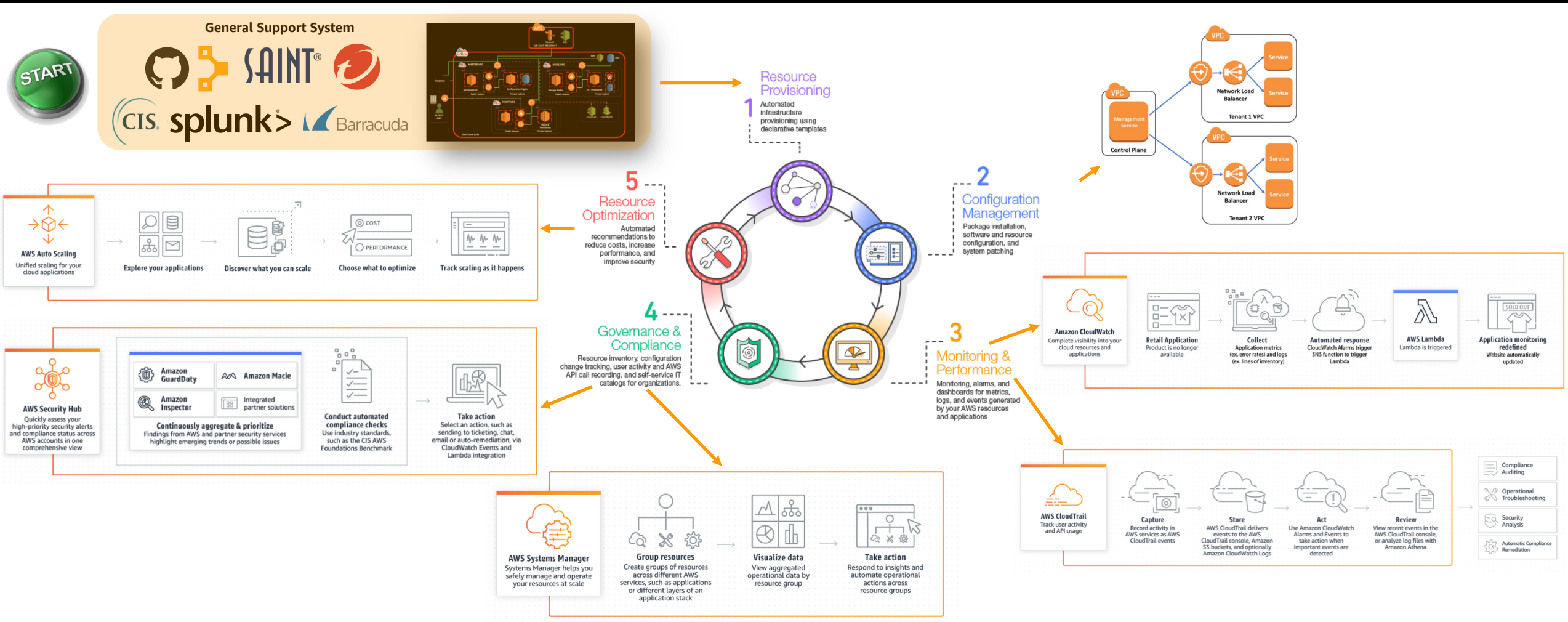
- ***Type Accredit*** – Pre-Audit automation package builds through APN Consulting Partners for PCI-DSS, FedRAMP and other compliance programs through (third-party assessment organizations).

- ***Solution Set –*** Distribution of SAO services, partner solutions and documentation library as single purchase through the use of marketplace contract terms. (e.g. **AWS SAO Trust Boundary in a Box**)

ato authority to operate on aws

aws

ATO on AWS using SAO…



ato authority to operate on aws

AWS SAO Pilots

FedRAMP

GitHub

circleci

Innovest
Forward thinking financial technology

smartsheet

CloudCheckr

DFARS

SNC SIERRA NEVADA CORPORATION
Space Systems

LOCKHEED MARTIN

COBHAM

esri

PCI-DSS

WORLD WEB TECHNOLOGY
We make your !deas work

Seattle

CollegeBoard

PROVENIR

HITRUST/HIPAA GDPR

ORION HEALTH

EDU

PEARSON
Education

CJIS

Nlets

REDFLEX TRAFFIC SYSTEMS

DoD

Newport News Shipbuilding

AIR FORCE LCMC

SLG

THE GREAT SEAL OF THE STATE OF MINNESOTA · L'ETOILE DU NORD · 1858

STATE OF COLORADO · NIL SINE NUMINE · 1876

CITY OF VANCOUVER

ato authority to operate on aws

aws

Thank you!

Questions

ato authority to operate on aws

aws