OPS Track ATO Sales Kick Off 2019

ATO on AWS

Joint Operations delivery (Documentation, Engagement and Technical)

Ted Steffan
Tres Vance
Luis Tapia

ATO on AWS (Documentation, Engagement and Technical)

Three focus areas for Operations:

1. Documentation
    1. ATO on AWS will create the documentation for AWS services
    2. ATO on AWS work with ISV partners to document how their solution treats security controls
2. Engagement
    1. ATO on AWS will maintain the ATOonAWS@amazon.com email box
        1. AWS will prescreen (qualify) opportunities (ISV, Consulting, SaaS/PaaS Provider)
        2. Qualified opportunities will be shared ATO on AWS partners
3. Technical
    1. ATO on AWS will create the automated deployment scripts for AWS services
    2. ATO on AWS work with ISV partners to create the automated deployment scripts for their solutions

ATO on AWS (Documentation)

ATO on AWS (Documentation)

Regulated workloads require significant amounts of documentation

For example, FedRAMP requires a cloud service provider to provide the flowing suite of documents:

- System Security Plan (SSP)
- Information Security Policies and Procedures
- User Guide
- Electronic Authentication (E-Authentication) Plan
- Privacy Impact Assessment (PIA)
- Rules of Behavior (RoB)
- Information System Contingency Plan (ISCP)
- Configuration Management Plan (CMP)
- Incident Response Plan (IRP)
- Control Implementation Summary (CIS) Workbook
- Federal Information Processing Standard (FIPS) 199 Categorization

ATO on AWS (Documentation)

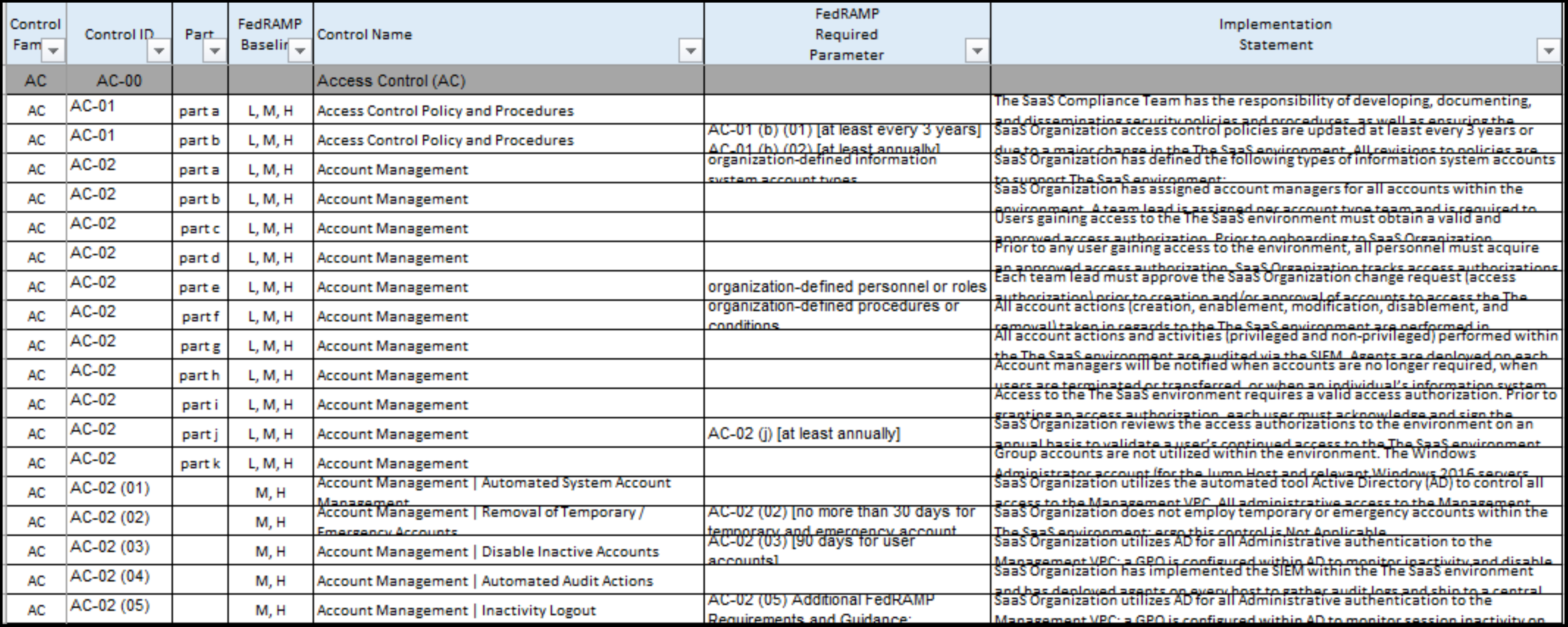
For ATO on AWS, we will create samples of the following documents based on the implementation of the AWS services:

- System Security Plan (SSP)
- Information Security Policies and Procedures
- User Guide
- Electronic Authentication (E-Authentication) Plan
- Privacy Impact Assessment (PIA)
- Rules of Behavior (RoB)
- Information System Contingency Plan (ISCP)
- Configuration Management Plan (CMP)
- Incident Response Plan (IRP)
- Control Implementation Summary (CIS) Workbook
- Federal Information Processing Standard (FIPS) 199 Categorization

ATO on AWS (Documentation)

- Our team will also work with our ISV partners to create the implementation statements relevant to their solutions.
- These statements will be maintained in a repository that will be equally available to all AWS partners.
- The intent is to make this documentation available to our SaaS and PaaS partners to accelerate them on their compliance journey.

ATO on AWS (Documentation)



Control Fam	Control ID	Part	FedRAMP Baselir	Control Name	FedRAMP Required Parameter	Implementation Statement
AC	AC-00			Access Control (AC)		
AC	AC-01	part a	L, M, H	Access Control Policy and Procedures		The SaaS Compliance Team has the responsibility of developing, documenting, and disseminating security policies and procedures, as well as ensuring the
AC	AC-01	part b	L, M, H	Access Control Policy and Procedures	AC-01 (b) (01) [at least every 3 years] AC-01 (b) (02) [at least annually]	SaaS Organization access control policies are updated at least every 3 years or due to a major change in the The SaaS environment. All revisions to policies are
AC	AC-02	part a	L, M, H	Account Management	organization-defined information system account types	SaaS Organization has defined the following types of information system accounts to support The SaaS environment:
AC	AC-02	part b	L, M, H	Account Management		SaaS Organization has assigned account managers for all accounts within the environment. A team lead is assigned per account type team and is required to
AC	AC-02	part c	L, M, H	Account Management		Users gaining access to the The SaaS environment must obtain a valid and approved access authorization. Prior to onboarding to SaaS Organization
AC	AC-02	part d	L, M, H	Account Management		Prior to any user gaining access to the environment, all personnel must acquire an approved access authorization. SaaS Organization tracks access authorizations
AC	AC-02	part e	L, M, H	Account Management	organization-defined personnel or roles	Each team lead must approve the SaaS Organization change request (access authorization) prior to creation and/or approval of accounts to access the The
AC	AC-02	part f	L, M, H	Account Management	organization-defined procedures or conditions	All account actions (creation, enablement, modification, disablement, and removal) taken in regards to the The SaaS environment are performed in
AC	AC-02	part g	L, M, H	Account Management		All account actions and activities (privileged and non-privileged) performed within the The SaaS environment are audited via the SIEM. Agents are deployed on each
AC	AC-02	part h	L, M, H	Account Management		Account managers will be notified when accounts are no longer required, when users are terminated or transferred, or when an individual's information system
AC	AC-02	part i	L, M, H	Account Management		Access to the The SaaS environment requires a valid access authorization. Prior to granting an access authorization, each user must acknowledge and sign the
AC	AC-02	part j	L, M, H	Account Management	AC-02 (j) [at least annually]	SaaS Organization reviews the access authorizations to the environment on an annual basis to validate a user's continued access to the The SaaS environment
AC	AC-02	part k	L, M, H	Account Management		Group accounts are not utilized within the environment. The Windows Administrator account (for the Jump Host and relevant Windows 2016 servers
AC	AC-02 (01)		M, H	Account Management | Automated System Account Management		SaaS Organization utilizes the automated tool Active Directory (AD) to control all access to the Management VPC. All administrative access to the Management
AC	AC-02 (02)		M, H	Account Management | Removal of Temporary / Emergency Accounts	AC-02 (02) [no more than 30 days for temporary and emergency account	SaaS Organization does not employ temporary or emergency accounts within the The SaaS environment; ergo this control is Not Applicable.
AC	AC-02 (03)		M, H	Account Management | Disable Inactive Accounts	AC-02 (03) [90 days for user accounts]	SaaS Organization utilizes AD for all Administrative authentication to the Management VPC; a GPO is configured within AD to monitor inactivity and disable
AC	AC-02 (04)		M, H	Account Management | Automated Audit Actions		SaaS Organization has implemented the SIEM within the The SaaS environment and has deployed agents on every host to gather audit logs and ship to a central
AC	AC-02 (05)		M, H	Account Management | Inactivity Logout	AC-02 (05) Additional FedRAMP Requirements and Guidance:	SaaS Organization utilizes AD for all Administrative authentication to the Management VPC; a GPO is configured within AD to monitor session inactivity on

ATO on AWS (Engagement)

ato authority to operate on aws

aws

ATO on AWS (Engagement)

1. Engagement
    1. AWS will maintain the ATOonAWS@amazon.com & SAO@amazon.com email boxes

ATO on AWS (Engagement)

1. Engagement
   1. AWS will prescreen (qualify) opportunities (ISV, Consulting, SaaS/PaaS Provider)
      1. ISV partners, once qualified, we will onboard them into the program
         1. ISV partners will receive a detailed orientation of the program, instructions and coaching on creating their documentation and automated deployment capability (covered in more detail in the Technical presentation)
            1. API integration capability (how can auditing be automated?)
            2. Pricing structures will need to be provided to AWS (under NDA) to assist in the qualification process

ATO on AWS (Engagement)

1. Engagement
    1. AWS will prescreen (qualify) opportunities (ISV, Consulting, SaaS/PaaS Provider)
        1. Consulting partners, once qualified, we will onboard them into the program
            1. Consulting Partners will receive a detailed orientation on the program and provided access to shared resources to enable them to build out their deployment capability
                1. All opportunities must be entered into APN Opportunity Management Tool located in APN Partner Central and tied to the “NA-US-FY19-ATO-ON-AWS-Program”
            2. SaaS & PaaS providers that are qualified will be shared with consulting partners for further discussion and quoting
                1. AWS will maintain visibility into consulting partner opportunities to help eliminate roadblocks and provide resources where appropriate

ATO on AWS (Technical)

Thank you!

Ted Steffan

ato authority to operate on aws