ATO on AWS Program

Technology Partner Validation Checklist

March 15, 2021
Version 1.2

aws partner network

Table of Contents

Introduction

The goal of the Authority to Operate (ATO) on AWS Program (Program) is to recognize and work jointly with AWS Partner Network Partners (AWS Partners) who demonstrate technical proficiency and proven customer success in specialized solution areas, namely associated with specific security and compliance frameworks.

The ATO on AWS Partner Validation Checklist (Checklist) is intended for AWS Partners who are interested in applying for the Program. As part of the application process, AWS Partners will perform a self-assessment using the Checklist and submit all application materials through the AWS Partner Central portal. Once submitted, the ATO on AWS team will be alerted, and AWS Partners will undergo an audit of their capabilities to validate Program eligibility.

Expectations of Parties

AWS Partners are expected to review this document in detail before requesting membership in the Program. AWS Partners should prepare for the audit by completing a self-assessment using the Checklist in addition to gathering and organizing objective evidence to share with the ATO on AWS team. Once AWS Partners have submitted their application, the ATO on AWS team will aim to review the application and reach out to the AWS Partner within five (5) business days of the date submitted to schedule the audit or request additional information.

AWS recommends that AWS Partners identify specific points-of-contact within their organization who are able to speak in-depth to the Checklist requirements. AWS Partners are expected to make the following personnel available to respond to any questions/comments from the ATO on AWS team: (1) one or more highly technical AWS certified engineers/architects and, (2) an operations manager who is responsible for the operations and support elements. Please note that this could be the same individual.

If you have questions about any of the items in the Checklist, please contact your AWS Partner Development Representative (PDR) or AWS Partner Development Manager (PDM) as the first step. If further assistance is required, your PDR/PDM will escalate to the ATO on AWS team. The ATO on AWS team will respond to any questions within five (5) business days.

ATO on AWS Program Prerequisites

To ensure prospective ATO on AWS Partners can demonstrate their expertise and experience supporting customers seeking security and compliance certifications and authorizations, applicants must be able to provide the following items/information which will be validated by the ATO on AWS team. If items are missing or incomplete, the scheduling of your validation review may be delayed as all open items will first have to be addressed.

1.0 APN Program Requirements		**Met Y/N**
1.1 Program Guidelines	AWS Partner must read the Program Guidelines before applying to the ATO on AWS Program. Program details can be found here.	
1.2 Solution Category	AWS Partner must describe whether their ATO on AWS solution is: • **Multi-tenant Software as a Service (SaaS):** Serves multiple customers from shared AWS infrastructure. All AWS accounts are managed by the AWS Partner. • **Single-tenant SaaS:** Serves multiple customers but have some infrastructure components deployed in AWS accounts dedicated to individual customers. All AWS accounts are managed by the AWS Partner. • **Managed Service:** Deployed on AWS and serve a single customer. All AWS accounts are managed by the AWS Partner. • **Customer-Deployed:** Deployed in a customer AWS environment. All AWS accounts are managed by the customer.	
1.3 Program Membership	AWS Partner must be a member of the Public Sector Partner Program (PSP).	
2.0 AWS Case Studies		**Met Y/N**
2.1 Security and Compliance Authorization - Specific Case Studies	AWS Partner must have two (2) AWS Case Studies specific to a single security and compliance authorization solution under review. Case studies must have been created or updated within the past 18 months, and must be for projects that are in production, rather than in a 'pilot' or proof of concept stage. For each AWS Case Study, the AWS Partner must provide the following information: ▪ Name of the customer ▪ Customer challenge ▪ Specific security and compliance framework(s)/program(s) authorization supported as defined in the AWS Compliance Program ▪ How the solution was deployed to meet the challenge ▪ Third party applications or solutions used ▪ Date the solution entered production ▪ Outcome(s)/result(s) ▪ Specific architecture diagrams, deployment guides and other materials depending on the type of solution, as described in the next section. This information will be requested as part of the program application process in the AWS Partner Central portal. The information provided as part of the AWS Case Study can be private and will not be made public. All applicable AWS Case Studies provided will be examined in the documentation review of the technical validation. The AWS Case Study will be removed from consideration for inclusion in the program if the AWS Partner cannot provide the documentation necessary to access the case study against each checklist item or if there were critical findings identified during the validation.	
2.2 Security and Compliance Specific Solution Criteria	The AWS Partner solution used in the AWS Case Studies must be meet the following requirements: ▪ It must be a security and compliance framework(s)/program(s) authorization solution, targeting one or more of the following primary steps in achieving compliance through automation: Product Design, Production Design, Production, and Operations. ▪ It must follow AWS best practices as defined in the AWS Well-Architected Framework. ▪ It must be clearly differentiated from existing solutions. (AWS Partner Network Program Solutions enable customers to do things that were previously unviable, cost-	

	prohibitive, or too difficult.)	
3.0 ATO on AWS Web Presence and Thought Leadership		**Met Y/N**
3.1 AWS Partner: AWS Landing Page	AWS customers are looking for solutions on AWS specifically to reduce the time required for security and compliance certifications and authorizations. An AWS Partner's publically available information online, specific to their AWS solution offering, provides customers with confidence about the AWS Partner's capabilities and experience in helping organizations achieve security and compliance certifications and authorizations. AWS Partner must have an AWS landing page that describes their security and compliance framework(s)/program(s) authorization solution(s), public AWS Case Studies, technology partnerships, and any other relevant information supporting the AWS Partner's expertise related to the pursuit of security and compliance certifications and authorizations on AWS. This AWS-specific security and compliance framework(s)/program(s) authorization page must be accessible from the AWS Partner's home page. The home page itself is not acceptable as an AWS Landing Page unless AWS Partner is a dedicated ATO on AWS Technology company and the home page reflects AWS Partner's concentration on ATO on AWS. While public AWS Case Studies are highly preferred, there could be constraints that disallow the AWS Partner from making these case studies public. The AWS Partner should engage their PDR/PDM to relay such constraints to the ATO on AWS team on their behalf. The ATO on AWS team will review and aim to respond back with any questions, clarifications or request more information within five (5) business days. The ATO on AWS team will advise on the gap in artifact requirements for the AWS Landing Page, subsequently.	
3.2 ATO on AWS Public Thought Leadership	ATO on AWS Program Partners are viewed as having deep domain expertise in ATO on AWS, having developed innovative solutions that leverage AWS services. AWS Partner must have public-facing materials (e.g., blog posts, press articles, videos, etc.) showcasing the AWS Partner's focus on and expertise in Security and Compliance framework(s)/program(s) authorization support. Links must be provided to examples of materials published within the last twelve (12) months.	
4.0 Business Requirements		**Met Y/N**
4.1 Field-Ready Toolkits	AWS Partner must have field-ready documentation and seller toolkits including a clear product value proposition that can be articulated to the AWS sales organization with all relevant information needed to determine fit for a customer opportunity (e.g., sales collateral, presentation, and customer use cases). Evidence must be in the form of sales collateral including a presentation, one-pager, and use-case checklist.	
4.2 Product Support/Help Desk	AWS Partner must show that they offer product support via web chat, phone, or email support to customers. Evidence must be in the form of description of support offered to customers for their product or solution.	
4.3 Joint AWS/AWS Partner Wins	AWS Partner must have a process to document and publicize joint wins. Evidence must be in the form of verbal description of process.	
5.0 AWS Partner Self-Assessment		**Met Y/N**
5.1 AWS Program Partner Program Validation Checklist Self-Assessment	AWS Partner must conduct a self-assessment of their compliance to the requirements of the ATO on AWS Technology Partner Validation Checklist. ▪ AWS Partner must complete all sections of the checklist. ▪ Completed self-assessment must be submitted through APN Partner Central, along with all supporting artifacts. It is recommended that AWS Partner has their solutions architect or PDM review the completed self-assessment before submitting to AWS. The purpose of this is to ensure the AWS Partner's AWS team is engaged and working to provide recommendations prior to the review and to help ensure a productive review experience.	

ATO on AWS Program Technology Partner Validation Checklist

In preparation for the validation process, AWS Partner should become familiar with the items outlined in this checklist and prepare objective evidence, including but not limited to: prepared demonstration to show capabilities, process documentation, and/or actual customer examples.

Note that several requirements below include "Supplemental Information." Supplemental Information will consist of either rationale for the requirement or additional AWS guidance to help AWS Partners meet the requirement. The ATO on AWS Program is guided by AWS Security and Compliance Best Practices and the Well-Architected Framework.

Technical Validation

AWS Partner will need to describe the AWS Case Study with an architecture diagram(s) in 1 of the 4 following categories:

- **Multi-tenant SaaS:** If listed as applicable, provide one architecture diagram for the whole solution and one architecture diagram for each AWS Case Study.
- **Single-tenant SaaS:** If listed as applicable, provide one architecture diagram for the whole solution and one architecture diagram for each AWS Case Study.
- **Managed Service:** If listed as applicable, provide one architecture diagram for each AWS Case Study.
- **Customer Deployed:** If listed as applicable, provide one architecture diagram for each AWS Case Study.

More information on the categories can be found in **Section 1.2**.

The architecture diagram(s) must meet all of the following requirements:

1. Shows the major elements of the architecture and how they combine to provide the AWS Partner solution to customers
2. Shows all of the AWS services used using the appropriate AWS service icons
3. Shows how the AWS services are deployed, including, Amazon Virtual Private Clouds (Amazon VPC), Availability Zones (AZs), subnets, and connections to systems outside of AWS
4. Shows the systems are highly available and that there are no single point of failures
5. Includes elements deployed outside of AWS (e.g. on-premises components or hardware devices)

1.0 Baseline

The baseline review is a set of items from the AWS Well-Architected Review deemed critical for the success of an APN Technology Partner solution that is built on or integrated with AWS.		**Applicability**	**Met Y/N**
1.1 AWS Business Support is enabled for the AWS Account	AWS Partner must show that Business Support (or greater) is enabled for the AWS Account to participate in the Program, though exceptions to this rule may be made on a case-by-case basis.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, and **Managed Service** Not applicable to **Customer-Deployed**	
1.2 AWS account root user is not used for routine activities	AWS Partner must show that the AWS account root user is not used for everyday tasks, even administrative tasks. **Supplemental Information:** Instead of using the AWS account root user for everyday tasks, adhere to the best practice of using the root user only to create your first IAM user. Then, securely lock away the root user credentials and use them to perform only a few account and service management tasks. To view the tasks that require you to sign in as the AWS account root user, see AWS Tasks That Require Root User. For a tutorial on how to set up an administrator for daily use, see Creating Your First IAM Admin User and Group.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	

1.3 AWS Identity and Access Management (IAM) user accounts used for all routine activities	AWS Partner must show that they do not use the AWS account root user for any task where it is not required. **Supplemental Information:** Instead, AWS Partner should show that they create a new IAM user for each person that requires administrator access and then make those users administrators by placing the users into an administrators group to which they attach the administrator access managed policy. Thereafter, the users in the administrators group should set up the groups, users, and so on, for the AWS account. All future interaction should be through the AWS account's users and their own keys instead of the root user. However, to perform some account and service management tasks, you must log in using the root user credentials.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
1.4 Multi-Factor Authentication (MFA) has been enabled on the AWS account root user	AWS Partner must show that they enable multi-factor authentication (MFA) for AWS account root user. **Supplemental Information:** Because your AWS account root user can perform sensitive operations in your AWS account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available including virtual MFA and hardware MFA.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
1.5 AWS CloudTrail is enabled for all AWS accounts in every AWS Region	AWS Partner must show that CloudTrail is enabled on all AWS accounts and in every AWS Region. **Supplemental Information:** Visibility into your AWS account activity is a key aspect of security and operational best practices. You can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.	Applicable **to Multi-tenant SaaS**, **Single-tenant SaaS**, and **Managed Service** Not applicable to **Customer-Deployed**	
1.6 CloudTrail logs are stored in an Amazon Simple Storage Service (Amazon S3) bucket owned by another AWS account	AWS Partner must show that CloudTrail logs are emplaced in a bucket owned by another AWS account and configured for extremely limited access, such as audit and recovery only.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, and **Managed Service** Not applicable to **Customer-Deployed**	
1.7 Amazon S3 log bucket for CloudTrail has Versioning or MFA Delete enabled	AWS Partner must show that CloudTrail log bucket contents are protected with versioning or MFA Delete.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, and **Managed Service** Not applicable to **Customer-Deployed**	
1.8 MFA is enabled for all interactive IAM users	AWS Partner must show that they enable MFA for all interactive IAM users. **Supplemental Information:** With MFA, users have a device that generates a unique authentication code (a one-time password [OTP]). Users must provide both their normal credentials (user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, and **Managed Service** Not applicable to **Customer-Deployed**	

1.9 IAM credentials are rotated regularly	AWS Partner must change passwords and access keys regularly and make sure that all IAM users in your account do as well. **Supplemental Information:** This way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a password policy to your account to require all your IAM users to rotate their passwords, and you can choose how often they must do so. For more information about rotating access keys for IAM users, see Rotating Access Keys.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, and **Managed Service** Not applicable to **Customer-Deployed**	
1.10 Strong password policy is in place for IAM users	AWS Partner must show that they configure a strong password policy for IAM users. **Supplemental Information:** If you allow users to change their own passwords, require that they create strong passwords and that they rotate their passwords periodically. On the Account Settings page of the IAM console, you can create a password policy for your account. You can use the password policy to define password requirements, such as minimum length, whether it requires non-alphabetic characters, how frequently it must be rotated, and so on. For more information, see Setting an Account Password Policy for IAM Users.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, and **Managed Service** Not applicable to **Customer-Deployed**	
1.11 IAM credentials are not shared among multiple users	AWS Partner must show that they create an individual IAM user account for anyone who needs access to their AWS account and that they create an IAM user for themselves as well, give that user administrative privileges, and use that IAM user for all their work. **Supplemental Information:** By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can change or revoke an IAM user's permissions any time. (If you give out your root user credentials, it can be difficult to revoke them, and it is impossible to restrict their permissions.)	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, and **Managed Service** Not applicable to **Customer-Deployed**	
1.12 IAM policies are scoped down to least privilege	AWS Partner must follow the standard security advice of granting least privilege. **Supplemental Information:** This means granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. Defining the right set of permissions requires some research. Determine what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS,** and **Managed Service** Not applicable to **Customer-Deployed**	
1.13 Hard-coded credentials (e.g., access keys) are not used	AWS Partner must follow best practices for managing AWS access keys and avoid the use of hard-coded credentials. **Supplemental Information:** When you access AWS programmatically, you use an access key to verify your identity and the identity of your applications. Anyone who has your access key has the same level of access to your AWS resources that you do. Consequently, AWS goes to significant lengths to protect your access keys, and, in keeping with our shared responsibility model, and you should, as well.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS, Managed Service,** and **Customer-Deployed**	

1.14 All credentials are encrypted at rest	AWS Partner must follow baseline requirement of ensuring the encryption of any credentials at rest.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS, Managed Service,** and **Customer-Deployed**	
1.15 Regular data backups are being performed	AWS Partner must perform regular backups to a durable storage service. Backups ensure that you have the ability to recover from administrative, logical, or physical error scenarios. **Supplemental Information:** Amazon S3 and Amazon Glacier are ideal services for backup and archival. Both are durable, low-cost storage platforms. Both offer unlimited capacity and require no volume or media management as backup data sets grow. The pay-as-you-go model and low cost per GB/month make these services a good fit for data protection use cases.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS, Managed Service,** and **Customer-Deployed**	
1.16 Recovery mechanisms are being tested on a regular schedule and after significant architectural changes	AWS Partner must test recovery mechanisms and procedures, both on a periodic basis and after making significant changes to your cloud environment. **Supplemental Information:** AWS provides substantial resources to help you manage backup and restore of your data.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS, Managed Service,** and **Customer-Deployed**	
1.17 Disaster Recovery (DR) plan has been defined	A well-defined DR plan includes a Recovery Point Objective (RPO) and a Recovery Time Objective (RTO). AWS Partner must define an RPO and an RTO for all in-scope services, and the RPO and RTO must align with the service level agreement (SLA) you offer to your customers	Applicable to **Multi-tenant SaaS, Single-tenant SaaS, Managed Service,** and **Customer-Deployed**	
1.18 RTO is less than 24 hours	AWS Partner must adhere to the baseline requirement of having RTO be less than 24 hours for core services.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS, Managed Service,** and **Customer-Deployed**	
1.19 DR plan is adequately tested	AWS Partner must have a DR plan that is tested against your RPO and RTO, both periodically and after major updates. At least one DR test must be completed.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS, Managed Service,** and **Customer-Deployed**	
1.20 Amazon S3 buckets within your account have appropriate levels of access	AWS Partner must ensure that the appropriate controls are in place to control access to each Amazon S3 bucket. **Supplemental Information:** When using AWS, it's best practice to restrict access to your resources to the people that absolutely need it (the principle of least privilege). For more on least privilege, see **Requirement 1.12**.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS, Managed Service,** and **Customer-Deployed**	

1.21 Amazon S3 buckets have not been misconfigured to allow public access	AWS Partner must ensure that buckets should not allow public access and are properly configured to prevent public access. **Supplemental Information:** By default, all Amazon S3 buckets are private and can only be accessed by users that have been explicitly granted access. Most use cases won't require broad-ranging public access to read files from your Amazon S3 buckets, unless you're using Amazon S3 to host public assets (for example, to host images for use on a public website), and it's best practice to never open access to the public.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS, Managed Service,** and **Customer-Deployed**	
1.22 A monitoring mechanism is in place to detect when Amazon S3 buckets or objects become public	AWS Partner must have monitoring or alerting in place to identify when Amazon S3 buckets become public. **Supplemental Information:** One option for this is to use AWS Trusted Advisor. Trusted Advisor checks buckets in Amazon S3 that have open access permissions. Bucket permissions that grant List access to everyone can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant Upload/Delete access to everyone create potential security vulnerabilities by allowing anyone to add, modify, or remove items in a bucket. The Trusted Advisor check examines explicit bucket permissions and associated bucket policies that might override the bucket permissions.	Applicable to **Multi-tenant SaaS, Single-tenant SaaS,** and **Managed Service** Not applicable to **Customer-Deployed**	

2.0 Security

The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.		**Applicability**	**Met Y/N**

2.1 AWS Access Keys only used by interactive users	AWS Partner must show that no AWS Access Keys are in use, except for in the following cases:
	
	1. Used by humans to access AWS services, and stored securely on a device controlled by that human.
	2. Used by a service to access AWS services, but only in cases where:
	  a. It is not feasible to use an Amazon Elastic Cloud Compute (Amazon EC2) instance role, Amazon Elastic Container Service (Amazon ECS) Task Role or similar mechanism
	  b. The AWS Access Keys are rotated at least weekly
	  c. The IAM Policy is tightly scoped so that it:
	  i. Allows only access to only specific methods and targets, and
	  ii. Restricts access to the subnets on from which the resources will be accessed.
		Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	

2.2 Amazon EC2 security groups are tightly scoped	AWS Partner must show that all Amazon EC2 security groups restrict access to the greatest degree possible. This includes at least: 1. Implementing Security Groups to restrict traffic between Internet and Amazon VPC, 2. Implementing Security Groups to restrict traffic within the Amazon VPC, and 3. In all cases, allowing only the most restrictive possible settings.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	

2.3 A monitoring mechanism is in place to detect changes in Amazon EC2 instances and Containers	AWS Partner must show that any changes to Amazon EC2 instances or Containers may indicate unauthorized activity and must, at a minimum, be logged to a durable location to allow for future forensic investigation. The mechanism employed for this purpose must at least: 1. Detect any changes to the OS or application files in the Amazon EC2 instances or Containers used in the solution. 2. Store data recording these changes in a durable location, external to the Amazon EC2 instance or Container. Examples of suitable mechanisms include: a. Deployment of file integrity checking via scheduled configuration management (e.g. Chef, Puppet, etc.) or a specialized tool (e.g. OSSEC, Tripwire or similar) b. Extending configuration management tooling to validate Amazon EC2 host configuration, and alert on updates to key configuration files or packages with 'canary' (logged no-op) events configured to ensure the service remains operational on all in-scope hosts during runtime c. Deploying a Host Intrusion Detection System such as an open source solution like OSSEC with ElasticSearch and Kibana or using a partner solution. (Note that the following mechanism does not meet this requirement: Frequently cycling Amazon EC2 instances or Containers.)	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service** Not applicable to **Customer-Deployed**	
2.4 All data is classified	AWS Partner must show that all customer data processed and stored in the workload is considered and classified to determine its sensitivity and the appropriate methods to use when handling it.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
2.5 All sensitive data is encrypted	AWS Partner must show that customer data classified as sensitive is encrypted in transit and at rest.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
2.6 All data in transit is encrypted	AWS Parter must show that data in transit across an Amazon VPC boundary is encrypted.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
2.7 Cryptographic keys are managed securely	AWS Partner must show that all cryptographic keys are encrypted at rest and in transit, and access to use the keys is controlled using an AWS solution such as AWS Key Management Service (AWS KMS) or an AWS Partner solution such as HashiCorp Vault.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
2.8 Security incident response	AWS Partner must adhere to the following security procedure: A security incident response process must be defined for handling incidents such as AWS account compromises. This process must be	Applicable to **Multi-tenant SaaS**, **Single-**	

process is defined and rehearsed	tested by implementing procedures to rehearse the incident response process (e.g., by completing a security game day exercise). A rehearsal must have been held within the last 12 months to confirm that: 1. The appropriate people have access to the environment. 2. The appropriate tools are available. 3. The appropriate people know what to do to respond to the various security incidents outlined in the plan.	**tenant SaaS**, and **Managed Service** Not applicable to **Customer-Deployed**	

3.0 Reliability

The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.		**Applicability**	**Met Y/N**
3.1 Network connectivity is highly available	AWS Partner must show that network connectivity to the solution is highly available. If using VPN or AWS Direct Connect to connect to customer networks, the solution must support redundant connections, even if the customers do not always implement this.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service** Not applicable to **Customer-Deployed**	
3.2 Solution is resilient to availability zone disruption	AWS Partner must show that the solution continues to operate in the case where all of the services within a single AZ have been disrupted.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
3.3 Resiliency of the solution has been tested	AWS Partner must show that the resiliency of the infrastructure to disruption of a single AZ has been tested in production (e.g., through a game day exercise) within the last 12 months.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
3.4 DR plan includes recovery to another AWS account	AWS Partner must show that their DR plan includes a strategy for recovering to another AWS account, and periodic recovery testing must test this scenario. AWS Partner must have completed at least one full test of the DR plan, including at least recovery to another AWS account, within the last 12 months. **Supplemental Information**: Although processes restoring data into test environments or exporting data for users are useful ways to verify backups, these processes do not fulfill the requirement to perform a full restore test to another AWS account.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service** Not applicable to **Customer-Deployed**	

4.0 Performance Efficiency			
The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.		**Applicability**	**Met Y/N**
4.1 Infrastructure scaling mechanisms align with business requirements	AWS Partner must show that infrastructure scaling mechanisms align with business requirements, either by: 1. Implementing auto-scaling mechanisms at each layer of the architecture, or 2. Confirming that current business requirements, including cost requirements and anticipated user growth, do not require auto-scaling mechanisms AND manual scaling procedures are fully documented and frequently tested.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	

5.0 Operational Excellence			
The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.		**Applicability**	**Met Y/N**
5.1 Infrastructure provisioning and management is automated	AWS Partner must show that the solution uses an automated tool such as AWS CloudFormation or Terraform to provision and manage the AWS infrastructure. The AWS Console must not be used to make routine changes to the production AWS infrastructure.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
5.2 Deployment of code changes is automated	AWS Partner must show that the solution uses an automated method of deploying code to the AWS infrastructure. Continuous Integration (CI) & Continuous Delivery (CD) practices must be used to deploy updates in the AWS infrastructure. Services such as AWS CodeCommit and AWS CodeBuild are suggested.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
5.3 AWS and Application logs are managed centrally	AWS Partner must show that the application and the AWS infrastructure are monitored centrally with alarms generated and sent to the appropriate operations staff as needed. Services such as Amazon CloudWatch and CloudTrail are suggested.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	
5.4 Runbooks and escalation process are defined	AWS Partner must adhere to the following operational excellence procedure: Runbooks must be developed to define the standard procedures used in response to different application and AWS events. An escalation process must be defined to deal with alerts and alarms generated by the system, and to respond to customer-reported incidents.	Applicable to **Multi-tenant SaaS**, **Single-tenant SaaS**, **Managed Service**, and **Customer-Deployed**	

AWS Resources

AWS Partners can use the following resources to prepare for the checklist self-assessment and validation review.

Title	Description
How to Build a Practice Landing Page	Provides guidance how to build a Practice/solution page that will meet the prerequisites of the Program.
How to write a Public Case Study	Provides guidance how to build a Public Customer Case Study that will meet the prerequisites of the Program.
How to build an Architecture Diagram	Provides guidance how to build architecture diagrams that will meet the prerequisites of the Program.
Partner Readiness Doc	Provides guidance and best practice examples of the Program prerequisites.
AWS Government Website	Provides information on the ways that AWS helps public sector customers pave for innovation and supporting world-changing projects in government, education and nonprofit organizations

AWS reserves the right to make changes to the ATO on AWS Program at any time and has sole discretion over whether AWS Partners qualify for the Program.