ATO on AWS Program

Consulting Partner Validation Checklist

June 2019
Version 1.0

aws partner network

Table of Contents

Introduction

The goal of the Authority to Operate ("ATO") on AWS program is to recognize AWS Partner Network Partners ("APN Partners") who demonstrate technical proficiency and proven customer success in specialized solution areas, namely associated with specific compliance regimes. The ATO on AWS Partner Validation Checklist ("Checklist") is intended for APN Partners who are interested in applying for the program. APN Partners undergo an audit of their capabilities upon applying for the ATO on AWS.

Expectations of Parties

It is expected that APN Partners will review this document in detail before requesting membership in the Program. If items in this document are unclear and require further explanation, please contact your AWS Partner Development Representative (PDR) or AWS Partner Development Manager (PDM) as the first step. Your PDR/PDM will contact the ATO on AWS team if further assistance is required.

The ATO on AWS team will review and aim to respond back with any questions within five (5) business days to initiate scheduling of your audit or to request additional information.

APN Partners should prepare for the audit by reading the Checklist, completing a self-assessment using the Checklist, and gathering and organizing objective evidence to share with the ATO on AWS team.

AWS recommends that APN Partners have individuals who are able to speak in-depth to the requirements. The best practice is for the APN Partner to make the following personnel available to respond to any questions/comments from the ATO on AWS team: one or more highly technical AWS certified engineers/architects and an operations manager who is responsible for the operations and support elements. Please note that this could be the same individual.

ATO on AWS Program Prerequisites

ATO on AWS Partners provide solutions to, or have deep experience working with, organizations to help them implement continuous integration and delivery practices, or automating infrastructure provisioning and management with configuration management tools with the expressed goal of reducing the time for the organization to achieve an ATO on AWS.

The following items will be validated by the ATO on AWS team; missing or incomplete information must be addressed prior to scheduling of the validation review.

1.0 APN Program Requirements		**Met Y/N**
1.1 Program Guidelines **1.2 Consulting Partner Tier**	The APN Partner must read the Program Guidelines and Definitions before applying to the ATO on AWS program. Click here for Program details APN Partner must be a Select Tier or above APN Consulting Partner before applying to the ATO on AWS program.	
1.3 Program Membership	APN Partner must be a member of the Public Sector Partner Program (PSP).	
2.0 ATO on AWS References		**Met Y/N**
2.1 ATO-Specific References	APN Partner must have two (2) ATO on AWS references specific to completed ATO projects; APN Partner must provide the following information for each reference: ▪ Name of the customer ▪ Problem statement/definition ▪ What you proposed ▪ How AWS services were used as part of the solution ▪ Third party applications or solutions used ▪ Start and end dates of project. References must be for projects started within the past 18 months, and must be for projects that are in production, rather than in a “pilot” or proof of concept stage ▪ Outcome(s)/results ▪ Total time to achieve ATO ▪ Total cost of achieving ATO	

3.0 ATO on AWS Practice and Focus		Met Y/N
3.1 ATO on AWS APN Partner Practice	AWS customers are looking for expertise in the development and delivery of solutions on AWS, specifically to reduce the time required to achieve an ATO; an APN Partner's internet presence specific to their AWS practice provides customers with confidence about the APN Partner's capabilities and experience in helping organizations achieve an ATO. APN Partner must have a landing page that describes their AWS practice, AWS solutions and use cases, technology solution, links to AWS Case Studies, and any other relevant information supporting the APN Partner's expertise related to achieving an ATO and highlighting the work on AWS. APN Partner must have a reference architecture for all use cases which is optimized for security, reliability, performance, cost optimization, and operational excellence in keeping with AWS best practices as outlined in the AWS Well Architected Framework.	

4.0 APN Partner Self-Assessment		Met Y/N
4.1 AWS Competency Partner Program Validation Checklist Self-Assessment	APN Partner must conduct a self-assessment of their compliance to the requirements of the ATO on AWS Consulting Partner Validation Checklist. ▪ APN Partner must complete all sections of the checklist. ▪ Completed self-assessment must be emailed to using the following convention for the email subject line: "[APN Partner Name], ATO on AWS Consulting Partner Completed Self-Assessment." ▪ It is recommended that APN Partner has their solutions architect or PDM review the completed self-assessment before submitting to AWS. The purpose of this is to ensure the APN Partner's AWS team is engaged and working to provide recommendations prior to the audit and to help ensure a positive audit experience.	

ATO on AWS Consulting Partner Validation Checklist

In preparation for the validation process, APN 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. APN Partners are not limited to the two (2) references submitted as part of the prerequisite process but should be prepared to describe how the new references meets the minimum acceptable criteria for an ATO on AWS reference if being used during the validation. References that incorporate more than one applicable technology or solution may be submitted under multiple solution categories below.

The ATO on AWS Program is guided by AWS best practices and the Well Architected Framework.

1.0 AWS Practice Overview		Met Y/N
1.1 Customer Presentation	APN Partner has a company overview presentation that sets the stage for customer conversations about their ATO on AWS capabilities and showcases APN Partner's demonstration capabilities. Presentation contains information about the APN Partner's ATO on AWS capabilities, including AWS-specific differentiators, e.g., what is unique about the APN Partner's practice that can only be accomplished leveraging AWS. Overview presentations contain: ▪ Company history ▪ Office locations ▪ Number of employees ▪ Customer profile, including number and size of customers, including industry ▪ Overview of Security Automation & Orchestration philosophy, practices, and tools Evidence must be in the form of a documented presentation.	
1.2 Maintaining AWS Expertise	APN Partner can describe how they stay current on AWS services and tools, particularly as it relates to compliance programs, such as Federal Risk and Authorization Management Program (FedRAMP), US Department of Defense (DoD) IL2/4/5, etc. Evidence must be in the form of a verbal description on enablement materials leveraged by APN Partner to stay current on AWS services and features.	
1.3 Solution Selling	APN Partner can describe how ATO opportunities are identified, how their sellers are trained to identify and sell those opportunities, and specific demand generation/lead generation efforts associated to their ATO on AWS practice. Evidence must be in the form of a verbal or written description how APN Partner engages with customers, their internal sellers, and AWS sellers if applicable.	
1.4 AWS Sales Engagement	APN Partner can describe how and when they engage with AWS sellers and AWS Solutions Architects. Evidence must be in the form of a written description of how and when APN Partner engages AWS sellers or Solutions Architects on an opportunity or in the form of a demonstration of the AWS Opportunity Management tool with sales qualified opportunities submitted (sales qualified = budget, authority, need, timeline, and competition fields completed). The AWS Opportunity Management Tool can be found within APN Partner Central.	
1.5 End of Project Customer Satisfaction Survey	APN Partner asks customer to complete AWS Customer Satisfaction Survey at the end of the project. This is accomplished by searching for the APN Partner in the AWS Partner Solutions Finder and asking Customer to leverage the "Rate this APN Partner" feature.	

2.0 Solution Design		Met Y/N	Notes
2.1 Solution Capabilities	APN Partner demonstrates that during customer engagements, a complete detailed design document is delivered such that customers and APN Partner are both assured that due diligence, capacity planning, architectural review, and long-term operational process have been assessed for the customer engagement. APN Partner must provide detailed design documents for the four (4) submitted AWS Customer References. Design documents contain the following components:		Waived if APN Partner is approved AWS MSP (SSP template shall still be provided as evidence)
	2.1.1 Documentation of customer requirements		
	2.1.2 Assessment of current infrastructure/application environment		
	2.1.3 Architectural details of the proposed design 2.1.4 System Security Plan Template with Control Implementation Statements for the APN Partner's General Support System		

3.0 Security		Met Y/N	Notes
	The security pillar focuses on protecting information and 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.		
3.1 Identity and Access Management	APN Partner has a documented Access Management Strategy and leverages those practices as a key aspect to their ATO on AWS solution for customers, including but not limited to: AWS Identity and Access Management (IAM) users, federated roles, AWS Security Token Service (AWS STS) credentials, access keys, console passwords, and FIPS 140-2 validated multi-factor authentication (MFA) devices. Evidence must be in the form of process documentation that addresses the above requirements.		Waived if APN Partner is approved AWS MSP
3.2 Protection of Root Account Credentials	APN Partner does not administer AWS accounts by use of root account credentials and teaches this to customers. Evidence must be in the form of documentation describing this as a best practice.		Waived if APN Partner is approved AWS MSP
3.3 Least Privilege Principle	APN Partner has a system that provides access to customer resources to its engineers based on the principle of least privilege and makes this a key component of customer security best practices. Customers have a process for defining and maintaining the appropriate level of access is in place. Access to critical or sensitive data (as defined by the customer) is further controlled by multi-factor or quorum authentication with access-based alerts. Evidence must be in the form of process documentation for maintaining least privilege access policies.		Waived if APN Partner is approved AWS MSP
3.4 Multi-Factor Authentication	APN Partner ensures that FIPS 140-2 validated multi-factor authentication is activated on all APN Partner and customer AWS root accounts and that this is taught to customers as part of the AWS Security Automation & Orchestration (SAO) methodologies. Evidence must be provided showing of the use of technology for regular auditing of accounts for MFA activation (e.g., using AWS Trusted Advisor) and must show policies and process for activation of MFA on new AWS root accounts.		Waived if APN Partner is approved AWS MSP
3.5 Communication of Security Best Practices	APN Partner ensures customers understand AWS security processes and technologies as outlined in https://aws.amazon.com/whitepapers/aws-security- best-practices/ Evidence must be in the form of onboarding and governance documents provided to customers that specifically cover customer security considerations in the APN Partner's environment.		Waived if APN Partner is approved AWS MSP
3.6 Protection of Customer Systems from Attacks	APN Partner has security policies and procedures to protect its customers' systems from attacks. Evidence must be in the form of security policies and procedures.		Waived if APN Partner is approved AWS MSP

3.7 SOC implementation and Incident Response	APN Partner can advise on the design, implementation, and enablement of a SOC. APN Partner provides customers the ability to detect, respond, forensically investigate, and remediate/recover from incidents. APN Partner must have the ability to analyze AWS telemetry including AWS CloudTrail, Amazon GuardDuty findings, AWS WAF logs, Amazon Simple Storage Service (Amazon S3) access logs, Amazon Virtual Private Cloud (Amazon VPC) flow logs, as well as OS and Application logs. APN Partner must have the ability to integrate these into security workflows, alerts, and logs into a centralized SIEM and ticketing system. Evidence must be provided in the form of standard IR playbooks and demonstration of automated response plan.	Waived if APN Partner is approved AWS MSP, or not providing managed services.
3.8 Application and Operating System Hardening	APN Partner can provide industry best practices for hardening and configuring applications and operating systems to industry standards or vendor best practices. As an example, this may be to CIS standards or mandating that an application is only using FIPS-certified software libraries. Evidence must be in the form of automated scripts and/or documentation that includes the processes and steps taken to achieve the hardening.	Waived if APN Partner has Government Competency
3.9 Encryption at Rest and in-transit	APN Partner uses best practices to encrypt all sensitive information at-rest, and in-transit including personally identifiable information (PII). For example, at rest encryption using native AWS encryption capabilities, such as server-side encryption with AWS managed keys or AWS KMS. In-transit using secure protocols such as HTTPS, IPsec, and SFTP. Evidence must be in the form of documentation such as a design document.	Waived if APN Partner has Government Competency
3.10 Detective Controls	Activity is monitored appropriately, including by maintenance of logs for capturing performance and security event data, e.g., Amazon CloudWatch logs, events, GuardDuty, CloudTrail, VPC flow logs, ELB logs, S3 bucket logs, etc. Evidence must be in the form of an example of logs maintained, including demonstration that logs are retained per customer-agreed retention periods.	Waived if APN Partner has Government Competency
3.11 Configuration Drift	APN Partner has built mechanisms either for self or customer to detect configuration drift of the environment. Documentation should include capabilities to monitor, alert, and remediate where applicable when there is configuration drift. Evidence must be provided in the form of templates and scripts to show identification and remediation steps associated with configuration drift.	Waived if APN Partner has Government Competency

4.0 Reliability		Met Y/N	Notes
4.1 Service Availability	APN Partner has process to determine service availability needs for customers. See AWS Reliability Pillar whitepaper for specific considerations and guidance on how to calculate service availability with downstream dependencies.		Waived if APN Partner is approved AWS MSP
4.2 Application Availability	Evidence must be in the form of verbal description and/or process documentation. APN Partner designs applications according to customer needs, factoring in cost of building/maintaining that application to the desired availability levels.		Waived if APN Partner is approved AWS MSP
4.3 Monitoring Systems	Evidence must be in the form of verbal description and/or APN partner documentation leveraged in design process. APN Partner has introduced or modernized a monitoring system that supports software-defined infrastructure and is integrated with deployment and build mechanisms. Monitoring system should also introduce success criteria measurement. Evidence must be in the form of a customer implementation, such as design documentation for monitoring.		Waived if APN Partner is approved AWS MSP
4.4 Automation and Infrastructure as Code	APN Partner has demonstrated competency in the following areas: • Leveraging infrastructure-as-code tools such as AWS CloudFormation to automate the deployment of AWS services • Building and running continuous integration and continuous deployment pipelines in AWS. • Security Automation & Orchestration Framework Evidence must be in the form of a customer implementation, such as AWS CloudFormation Templates, architecture diagram for CI/CD pipeline.		Not eligible for waiver

5.0 Performance Efficiency

For this section, APN Partner must select two (2) of the four (4) submitted customer references and discuss performance efficiency considerations for both examples. ***Waived if Partner has AWS Government Competency***			
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.			
Customer Case Studies for Performance Efficiency Considerations		**[Insert Link or Title of Case Study #1 Here]**	**[Insert Link or Title of Case Study #2 Here]**
Selection			
5.1 Compute	APN Partner to describe considerations for how they select the right AWS compute options specifically outlining choice of instances, containers, services and functions. Evidence must be provided in the form of verbal description as it relates to two (2) of the four (4) submitted customer case studies.		
5.2 Storage	APN Partner to describe considerations for how they select the right AWS Storage options specifically outlining access method, pattern of access, throughput required, frequency of access, frequency of update, and availability and durability constraints. Evidence must be provided in the form of verbal description as it relates to two (2) of the four (4) submitted customer case studies.		
5.3 Database	APN Partner to describe considerations for how they select the right AWS database options specifically outlining requirements for availability, consistency, partition tolerance, latency, durability, scalability, and query capability. Evidence must be provided in the form of verbal description as it relates to two (2) of the four (4) submitted customer case studies.		
5.4 Network	APN Partner to describe considerations for how they select the right Network options specifically outlining latency, throughput requirements, and location. Evidence must be provided in the form of verbal description as it relates to two (2) of the four (4) submitted customer case studies.		
Performance Monitoring and Review			
5.5 Performance Monitoring	APN Partner introduced, setup and configured a solution to monitoring the environment with automated alerts and remediation. Evidence must be provided in the form of design documents.		

6.0 Operational Excellence		Met Y/N	Notes
6.1 Deployment Checklist	APN Partner uses consistent processes (e.g., checklists) to know when ready to go live with a workload. Evidence must be in the form of completed checklists.		Waived if APN Partner is approved AWS MSP
6.2 Runbooks/ Playbooks	APN Partner uses runbooks that document routine activities and playbooks that guide the issue resolution process. Evidence must be in the form of runbooks/playbooks for relevant components of compliant solutions.		
6.3 Automation through Scripting	APN Partner leverages scripting and tagging to automate execution of runbooks if/where applicable. Evidence must be in the form of script library/demonstration.		

6.4 Configuration Management	APN Partner has process to automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems. If EC2 Systems manager is not leveraged, APN Partner can show documented processes or provide technical demonstration for how configurations and infrastructure updates are managed, and the methods used to automate these functions. Evidence must be in the form of technology demonstration or documentation provided to the customer.		

7.0 Cost Optimization		Met Y/N	Notes
7.1 Service and Pricing Models	APN Partner considers cost when selecting AWS services, including optimizing by using the most appropriate services and by selecting the appropriate pricing models to meet cost targets, including by the use of Reserved Instances and Spot Instances and by factoring costs into Region selections. Evidence must be in the form of a description of how AWS services and price models are selected for cost optimization.		Waived if APN Partner is approved AWS MSP
7.2 Cost Management	APN Partner has a methodology to ▪ Review metrics and provide recommendations to optimize cost. ▪ Set up AWS environment to support charge backs in a decentralized IT environment. ▪ Accept pre-payments or implement spending caps within a comprehensive billing system Evidence must be in the form of a customer implementation using AWS native tools and/or third party tools.		Waived if APN Partner is approved AWS MSP

8.0 Compliance		**Met Y/N**	Notes
8.1 Controls Mapping	APN Partner has established a standard method for mapping solutions to regulatory standards, such as National Institutes of Standards and Technology (NIST) 800-53, DoD Security Requirements Guide (SRG), Health Insurance Portability and Accountability Act (HIPAA), Center for Internet Security (CIS), etc. to ensure customer solutions adhere to their regulatory requirements. Evidence must be in the form of a controls mapping and/or policy document.		Not eligible for waiver
8.2 Compliant Architecture	APN Partner has developed reference architectures that adhere to the compliance standards, such as NIST 800-53, DoD SRG, HIPAA, CIS, etc. Evidence must be in the form of a customer implementation or reference architecture developed by the APN Partner.		Not eligible for waiver
8.3 General Support System (GSS)	APN Partner has developed a General Support System (GSS) that adheres to the compliance standards, such as NIST 800-53, DoD SRG, HIPAA, CIS, etc. Evidence must be in the form of a customer implementation or reference architecture developed by the APN Partner.		Not eligible for waiver
8.3 System Security Plan (SSP)	APN Partner has developed a System Security Plan (SSP) that adheres to the appropriate compliance standards, such as NIST 800-53, DoD SRG, etc., which includes control implementation statements for their General Support System (GSS), inclusive of 3rd party tools. Evidence must be in the form of a System Security Plan developed by the APN Partner.		Not eligible for waiver

9.0 Compliance Designations			Met Y/N	Notes
Partner must meet all of the criteria in at least one of the below sections to qualify for that compliance designation. Final determinations as to whether criteria are satisfied rest solely with AWS.				
FedRAMP	Solutions that allow customers to address their compliance needs in accordance with the FedRAMP PMO and NIST 800-53.	• ≥ 2 qualifying references specific to either FedRAMP LI-SaaS, FedRAMP Moderate or FedRAMP High workloads • APN partner has developed approach and guidance on secure mechanisms to deploy technology infrastructure in compliance with NIST 800-53		
Federal Information Security Management Act (FISMA)	Solutions that allow customers to address their compliance needs in accordance with FISMA and NIST 800-53.	• ≥ 2 qualifying references specific to FISMA workloads • APN partner has developed approach and guidance on secure mechanisms to deploy technology infrastructure in compliance with NIST 800-53		

DoD SRG	Solutions that allow customers to address their compliance needs in accordance with the DoD Security Requirements Guide (DoD SRG)	• ≥ 2 qualifying references specific to DoD SRG workloads (IL2/4/5) • APN partner has developed approach and guidance on secure mechanisms to deploy technology infrastructure in compliance with NIST 800-53		
HIPAA	Solutions that allow customers to address compliance needs in accordance with the Health Insurance Portability Accountability Act (HIPAA)	• ≥ 2 qualifying references specific to HIPAA workloads • APN partner has developed approach and guidance on secure mechanisms to deploy technology infrastructure in compliance with HIPAA or workloads referencing GxP (GCP, GMP, GLP) best practices		
IRS 1075	Solutions that allow customers to address compliance needs in accordance with IRS Publication 1075 requirements associated with Federal Tax Information (FTI).	• ≥ 2 qualifying references specific to Federal Tax Information (FTI) workloads • APN partner has developed approach and guidance on secure mechanisms to deploy technology infrastructure in compliance with IRS Publication 1075		
CJIS	Solutions that allow cusomters to address compliance needs in accordance with the Criminal Justice Information Services (CJIS) Policy Areas.	• ≥ 2 qualifying references specific to CJIS workloads • APN partner has developed approach and guidance on secure mechanisms to deploy technology infrastructure in compliance with CJIS requirements		
IRAP	Solutions that allow customers to address compliance needs of the Information Security Registered Assessors Program (IRAP) to comply with the Australian Government Information Security Manual (ISM).	• ≥ 2 qualifying references specific to IRAP/ISM workloads • APN Partner has developed approach and guidance on secure mechanisms to deploy technology infrastructure in compliance with IRAP/ISM requirements		
GDPR	Solutions that allow customers to address compliance needs of the European Union's General Data Protection Regulation (GDPR).	• ≥ 2 qualifying references specific to GDPR workloads • APN Partner has developed approach and guidance on secure mechanisms to deploy technology infrastructure in compliance with IRAP/ISM requirementsor programs		
PCI DSS	Solutions that allow customers to address compliance needs of the Payment Card Industry Data Security Standard (PCI DSS).	• ≥ 2 qualifying references specific to PCI DSS workloads • APN Partner has developed approach and guidance on secure mechanisms to deploy technology infrastructure in compliance with IRAP/ISM requirementsor programs		

AWS Resources

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 an architecture diagrams that will meet the prerequisites of the Program.
Partner Readiness Doc	Provides guidance and best practice examples of the Program perquisites.
AWS Government Website	Paving the way 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 APN Partners qualify for the Program.