AWS Government Competency
Technology Partner Validation Checklist

March 2018
Version 2.0

Table of Contents

Introduction

The Competency Partner Validation Checklist is intended for APN Partners who are interested in applying for AWS Competency. This checklist provides the criteria necessary to achieve the designation under the AWS Competency Program.

The goal of the AWS Competency Program is to recognize APN Partners who demonstrate technical proficiency and proven customer success in specialized solution areas.

APN Partners undergo a validation of their capabilities upon applying for the specific Competency, and every 12 months thereafter. AWS leverages in-house expertise to facilitate the review.

AWS reserves the right to make changes to this document at any time. **It is expected that APN Partners will review this document in detail *before* submitting a Competency application, even if all of the pre-requisites are met.** If items in this document are unclear and require further explanation, please contact your AWS Partner Development Representative (PDR) or Partner Development Manager (PDM) as the first step. Your PDR/PDM will contact the Competency Program Team if further assistance is required.

Competency Application and Audit Process

In order to begin the validation process, please follow the steps outlined below:

- Step #1: Review the Partner Validation Checklist
- Step #2: Submit a Competency Application through the APN Portal
  - Login to the APN Portal
  - Click “View My APN Account” in left navigation
  - Scroll to AWS Competencies and select the appropriate Competency
  - Complete the Competency Application

Incomplete applications will not be considered and will be rejected.

Once your firm’s application has been submitted through the APN Portal, the APN Team will review for compliance.

AWS recommends that APN Partners have individuals who are able to provide evidence of compliance and to speak in-depth to the requirements available during the validation process.

Upon completion of the review, a recommendation is given to the APN Team regarding APN Partner acceptance into the Competency. The final decision regarding acceptance is made by the APN Team; APN Partners will be notified of their status by AWS.

Program Policies

An APN Partner's application to the Competency may be rejected at the discretion of the Global Segment Business or Technical Lead. Rejections may be made due to estimated ability to consistently implement technical solutions, lack of current required APN Partner certifications, judgment of the technical or business merit of the proposed solution, perceived lack of solution delivery capabilities, or any other business or technical criteria deemed critical.

Competency status can be revoked at the discretion of the Global Segment Business or Technical Lead. Revocations may be issued due to loss of required APN Partner certifications, lack of progress toward billing or win goals, repeated violations of AWS PR guidelines, evidence of poor customer experience, including cost vectors, when using the solution, or any other business/technical factors that would indicate that the practice or solution may not meet current requirements, or is projected not to meet future requirements.

Competency status must be renewed annually on a calendar year basis. Requirements for renewal may change from year to year, subject to the business and technical needs of AWS and its customers.

AWS Government Competency Program Prerequisites

AWS Government Competency Partners provide solutions to—and/or have deep experience working with—government customers to deliver mission-critical workloads and applications on AWS. Partners must meet the minimum requirements in the table below to be considered for Government Competency review. Note that the minimum program requirements are subject to change at any time, at AWS's discretion.

Vertical AWS Competencies are designed for APN Partners with segment-specific solutions and practices on AWS. These are specialized APN Partners with extensive expertise and experience focused on a specific market segment. APN Partners with highly targeted solutions to industry-specific challenges and consulting practices that offer a unique segment domain knowledge are best positioned to pursue Vertical AWS Competencies. This especially applies to heavily regulated vertical segments, such as Healthcare, Financial Services, and Government where solutions must be specifically tailored for compliance, security, and governance regulations.

AWS Government Competency – Technology Partner Prerequisites	
APN Membership	APN Partner must be Advanced or Premier APN Technology Partner (view requirements)
AWS Programs	APN Partner must be a member of the AWS Public Sector Partner (PSP) Program.
AWS Support	APN Partner must have Business level+ Support plan (view Support plans)
AWS Customer References	APN Partner must provide at least 4 AWS customer references specific to completed or ongoing Government projects: ▪ ***Recommended***: Partners submit public AWS Customer References (i.e., case study, whitepaper, blog post, etc.) ▪ References must be for projects completed within the past 18 months, or currently ongoing, and must be for projects that are in production, rather than in pilot or proof of concept stage.
AWS Government Product or Solution	APN Partner must have a landing page that describes their AWS Government product or solution, Government Competency use cases, technology partnerships, links to AWS customer references or case studies, compliance with region-specific Government requirements, and any other relevant information supporting the Partner's expertise related to Government and highlighting the partnership with AWS. Government practice page must be accessible from APN Partner home page.

AWS Government Technology Partner Validation Checklist

In preparation for the validation process, APN Partners should become familiar with the requirements of this checklist. Supporting documentation (e.g., design and architectural documents) related to Partner solution(s) for the submitted customer references must be provided, in order to demonstrate compliance to the below requirements. If any of the below requirements are not applicable to the APN Partner solution(s), APN Partner must specify with written documentation as to why it is not covered by the APN Partner solution.

1.0 AWS Customer References		Met	Not Met
1.1 Customer References	APN Partner has four (4) government customer references for completed or ongoing projects that rely on AWS services, where the majority of work has been completed and is running continuously. We recommend that these be publicly referenceable; this is not required, however. APN Partner must provide 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 ▪ Outcome(s)/results ▪ Lessons learned If APN Partner has provided public references, the publicly available case studies, whitepapers, blog posts or equivalent must include reference to the customer name, Partner Name, and AWS.		

2.0 Solution Details		Met	Not Met
2.1 Solution Capabilities	2.1.1 Documentation showing that the partner has addressed government procurement strategy.		
	2.1.2 Well defined support options, expected service levels and disaster recovery targets. Service levels must be clearly defined and publicly available.		
	2.1.3 Solution performance, capacity and/or availability claims made for the solutions.		
	2.1.4 Detailed design demonstrating that the architecture allows for governance and risk management at scale as per the AWS Security at Scale whitepaper and the AWS Risk and Compliance whitepaper.		

3.0 Solution Architecture		Met	Not Met
3.1 AWS Architecture Best Practices	3.1.1 A Solution must follow the best practices defined in the AWS Well Architected Framework whitepaper. A SaaS or Hosted solution must complete a Well Architected review with AWS personnel. A plan of action for improvements must be in place for all open issues. If open critical issues exist with which the solution cannot comply, an explanation should be provided. It is strongly recommended that no open critical issues exist. A software solution, deployed in customer environments, must enable the customer to follow best practices outlined in the Well Architected Framework.		

	3.1.2 A solution must follow guidance provided in the AWS Security Best Practices whitepaper. A SaaS or Hosted solution must follow AWS Security Best Practices. A software solution deployed in customer environments must enable the customer to follow AWS Security Best Practices.		
3.2 Architecture Documentation	3.2.1 A VPC architecture diagram must be provided for all solutions using VPC. This diagram must include regions, availability zones, subnets, Amazon EC2 instances and leveraged AWS services or components such as Elastic Load Balancers and Virtual Private Gateways.		
	3.2.2 A high-level data flow diagram must be provided for all solutions. This diagram should include all AWS services in use by the solution. For hybrid solutions, data flows crossing the boundary between AWS and other resources should be documented.		
	3.2.3 The partner must submit evidence that supports service level and recoverability claim(s) of the solutions. Evidence should define how claim(s) are met in the architecture and demonstrate ongoing assessment of these claims for historical service level performance. Note: A solution should be designed to be highly available under most use-case scenarios.		
	3.2.4 SaaS and Hosted solutions must submit evidence that supports data durability claims. Evidence should define how claim(s) are met in the architecture.		
	3.2.5 The solution design document should include each AWS service used and an explanation of how it supports a solution requirement.		

4.0 Solution Security		Met	Not Met
4.1 Security Management	4.1.1 Code security management systems and practices must be in place. This can include integration of source code analysis tools, security testing frameworks, or other mechanisms that allow for seamless threat analysis in development and deployment pipelines. A process for evaluation of security impact prior to the release of new code and release approval must be in place.		
	4.1.2 An automated or manual process must be in place to review audit logs from both infrastructure and application to monitor for unauthorized events.		
	4.1.3 The solution documentation must include an incident response plan that outlines how the partner will identify and respond to security incidents in the environment. This plan must also include customer notification process(s) and requirements for all security concerns and incidents.		
4.2 Compliance	4.2.1 Solutions should account for all customer compliance requirements and such requirements must be documented. All compliance claims must be supported with evidence of a completed compliance process, such as an authorization to operate. Third party validation of compliance claims is strongly preferred. For example, a government certification such as FedRAMP or customer references showing that the solution has been certified under a government compliance program. AWS recommends that the Security AWS Foundations benchmark by the Center for Internet Security be evaluated for this requirement if no other compliance claims can be made and/or supported.		

4.3 Foundational Requirements	The below foundational security requirements are required for any SaaS or Hosted solution providers where the partner is responsible for operation of the AWS environment. Software solutions that run in customer operated environments must not interfere with customer's ability to complete these configurations.		
	4.3.1 Restrict use of the root account and protect the root account with multi factor authentication. Hardware MFA preferred. The root account must only be used for root-only activities such as configuring MFA Delete on Amazon S3 buckets, managing Amazon CloudFront signing keys or configuring support level. Billing and cost management should be done with a limited AWS Identity and Access Management (IAM) account and use of the root account for this purpose does not meet this requirement.		
	4.3.2 Audit for unauthorized changes on at least a weekly basis. Ongoing audits with automated alerts such as using AWS CloudTrail and Amazon CloudWatch Logs are preferred. Audits should include checks for • Unauthorized changes to AWS IAM users and AWS IAM Policy • Unauthorized changes to auditing (AWS CloudTrail, AWS Config, etc.) • Unauthorized resource creation		
	4.3.3 Monitor for resource compliance and possible compromise.		
	4.3.4 Passwords and API access keys must be rotated regularly. Storing credentials in plain text should be avoided and credentials must not be hard-coded into the application. AWS IAM Roles should be used when possible.		
	4.3.5 Privileged user accounts must implement MFA protection. Privileged accounts should include any accounts with the ability to destroy customer data or affect audit logging and monitoring processes.		
	4.3.6 IAM users must be for individual users only. Delegated access or shared accounts must be implemented using AWS IAM Roles.		