AWS Healthcare Competency

Technology Partner Validation Checklist

February 2018
Version 2.1

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 Healthcare Competency Program Prerequisites

AWS Healthcare Competency Partners have demonstrated success in building solutions for healthcare payers and providers that securely store, process, transmit, and analyze clinical information. Working with these Competency Partners gives you access to innovative, cloud-based solutions that have a proven track record handling clinical data.

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 Healthcare Competency – Technology Partner Prerequisites	
APN Membership	APN Partner must meet Advanced tier+ APN Technology Partner (view requirements)
AWS Support	APN Partner must have Business level+ Support plan (view Support plans)
AWS Customer References	APN Partner must provide ≥ 4 AWS customer references specific to completed Healthcare projects: ▪ 2 of the 4 AWS customer references must be public (i.e., documented in a case study, white paper, or blog post). Public references must mention AWS, the end customer, and the APN Partner. ▪ References must be for projects started within the past 12 months, and must be for projects that are in production, rather than in pilot or proof of concept stage. ▪ All customer references submitted must have supporting documentation providing evidence of compliance to the requirements of this checklist.
AWS Healthcare Product or Solution	APN Partner must have a Healthcare product or solution on AWS, including: ▪ Availability of product or solution in 2 or more AWS regions ▪ Qualifying for and posting an AWS public support statement on APN Partner's website detailing the APN Partner's Healthcare practice on AWS and including public reference to the APN Partner's solution, practice, or guidance on Healthcare. For example, an acceptable public support statement is a landing page on the APN Partner's website that contains various elements, including the AWS solutions and competency use cases, reference architecture, technology partnerships, customer references, sample TCO pricing, and any other relevant information supporting the APN Partner's expertise related to Healthcare and highlighting the partnership with AWS through the APN. ▪ A reference architecture for a Healthcare use case which is optimized for security, reliability, performance, cost optimization, and operational excellence.
AWS Certifications/Training	In addition to the certification/training requirements for tier compliance, APN Partner must have: • At least 4 staff who have completed Healthcare Compliance Training

AWS Healthcare 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) AWS customer references of completed Healthcare projects. 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		
1.2 Public References	2 of the above 4 references are publicly endorsed by the customer. Evidence must be in the form of a publicly available case study, white paper, blog post, or equivalent that includes, as a minimum: ▪ Reference to customer name, APN Partner name, and AWS ▪ Customer problem that was solved ▪ How AWS was used as part of the solution ▪ Outcome(s)/results Public references must be easily discoverable on the APN Partner's website.		

2.0 Solution Details		Met	Not Met
2.1 Solution Capabilities	For each Healthcare solution considered for the competency, APN Partner submits a detailed design document that contains the following components:		
	2.1.1 Documentation of solution requirements		
	2.1.2 Architectural details of proposed design		
	2.1.3 Details of the system performance, capacity management, and availability measurement systems to measure success of solution		
	2.1.4 Description of security policies and procedures		
	2.1.5 Detailed design shows that solution is architected as per AWS security best practices as outlined as per AWS Security Best Practices		
	2.1.6 Detailed design shows that the proposed design allows for governance and risk management at scale as per AWS Security at Scale and AWS Risk and Compliance		
2.2 AWS Best Practices	APN Partner solution is aligned with AWS architecture best practices and reference architectures. The detailed design document from section 2.1 should include an architectural overview that provides the following details: Infrastructure architecture reliably utilizes services such as Multi-AZ Auto Scaling, Amazon Virtual Private Cloud (Amazon VPC), Elastic Load Balancing, and Multi-AZ Amazon Relational Database Service (Amazon RDS) to provide highly available and reliable infrastructure.		
2.3 Architectural Review	APN Partner solution has undergone an architectural review to ensure alignment to the AWS Well-Architected Framework or AWS Marketplace Best Practices.		

3.0 Security		Met	Not Met
3.1 Security Best Practices	APN Partner has documentation that proves that the solution is aligned as per AWS Security Best Practices and AWS Risk and Compliance.		
3.2 Security Control	APN Partner product or solution has the appropriate security controls: ▪ For SaaS solutions, the solution does not in any form or control ask customer to provide their AWS credentials. All access controls are implemented via Cross Account roles. ▪ For product being deployed by the customer, product has features to manage access to AWS resources and APIs using identity federation and IAM roles.		
3.3 Logging	APN Partner has introduced systems for log management across their entire application, specifically including integration with AWS CloudTrail and Amazon CloudWatch, or third party equivalent.		
3.4 Configuration Change Management	APN Partner has introduced systems for configuration change management using AWS Config, or third-party equivalent.		
3.5 Identity and Access Management	APN Partner has introduced best practices for identity and access management including least privilege and using IAM roles over IAM users whenever possible		
3.6 Data Security	APN Partner encrypts all sensitive data at-rest and in-transit.		
3.7 Operating System Security	APN Partner has introduced practices to ensure applications run on top of hardened Amazon Machine Images		
3.8 Security Management	3.8.1 APN Partner has introduced or modernized a code security management system. This can include integration into source code analysis tools, security testing frameworks or other mechanisms that allow for seamless threat analysis in development and deployment pipelines.		
	3.8.2 APN Partner has introduced or modernized an infrastructure security management system that specifically scans and audits appropriate accounts and infrastructure for AWS security and architecture best practices.		

4.0 Reliability and Operational Excellence		Met	Not Met
4.1 Configuration and Code Management	APN Partner has introduced or modernized design that supports automated deployment and infrastructure management on AWS.		
4.2 Design Patterns for Reuse	APN Partner has introduced design patterns that enable them to consistently deploy best practices building blocks like Amazon VPCs and Web App stacks.		
4.3 Ephemeral Infrastructure Design Patterns	APN Partner has introduced the concept of disposable and ephemeral infrastructure as part of designing for failure principles.		
4.4 Monitoring Systems	APN Partner has introduced or modernized a monitoring system that supports disposable infrastructure and is integrated with deployment and build mechanisms. Monitoring system should also introduce and measure success criteria measurement.		
4.5 Software Development Practices	APN Partner has demonstrated use of proper software development practices, including code versioning, continuous integration and continuous delivery.		
4.6 Automation	Where appropriate, APN Partner has automated common operations with code, including but not limited to, change management, configuration management, and responses to events.		
4.7 Resiliency and Disaster Recovery	APN Partner has implemented appropriate strategies for resiliency and disaster recovery with the appropriate Recovery Time Objective (RTO) and Recovery Point Objective (RPO).		

5.0 Performance Efficiency and Cost Optimization		Met	Not Met
5.1 Resource Provisioning	5.1.1 APN Partner has evaluated and chosen the appropriate compute option (instances, containers, functions) for each portion of their application.		
	5.1.2 APN Partner has architected for scalability and elasticity using Auto Scaling.		
5.2 Storage Optimization	APN Partner has optimized their Amazon S3 and Amazon EBS storage tiers for both cost and performance.		

6.0 Healthcare Compliance		Met	Not Met
6.1 HIPAA	6.1.1 APN Partner can provide documentation as to why their application does or does not fall under the HIPAA security, privacy or breach notification rules. Evidence must be in the form of a customer implementation description.		
	6.1.2 APN Partner can demonstrate knowledge of the current AWS Business Associate Agreement (BAA) by providing the following: ▪ Description of the BAA ▪ Examples of customer solutions leveraging or not leveraging the BAA and the technical safeguards that are put into place to meet BAA requirements ▪ If not current solution requires a BAA by an active customer, APN Partner must provide a hypothetical use case when it would be appropriate to sign a BAA with AWS as well as what steps they would take to ensure the BAA is met		
	6.1.3 If APN Partner does have a signed BAA with Amazon and they maintain Protected Health Information (PHI) for customers, they must provide the SANS top 20 critical controls that are used in their solution and specify the AWS implementation of the controls. See Appendix A. Evidence will be requested.		
6.2 HITRUST	APN Partner can provide documentation as to why their application does or does not fall under the HITRUST Cybersecurity Framework regulations. Evidence will be requested.		
6.3 FTC	APN Partner can provide documentation as to why their application does or does not fall under the FTC Personal Health Record (PHR) regulations. Evidence will be requested.		
6.4 FDA Medical Device	APN Partner can provide documentation as to why their application does or does not fall under FDA medical device compliance requirements. Evidence will be requested.		

Appendix A. Index of Critical Controls

Inventory of Authorized and Unauthorized devices Critical
Inventory of Authorized and Unauthorized Software
Secure Configurations for hardware and software on mobile devices, laptops, workstations, and servers
Continuous Vulnerability Assessment and Remediation
Controlled Use of Administrative Privileges
Maintenance, Monitoring, and Analysis of Audit Logs
Email and Web Browser Protections
Malware Defenses
Limitation and Control of Network Ports, Protocols, and Services
Data Recovery Capability
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Boundary Defense
Data Protection
Controlled Access Based on the Need to Know
Wireless Access Control
Account Monitoring and Control
Security Skills Assessment and Appropriate Training to Fill Gaps
Application Software Security
Incident Response and Management
Penetration Tests and Red Team Exercises

http://www.sans.org/critical-security-controls