



AWS Financial Services Competency Technology Partner Validation Checklist

May 2018
Version 2.2

Table of Contents

Introduction	3
Competency Application and Audit Process	3
Program Policies	3
Definitions	4
AWS Financial Services Technology Competency Categories	6
AWS Financial Services Competency Program Prerequisites	7
<i>1.0 AWS Case Studies</i>	<i>9</i>
<i>2.0 Technology Components</i>	<i>9</i>
<i>3.0 Security</i>	<i>9</i>

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 12-24 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 or every 24 months 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.

Definitions

APN Partner Solution

AWS Competencies are granted to APN Partners offering a specific solution or product that aligns to business and technical criteria outlined in this Validation Checklist.

AWS Case Studies

All APN Partners will need to provide a number of AWS Case Studies detailing completed deployments of the Partner Solution. An AWS Case Study is a written description of a completed customer project that includes individual customer solutions and outcomes. Case Studies should include an introduction to the customer, overview of the challenge, details about the solution implemented, AWS services and additional 3rd Party tools leveraged, date delivered, and outcomes realized by the customer.

AWS Case Studies should be identified in writing to AWS as being either *public* (can be shared with public audiences) or *non-public* (can only be shared with AWS and its third-party auditor for the purpose of the audit or demonstrating to AWS that APN Partner meets program requirements). Once approved for an AWS Competency, *public* AWS Case Studies will be used on the AWS website to showcase partner-customer success.

AWS Business Requirements Validation

All APN Partners will undergo an AWS Business Requirements Validation in order to achieve an AWS Competency. Business Requirements Validations are an assessment that the APN Partner meets the non-technical requirements for the Competency, including the requirements for APN Tier standing, minimum numbers of suitable public and private AWS Case Studies, an AWS-specific landing page, and active engagement in thought leadership activities.

AWS Technical Validation

All APN Partners will undergo an AWS Technical Validation in order to achieve an AWS Competency. Technical Validations are assessments of an APN Partner Solution in the context of specific AWS Case Studies. Technical Validations confirm the APN Partner's capabilities in developing and delivering customer solutions using AWS Services specific to a solution area, workload, or vertical market while conforming with the AWS best-practices described in the AWS Well-Architected Framework. APN Partners demonstrate to 3rd-party Auditors and/or AWS Partner Solutions Architects what they've done specific to the AWS Case Studies submitted for the Competency.

Requirements for Technical Validations are fully documented in the competency-specific Technical Validation Checklist below. Each Technical Validation is comprised of three elements:

1. **Documentation Review:** APN Partners will be expected to provide technical documentation detailing the Partner Solution and each AWS Case Study provided. Third-party Auditors and/or AWS Partner Solutions Architects will use the documentation to confirm alignment with the requirements of the Competency as described in the checklist.

The documentation is expected to consist of both public information (e.g. on- or offline deployment guides, installation manuals) and non-public information (e.g. architecture diagrams, design documents, and security assessments.) Public information will be assessed for alignment with best practices and the use of APN-approved marketing language. Non-public information may be anonymized at the APN Partner's discretion.

2. **Architecture Baseline Review:** APN Partners who configure or operate an AWS environment as part of the Partner Solution or AWS Case Study will undergo a competency-specific AWS Architecture Baseline Review of that environment. Requirements are based on the tenets of the AWS Well-Architected program and detailed in the checklist.
3. **Competency- and category-specific technical requirements:** Each Competency and category highlights a specific type of solution that addresses a particular class of customer problems. As such, the checklist may include competency-specific requirements highlighting specific methodologies and capabilities the solution must provide to customer. Please see the checklist for more information.

Elements of the APN Partner Solution or AWS Case Study that don't meet the requirements will be identified as 'Critical findings'. All Critical findings identified during the review will need to be remediated prior to achieving the Competency. If Critical findings relating to a specific AWS Case Study are unable to be remediated, the Case Study may be removed from consideration for inclusion in the competency.

AWS Financial Services Technology Competency Categories

AWS Financial Services Competency Partners have readily delivered effective solutions that help organizations manage through critical issues pertaining to the industry, such as risk management, core systems implementations, and data management.

APN Partner must select a distinct Financial Services category based on the AWS-provided category definitions below. Please note that an APN Partner may not apply for more than one category.

Category	Characteristics
Risk Management	<p>Solutions that are helping financial institutions identify, model, and assess risk, ensure monitoring and compliance with the industry regulations, or help in surveillance or fraud monitoring. Examples include companies in the market risk, credit risk, regulatory risk, compliance risk, fraud & cybersecurity, and operational risk.</p> <p>Technology that provides financial institutions:</p> <ul style="list-style-type: none"> ▪ Identification, modeling, and risk assessment ▪ Monitoring and compliance for industry regulation adherence ▪ Surveillance or fraud monitoring
Core Systems	<p>Transaction processing systems for banking/mortgage/payments, capital markets/brokerage/asset management, or the property & casualty insurance industry. Examples include core banking systems, core trading systems, core insurance systems, trade processing systems, and reconciliation systems.</p> <p>Technology that performs:</p> <ul style="list-style-type: none"> ▪ Transaction processing for a product used in retail banking, capital markets, asset management, or the insurance industry ▪ Transaction processing related to core banking systems, core insurance systems, core trading systems, trade processing systems, and reconciliation systems
Data Management	<p>Platforms providing market and reference data or data processing, pricing or financial analytics solutions.</p> <p>Technology that provides a platform for:</p> <ul style="list-style-type: none"> ▪ Market and reference data ▪ Financial data processing ▪ Price quoting ▪ Financial analytics solutions

AWS Financial Services Competency Program Prerequisites

Vertical AWS Competencies are designed for APN Partners with segment-specific solutions and practices on AWS. These are specialized APN Partners with comprehensive expertise and deep experience focused on a specific 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 Financial Services Competency – Technology Partner Prerequisites

APN Membership	APN Partner must meet Select tier+ APN Technology Partner (view requirements)
-----------------------	--

<p>AWS Case Studies</p>	<p>> 2 AWS public or private case studies specific to completed Financial Services projects at the time of application and 2 additional private or public case studies every 12 months:</p> <ul style="list-style-type: none"> ▪ Case study projects started within the past 12 months, and for projects that are in production, rather than in pilot or proof of concept stage ▪ Supporting documentation for each case study submitted with evidence of compliance to the requirements of this checklist <p>> 1 AWS public blog post highlighting partnership with AWS as well as thought leadership in the Financial Services technology segment or 1 public case study, customer can be anonymous.</p>
<p>APN Partner Solution Landing Page</p>	<p>Solution page or microsite highlighting the APN Partner’s cloud technology capabilities, Financial Services specific Compliance, and successes attributed to solution or product evaluated for the purposes of this Competency</p> <p>This page or microsite may include AWS Public Support Statement (see definition above), AWS services and Financial Services use cases, customer references, and any other relevant information supporting the APN Partner’s expertise related to Financial Services Technology and highlighting the partnership with AWS</p> <p>Suggestion to replace paragraph above: APN Partner must have a landing page that describes their AWS Financial Services practice, AWS solutions and Competency use cases, links to AWS case studies, and any other relevant information supporting the APN Partner’s expertise related to Financial Services and highlighting the partnership with AWS.</p> <p>Financial Services practice page must be accessible from APN Partners home page. Home page is not acceptable as a practice page unless APN Partner is a dedicated Financial Services technology company and home page reflects Partner’s concentration on Financial Services.</p>
<p>AWS Financial Services Product or Solution</p>	<p>A solution/product designed and built on AWS specifically for the Financial Services customers. This solution/product provides a comprehensive requirement or feature-set that is unique to Financial Services use cases rather than homogenous across multiple industries, or suited to address a domain-specific problem that is not addressed by many other products.</p> <p>APN Partner Solution Landing Page or a microsite described above, articulating the uniqueness of the solution undergoing Competency validation and its specific benefits to Financial Services customers as well as how the solution leverages AWS.</p> <p>The product/solution available in 2 or more AWS regions and optimized for security, reliability, performance, cost optimization, and operational excellence.</p>
<p>AWS Certifications/Training</p>	<ul style="list-style-type: none"> • ≥ 2 staff trained on AWS Security Fundamentals • ≥ 1 staff certified on AWS associate level or higher. See AWS Certifications

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 case studies 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 Case Studies		Met	Not Met
1.1 Case Studies	<p>APN Partner has two (2) case studies of completed Financial Services projects.</p> <p>APN Partner must provide for each reference:</p> <ul style="list-style-type: none"> ▪ 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 or anonymous case study and segment thought leadership	<p>One (1) AWS public blog post highlighting partnership with AWS and thought leadership in the Financial Services technology segment or one (1) public case study, customer can be anonymous.</p> <p>Evidenced in the form of a publicly available blog post or a case study, white paper, or equivalent that includes, as a minimum:</p> <ul style="list-style-type: none"> ▪ Reference to customer project or series of projects for Financial Services customers with similar customer challenges, APN Partner name, and AWS ▪ How AWS is used as part of these solutions ▪ Outcome(s)/results or benefits to customer/s 		
2.0 Technology Components		Met	Not Met
2.1 AWS Best Practices	APN Partner product provides customers with Financial Services solutions that are aligned with AWS architecture best practices and reference architectures. APN Partner must provide an architectural overview including details on the use of AWS services and patterns to provide highly available and reliable infrastructure.		
2.2 Industry Compliance	Technology solution has capabilities to enable compliance with applicable financial data regulations, including but not limited to PCI.		
2.3 Governance and Audit	Technology solution has capabilities that support good governance, such as real-time verification and reporting through the use of tools such as AWS Identity and Access Management (IAM), AWS CloudTrail, AWS CloudWatch, and AWS Config.		
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	<p>APN Partner product or solution has the appropriate security controls:</p> <ul style="list-style-type: none"> • 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, IAM users, and IAM roles. 		
3.3 Governance and Compliance	<p>Solution has capabilities that support good governance and security, specifically including services such as:</p> <ul style="list-style-type: none"> • AWS Identity and Access Management (IAM) 		



	<ul style="list-style-type: none">• AWS CloudTrail		
--	--	--	--