



# AWS Education Competency Technology Partner Validation Checklist

February 2018  
Version 1.1

---

## Table of Contents

<b>Introduction .....</b>	<b>3</b>
<b>Competency Application and Audit Process .....</b>	<b>3</b>
<b>Program Policies.....</b>	<b>3</b>
<b>AWS Education Technology Competency Categories .....</b>	<b>4</b>
<b>AWS Education Competency Program Prerequisites.....</b>	<b>5</b>
<b>AWS Education Competency Technology Partner Validation Checklist .....</b>	<b>6</b>
<b>1.0 AWS Customer References .....</b>	<b>6</b>
<b>2.0 Solution Architecture.....</b>	<b>6</b>
<b>3.0 Security.....</b>	<b>7</b>
<b>4.0 Compliance .....</b>	<b>7</b>

## 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 and a third-party firm 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 and will send to the third party firm to coordinate scheduling of your Competency review.

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 third party 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 Education Technology Competency Categories

AWS Education Competency Partners have demonstrated technical proficiency and proven customer success providing specialized solutions aligning with AWS architectural best practices to help support teaching and learning, administration, and academic research efforts in education.

In order to properly showcase the best APN Partner for specific customer needs, it is important to highlight areas of strength, depth, and experience.

APN Partner must meet the requirements of one of the following categories to achieve the AWS Education Competency, and cannot occupy more than one category per solution.

Category	Characteristics
<b>Teaching and Learning</b>	<p>Solutions that bring innovative teaching and learning technology to help teachers adapt to new standards, personalize learning, and deliver new and exciting digital learning experiences to students.</p> <p>Solutions in this category include but are not limited to:</p> <ul style="list-style-type: none"> <li>▪ Learning Management Systems</li> <li>▪ Content Management Systems</li> <li>▪ Virtual Classroom</li> </ul>
<b>Administrative and Operations</b>	<p>Solutions that assist educational institutions operate efficiently both on-campus and online. Technology that empowers educational institutions to gain better visibility into IT operations and assist with regulatory requirements.</p> <p>Solutions in this category include but are not limited to:</p> <ul style="list-style-type: none"> <li>▪ Analytical Solutions</li> <li>▪ Resource Management Systems</li> <li>▪ Student Information Systems</li> <li>▪ Facilities Management Systems</li> </ul>

## AWS Education 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 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 Education Competency – Technology Partner Prerequisites

<b>APN Membership</b>	APN Partner must meet Advanced tier+ APN Technology Partner (view <a href="#">requirements</a> )
<b>Public Sector Partner Program Membership</b>	APN Partner must be a current member of the AWS Public Sector Partner Program
<b>AWS Support</b>	APN Partner must have Business level+ Support plan (view <a href="#">Support</a> plans)
<b>AWS Customer References</b>	<p>APN Partner must provide <math>\geq 4</math> AWS customer references specific to completed Education projects:</p> <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ References must be for projects started within the past 36 months</li> <li>▪ All customer references submitted must have supporting documentation providing evidence of compliance to the requirements of this checklist</li> </ul>
<b>AWS Education Product or Solution</b>	<p>APN Partner must have a Education product or solution on AWS, including:</p> <ul style="list-style-type: none"> <li>▪ Availability of product or solution in 1 or more AWS regions</li> <li>▪ Qualifying for and posting an AWS public support statement on APN Partner's website detailing the APN Partner's Education practice on AWS and including public reference to the APN Partner's solution, practice, or guidance on Education. 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 Education and highlighting the partnership with AWS through the APN.</li> <li>▪ A reference architecture for an Education use case which is optimized for security, reliability, performance, cost optimization, and operational excellence.</li> </ul>

## AWS Education Competency 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) for the submitted customer references must be provided, in order to demonstrate compliance to the below requirements.

1.0 AWS Customer References		Met	Not Met
1.1 Customer References	<p>APN Partner has four (4) AWS customer references of completed Education projects.</p> <p>APN Partner must provide for each reference:</p> <ul style="list-style-type: none"> <li>▪ Name of the customer</li> <li>▪ Problem statement/definition</li> <li>▪ What you proposed</li> <li>▪ How AWS services were used as part of the solution</li> <li>▪ Third party applications or solutions used</li> <li>▪ Start and end dates of project</li> <li>▪ Outcome(s)/results</li> <li>▪ Lessons learned</li> </ul>		
1.2 Public References	<p>2 of the above 4 references are publicly endorsed by the customer.</p> <p>Evidence must be in the form of a publicly available case study, white paper, blog post, or equivalent that includes, as a minimum:</p> <ul style="list-style-type: none"> <li>▪ Reference to customer name, APN Partner name, and AWS</li> <li>▪ Customer problem that was solved</li> <li>▪ How AWS was used as part of the solution</li> <li>▪ Outcome(s)/results</li> </ul> <p>Public references must be easily discoverable on the APN Partner's website.</p>		
2.0 Solution Architecture		Met	Not Met
2.1 Solution Capabilities	For each solution considered for the competency, APN Partner submits a detailed 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		
2.2 Solution Architecture and Best Practices	<p>A Solution must follow the best practices defined in the AWS Well-Architected Framework:</p> <ul style="list-style-type: none"> <li>▪ A SaaS or hosted/managed solution must complete a Well-Architected review with AWS Solution Architecture team. Documentation should include plan of action for all open issues. For open critical issues provide an explanation for risk mitigation.</li> <li>▪ A software solution deployed in customer environments must enable the customer to follow best practices outlined in the Well-Architected Framework. Please refer to Section 2.3 for required documentation.</li> </ul>		

2.3 Architecture Documentation	<p>Architectural details of the solution must be provided:</p> <ul style="list-style-type: none"> <li>▪ For a SaaS or hosted/managed solution, supporting documentation must include AWS regions, availability zones, and all leveraged AWS services or components. Documentation should reflect high availability, data backup, and disaster recovery plans.</li> <li>▪ For a software solution (such as an AMI from AWS Marketplace) supporting documentation should include a reference architecture. The reference architecture is expected to adhere to AWS best practices including the Well-Architected Framework as discussed in 2.2.1.</li> </ul>		
--------------------------------	--	--	--

3.0 Security		Met	Not Met
3.1 Security Best Practices	<p>APN Partner solution must follow guidance provided in the <a href="#">AWS Security Best Practices</a> whitepaper:</p> <ul style="list-style-type: none"> <li>▪ A SaaS or hosted/managed solution must follow AWS Security Best Practices</li> <li>▪ A software solution (such as an AMI from AWS Marketplace) that can be deployed in customer environments must enable the customer to follow AWS Security Best Practices as applicable</li> </ul> <p>Documentation should clearly identify implementation details related to AWS Security related best practices.</p>		
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 Identity Access Management (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 Compliance		Met	Not Met
4.1 Compliance	<p>4.1.1 Customers with access to student information may be subject to local compliance and regulatory requirements. APN Partner must identify the compliance and regulatory programs applicable to the environment they support or manage.</p> <p>4.1.2 APN Partner must demonstrate knowledge of the compliance and regulatory programs as identified in 4.1.1 (if any) and provide the following:</p> <ul style="list-style-type: none"> <li>▪ Description of the programs</li> <li>• Documentation of the technical safeguards that are put in place to meet the identified compliance and regulatory requirements. Documentation may be in the form of an assessment (internal or external), and/or a detailed system security assurance plan.</li> </ul>		