aws partner network | competency

AWS Microsoft Workloads Competency

Technology Partner Validation Checklist

June 2019

Version 1.0

aws partner network

Table of Contents

Table of Contents 2
Introduction ..... **Error! Bookmark not defined.**
Expectations of Parties ..... **Error! Bookmark not defined.**
AWS Microsoft Workloads Competency Program 4
AWS Microsoft Workloads Competency Categories 4
AWS Microsoft Workloads Competency Program Prerequisites 5
AWS Microsoft Workloads Competency Program Validation Checklist 8
Microsoft Workloads Technical Requirements by Category 8
Microsoft Workloads 8
Migration 8
Operational Optimization 9
Data, Analytics and Machine Learning 10
AWS Technical Requirements 11

Introduction

The goal of the AWS Competency Program is to recognize AWS Partner Network Partners ("APN Partners") who demonstrate technical proficiency and proven customer success in specialized solution areas. The Competency Partner Validation Checklist ("Checklist") is intended for APN Partners who are interested in applying for an AWS competency. This checklist provides the criteria necessary to achieve the designation under the AWS Competency Program. APN Partners undergo an audit of their capabilities upon applying for the specific competency. AWS leverages in-house expertise and a third-party firm to facilitate the audit. AWS reserves the right to make changes to this document at any time.

Expectations of Parties

It is expected that APN Partners will review this document in detail before applying for the AWS Competency Program, even if all of the prerequisites are met. 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 program office if further assistance is required.

When ready to submit a program application, APN Partners should complete the Partner Self-Assessment column of the Checklist set forth below in this document.

To submit your application:

1. Log in to the APN Partner Central (https://partnercentral.awspartner.com/), as Alliance Lead
2. Select "View My APN Account" from the left side of the page
3. Scroll to "Program Details" section
4. Select "Update" next to AWS Competency you wish to apply for
5. Fill out Program Application and Click "Submit"
6. Email completed Self-Assessment to competency-checklist@amazon.com.

If you have any questions regarding the above instructions, please contact your PDR/PDM.

AWS will review and aim to respond back with any questions within five 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 auditor on the day of the audit.

AWS recommends that APN Partners have individuals who are able to speak in-depth to the requirements during the audit. The best practice is for the APN Partner to make the following personnel available for the audit: one or more highly technical AWS certified engineers/architects, an operations manager who is responsible for the operations and support elements, and a business development executive to conduct the overview presentation. APN Partners should ensure that they have the necessary consents to share with the auditor (whether AWS or a third-party) all information contained within the objective evidence or any demonstrations prior to scheduling the audit.

AWS Microsoft Workloads Competency requirements are available in the following languages:

Chinese (Simplified) | *Chinese (Traditional)* | *French* | *German* | *Italian* | *Japanese* | *Korean* | *Portuguese* | *Russian* | *Spanish*

AWS Microsoft Workloads Competency Program

This AWS Microsoft Workloads Competency Program (referred to as "AWS Microsoft Workloads Competency" or "Competency") identifies and validates APN Technology Partner offerings that help customers assess and migrate Microsoft workloads to AWS as well as deploy, optimize, and modernize Microsoft Workloads on AWS. The relevant offerings are segmented into three categories: Migration, Operational Optimization and Data/Analytics/Machine Learning. These categories are further divided into functionality subcategories. APN Partners can apply for and join the AWS Competency program through one or more of the categories.

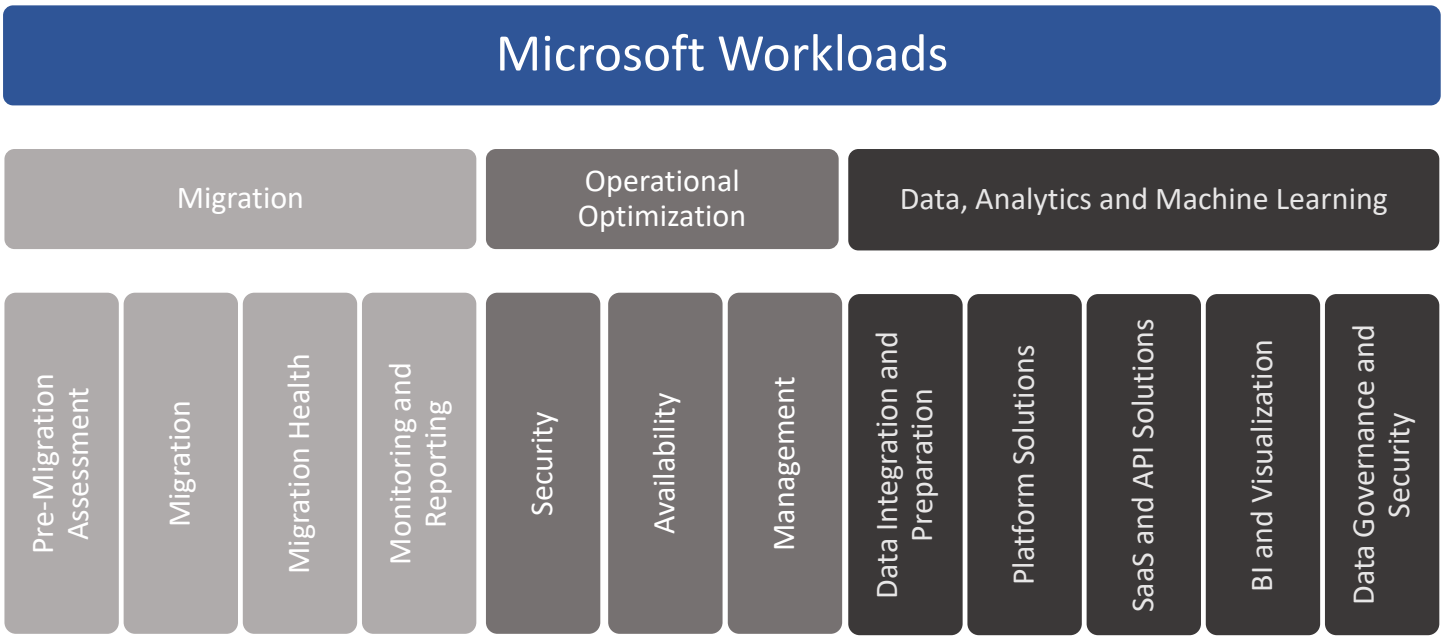
AWS Microsoft Workloads Competency Categories

APN Partners must identify the segment category and subcategory (or categories) that their solution fits into:

1. **Microsoft Workloads Migration**: Technologies in this category provide pre-migration assessment and planning or automate and manage the migration of Microsoft Workloads.

2. **Operational Optimization**: Technologies in this category are used to optimize and automate Microsoft Workloads on AWS in the areas including security, availability, and manageability.

3. **Data, Analytics and Machine Learning:** Technologies in this category prepare, transform, analyze, and govern Microsoft SQL Server data for the purpose of data analytics and machine learning on AWS.



AWS Microsoft Workloads Competency Program Prerequisites

The following items will be validated by the AWS Competency Program Manager; missing or incomplete information must be addressed prior to scheduling of the Technology Validation Review.

1.0 APN Program Requirements		Met Y/N
1.1 Program Guidelines	The APN Partner must read the Program guidelines and definitions before applying to the Microsoft Workloads Competency Program. Click here for Program details.	
1.2 APN Technology Partner Tier	APN Partner must be an Advanced Tier APN Technology Partner	
1.3 Solution Category	APN Partner must identify the Segment category and subcategory (or subcategories) for their solution. Category: ▪ **Microsoft Workloads Migration** ☐ Pre-Migration Assessment ☐ Application and Data Migration ☐ Migration Health ☐ Monitoring and Reporting ▪ **Microsoft Workloads Operational Optimization** ☐ Security and Threat Management ☐ Availability and Disaster Recovery ☐ Resource Management, Inventory/Health/Cost Monitoring and Reporting, Resource Management, Inventory/Health/Cost Monitoring and Reporting ▪ **Data, Analytics, and Machine Learning for Microsoft Workloads** ☐ Data integration and preparation ☐ Platform Solutions ☐ SaaS and API Solutions ☐ Business Intelligence and Visualization ☐ Data Governance, Compliance, and Security	
2.0 Case Studies		**Met Y/N**
2.1 Microsoft Workloads-Specific Case Studies	APN Partner must have a minimum of four (4) case studies that demonstrate the use of APN Partner's technology relevant to the category under review. For APN Partners already validated in AWS Migration, DevOps, or Data & Analytics Competencies, the requirement is reduced to a minimum of 2, one public and one private case studies, that demonstrate the use of APN Partner's technology with Microsoft Workloads relevant to the category under review. If more than one catetory is under review, at least one case study should demonstrate the use of technology in each subcategory. For each case study, the APN Partner must provide the following information: ▪ Name of the customer ▪ Customer challenge ▪ How the solution was deployed to meet the challenge ▪ Third party applications or solutions used ▪ Date the reference entered production ▪ Outcome(s)/results	

	▪ Specific Architecture Diagrams, Deployment Guides and other materials depending on the type of solution, as described in the next section. This information will be requested as part of the Program Application process in APN Partner Central. All four of the case studies provided will be examined in the Technical Validation. The case study will be removed from consideration for inclusion in the AWS Competency if the APN Partner cannot provide the documentation necessary to assess the case study against each checklist item, or if any of the checklist items are not met. Case studies must describe deployments that have been performed within the past 18 months, and must be for projects that are in production with customers, rather than in a 'pilot' or proof of concept stage.	
2.2 Public Case Studies	Publicly available case studies are used by AWS upon approval into the Competency to showcase the APN Partner's demonstrated success based on measurable Key Performance Indicators (KPIs) with the solution and provide customers with confidence that the APN Partner has the technology to meet their objectives. Two (2) of the four (4) customer deployments associated with the case studies must be publicized by the APN Partner as publicly available case studies. These publicly available case studies may be in the form of formal case studies, white papers, videos, or blog posts.	
	Publicly available case studies must be easily discoverable from the APN Partner's website, e.g. it must be possible to navigate to the publicly available case studies from the APN Partner's home page, and the APN Partner must provide links to these publicly available case studies in their application.	
	Publicly available case studies must include the following: ▪ Customer name, APN Partner name, and AWS ▪ Customer challenge ▪ How the solution was deployed to meet the challenge ▪ How AWS services were used as part of the solution ▪ Outcome(s)/results	
3.0 AWS Microsoft Workloads Web Presence and Thought Leadership		**Met Y/N**
3.1 Partner AWS Microsite	An APN Partner's internet presence specific to their AWS Microsoft Workloads solutions provides customers with confidence about the APN Partner's capabilities and experience. APN Partner must have an AWS microsite page that describes their AWS Microsoft Workloads solution, links to their publicly available case studies, lists technology partnerships, and provides any other relevant information supporting the Partner's expertise related to Microsoft Workloads and highlighting the partnership with AWS. This AWS-specific Microsoft Workloads microsite must be accessible from the APN Partner's home page. The home page itself is not acceptable as an AWS microsite unless APN Partner is a dedicated Microsoft Workloads company and home page reflects APN Partner's focus on Microsoft Workloads.	
3.2 Microsoft Workloads Thought Leadership	AWS Microsoft Workloads Competency Partners are viewed as having deep domain expertise in Cloud Management, having developed innovative solutions that leverage or help manage AWS services. APN Partner must have public-facing materials (e.g., blog posts, press articles, videos, etc.) showcasing the APN Partner's focus on and expertise in Microsoft Workloads. Links must be provided to examples of materials published within the last 12 months.	
4.0 Business Requirements		**Met Y/N**
4.1 Product Support/Help Desk	APN Partner offers product support via web chat, phone, or email support to customers. Evidence must be in the form of description of support offered to customers for their product or solution.	
4.2 Product is listed on AWS Marketplace	APN Partner makes solution available via AWS Marketplace. ☐ Yes ☐ No If "yes", APN Partner must provide a link to the AWS Marketplace listing. If "no", no further information is required. Note, AWS Marketplace is not mandatory to achieve the Competency.	

4.3 Deployment Model	APN Partner identifies all deployment model options available to customers. ☐ SaaS on AWS ☐ SaaS outside AWS (for Migration) ☐ BYOL on AWS ☐ BYOL on premises (for Migration)	
5.0 APN Partner Self-Assessment		**Met Y/N**
5.1 AWS Competency Partner Program Validation Checklist Self-Assessment	APN Partner must conduct a self-assessment of their compliance with this checklist. ▪ APN Partner must complete all sections of the Checklist. ▪ Completed self-assessment must be emailed to **competency-checklist@amazon.com**, using the following convention for the email subject line: "[APN Partner Name], Microsoft Workloads Competency Technology Partner Completed Self-Assessment." ▪ It is recommended that APN Partner has their Partner Solutions Architect, PDR, 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 review and to help ensure a productive review experience.	

AWS Microsoft Workloads Competency Program Validation Checklist

The following items will be validated by an AWS Partner Solutions Architect and/or the Third-party Auditors and/or AWS Partner Solutions Architects; missing or incomplete information must be addressed prior to scheduling of the Technology Validation Review.

Microsoft Workloads Technical Requirements by Category

Documentation describing how the APN Partner solution meets the requirements must be submitted as part of the AWS Competency self-assessment.

Microsoft Workloads Migration

Required Solution Features		Met Y/N
Pre-Migration Assessment	The technology solution must use either agent or agentless technology to automatically identify workloads to be migrated to AWS. This can include: ▪ Microsoft Workload Pre-Migration assessment of one (or more) of the following: o Assessment of servers and virtual machines running Microsoft Windows on premises o Docker container assessment (either running on Windows Server or if container is running .NET/.NET Core application) o .NET/.NET Core application assessment o Data Migration Assessment (SQL, file system, blob, etc.) o Enterprise solution migration assessment (Active Directory, OneDrive, Dynamics, Exchange, etc.). ▪ Pre-Migration assessment report should be generated. each workload into customer designated AWS resource group	
Migration	The technology solution must use either agent or agentless technology to automatically migrate identified workloads to AWS, or data as part of workload migration. This can include: ▪ Microsoft Workload Migration of one of the following: o Virtual machines migration o Docker containers migration (either running on Windows Server or if container is running .NET/.NET Core application) o .NET/.NET Core application migration o Data migration (SQL, file system, blob, etc.) o Enterprise solution migration (Active Directory, OneDrive, Dynamics, Exchange, etc.). ▪ Ability to perform backup and rollback in case any phase of migration is unsuccessful, at any point in time with minimal or no data loss. ▪ Enables hybrid cloud configurations for disaster recovery ▪ Difference delta synchronization to synchronize data after migration until cut over and source server/instance is shut down. ▪ Cutover of each workload into customer designated AWS resource group	
Migration Health	Technology solution should do an assessment during the migration to ascertain real time: ▪ Data integrity ▪ Application health ▪ Overall connected architecture health assessment	
Monitoring and reporting	Technology solution should:	

	▪ Monitoring migration progress ▪ Notifications, warnings and error reporting ▪ Overall Migration Reporting	

Operational Optimization

Required Solution Features		Met Y/N
Security	Technology Solution should perform the following: ▪ Security posture configuration (Role based access, identity access and management, proxy/firewall configuration, routing, encryption etc.) ▪ Providing analysis for DLP (Data Loss Prevention) ▪ Network and instance security posture (ports, certificates, security configuration) ▪ Threat modelling for network traffic (possible attack vectors) and alerting. ▪ Compliance (HIPAA, PCI, SOX etc) ▪ Ability to recommend improvements in security posture ▪ Source code check bad practices, memory leaks, data hygiene, and security issues.	
Availability	Technology Solution should perform the following: ▪ Continuous Disaster Recovery check. (Chaos Engineering) o Scalability o Availability o Data integrity and resilience ▪ Resource analysis for to determine high availability issues. ▪ Ability to auto scale (scale in and scale out) as workload varies	
Management	Technology Solution should perform the following: ▪ Inventory listing and analysis (in Amazon EC2 instances, containers, serverless) of: o Microsoft Workload assets o Microsoft Workload configuration o Microsoft infrastructure configuration. ▪ Automatic discovery of: o Network configuration o Compute resources (servers, clusters) o Storage resources (LUNs, iSCSI targets, etc.) o Databases (engine, configuration, version, compatibility) ▪ Historical analysis of inventory changes (over a selected period of time). ▪ Resource allocation, capacity utilization analysis. ▪ Continuous cost analysis and alerting (both resource utilization and licensing). ▪ Ability to recommend reduced provisioning based on utilization and workload patterns ▪ Continuous performance analysis and alerting. ▪ Common Microsoft Workload specific automation operational tasks such as: o Backup and restore	

	○ Patching ○ Workload state management ○ Configuration management ▪ Benchmark required/average performance of solutions/applications on premise. ▪ Provide instance, resource matching and recommendations on AWS based on benchmarking. ▪ POC and benchmark solutions/applications in AWS. ▪ Provide estimated TCO and resource utilization based on benchmarking. ▪ Reporting: ○ Performance reporting, delivery and alerting (for reports). ○ Infrastructure reporting, delivery and alerting (for reports). ○ Workload configuration and health reporting, delivery and alerting (for reports). ○ Patching reporting, delivery and alerting (for reports).	

Data, Analytics and Machine Learning

Required Solution Features		Met Y/N
Data Integration and Preparation	Technical solution should be able to: ▪ Ingest workload data and propose action ▪ Annotate descriptive, structural, administrative, reference and statistical data: ○ Syntactic and dependency tree-banking, including the identification of co-reference ○ Semantic annotation of text, including named-entity identification for search, sentiment analysis, and data-mining applications ○ Identification of language, dialect, and speaker demographics ○ Video, picture, word file, pdf, etc. ○ Department, business unit, process ○ Security protection level (Confidential, Public, Private, etc.) ○ Object type (Building, Person, Animal… etc.) ▪ Move and consolidate data from disparate sources. ▪ Transform and prepare data a for analytics. ▪ Data quality checking. ▪ Data replication. ▪ Data profiling. ▪ Feature Engineering - creating new input features from your existing ones.	
Platform Solutions	Technical solution should be: ▪ Tightly integrated tools designed to work together and resolve analytic challenges within standardized framework, components may include: ○ Storage ○ Processing ○ Scheduling ○ Security	

	○ Analytic facilities ▪ Enabling data scientists and machine learning practitioners with tools to take their data, train predictive models and make predictions on new data.	
SaaS and API Solutions	This category includes solutions that enable predictive (AI/ML) capabilities within customer applications: ▪ Web ▪ Client ▪ Frameworks	
Business Intelligence and Visualization	Technical solutions that turn raw data into actionable business information using analytic processing technologies such as: ▪ Reporting ▪ Dashboarding ▪ Data Visualization	
Data Governance and Security	Technical solutions to discover, categorize, and control data. This includes: ▪ Defining and enforcing policies. ▪ Security and management of personal information. ▪ Creating data catalogs and glossaries. ▪ Data lineage. ▪ Data masking.	

AWS Technical Requirements

The following are the technical requirements for each of the 4 case studies submitted by the APN Partner. Each must demonstrate that the APN Partner's deployed solutions meet AWS best practices and adhere to the AWS Well-Architected framework.

		Applies to:				Met Y/N
		Multi-tenant SaaS	Single-tenant SaaS	Customer Deployed On-Premises	Customer Deployed on AWS	
Required Documentation The following documentation must be submitted as part of the Competency Self-Assessment.						
Architecture Diagram	Depending on the Deployment Category, one or more Architecture Diagrams are required. Each Architecture Diagram must show: ▪ The major elements of the architecture, and how they combine to provide the APN Partner Solution to customers ▪ All of the AWS Services used, using the appropriate AWS Service icons. ▪ How the AWS Services are deployed, including Amazon Virtual Private Cloud (Amazon VPC), Availability Zones, subnets, and connections to systems outside of AWS. ▪ Includes elements deployed outside of AWS, e.g. on-premises components, or hardware devices.	Yes – one for the whole solution and one for each Case Study	Yes – one for the whole solution and one for each Case Study	Yes – one for each Case Study	Yes – one for each Case Study	

Deployment Guide	The Deployment Guide must provide best practices for deploying the APN Partner Solution on AWS, and include all of the sections outlined in "Baseline Requirements for Deployment Guides"	No	No	No	Yes – one for the solution.	
Completed Validation Checklist	For each of the four case studies, the APN Partner must provide a completed version of the following checklist indicating which checklist items are met.	Yes	Yes	Yes	Yes	
1.0 Security 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.						
1.1 AWS account root user is not used for routine activities	The AWS account root user must not be used for routine activities. Following the creation of your AWS account, you should immediately create AWS Identity and Access Management (IAM) user accounts, and use these IAM user accounts for all routine activities. Once your IAM user accounts have been created, you should securely store the AWS root account credentials and use them only to perform the few account and service management tasks that require the AWS account root user. For further information on how to set up an IAM user accounts and groups for daily use, see Creating Your First IAM Admin User and Group.	Yes	Yes	No	No	
1.2 Multi-Factor Authentication (MFA) has been enabled on the AWS account root user	Multi-Factor Authentication (MFA) must be enabled for your AWS account root user. Because your AWS account root user can perform sensitive operations in your AWS account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available, including virtual MFA and hardware MFA.	Yes	Yes	No	No	
1.3 IAM user accounts used for all routine activities	The AWS account root user must not be used for any task where it is not required. Instead, create a new IAM user for each person that requires administrator access. Then make those users administrators by placing the users into an Administrators group to which you attach the Administrator Access managed policy. Thereafter, the users in the administrators group should set up the groups, users, and so on, for the AWS account. All future interaction should be through the AWS account's users and their own keys instead of the root user. However, to perform some account and service management tasks, you must log in using the root user credentials.	Yes	Yes	No	No	
1.4 Multi-Factor Authentication (MFA) is enabled for all interactive IAM users	You must enable MFA for all interactive IAM users. With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).	Yes	Yes	No	No	
1.5 IAM credentials are rotated regularly	You must change your passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a password policy to your account to require all your IAM users to rotate their passwords, and you can choose how often they must do	Yes	Yes	Yes (for credentials used to integrate with AWS)	Yes (for credentials used to integrate with AWS)	

	so. For more information about rotating access keys for IAM users, see Rotating Access Keys.					
1.7 Strong password policy is in place for IAM users	You must configure a strong password policy for your IAM users. If you allow users to change their own passwords, require that they create strong passwords and that they rotate their passwords periodically. On the Account Settings page of the IAM console, you can create a password policy for your account. You can use the password policy to define password requirements, such as minimum length, whether it requires non-alphabetic characters, how frequently it must be rotated, and so on. For more information, see Setting an Account Password Policy for IAM Users.	Yes	Yes	Yes (for credentials used to integrate with AWS)	Yes (for credentials used to integrate with AWS)	
1.8 IAM credentials are not shared among multiple users	You must create an individual IAM user account for anyone who needs access to your AWS account. Create an IAM user for yourself as well, give that user administrative privileges, and use that IAM user for all your work. By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can change or revoke an IAM user's permissions any time. (If you give out your root user credentials, it can be difficult to revoke them, and it is impossible to restrict their permissions.)	Yes	Yes	No	No	
1.9 IAM policies are scoped down to least privilege	You must follow the standard security advice of granting least privilege. This means granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. Defining the right set of permissions requires some research. Determine what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions.	Yes	Yes	Yes (for solutions ran outside of AWS integrated via IAM roles, least privilege access should be applied)	Yes (for solutions ran outside of AWS integrated via IAM roles, least privilege access should be applied)	
1.10 Hard-coded credentials (e.g. access keys) are not used	You must follow best practices for managing AWS access keys and avoid the use of hard-coded credentials. When you access AWS programmatically, you use an access key to verify your identity and the identity of your applications. Anyone who has your access key has the same level of access to your AWS resources that you do. Consequently, AWS goes to significant lengths to protect your access keys, and, in keeping with our shared responsibility model, you should as well.	Yes	Yes	Yes (credentials used to integration with AWS should be easily changed and not hard coded)	Yes (credentials used to integration with AWS should be easily changed and not hard coded)	
1.11 All credentials are encrypted at rest	The requirement is to ensure the encryption of any credentials at rest.	Yes	Yes	Yes (credentials stored in partner solution used to integrate with AWS should be	Yes (credentials stored in partner solution used to integrate with AWS	

				encrypted)	should be encrypted)	
1.12 AWS Access Keys only used by interactive users	No AWS Access Keys should be in use, except in the following cases: 1. Used by humans to access AWS Services, and stored securely on a device controlled by that human. 2. Used by a service to access AWS Services, but only in cases where: a) It is not feasible to use an Amazon Elastic Compute Cloud (Amazon EC2) instance role, Amazon ECS Task Role or similar mechanism, b) The AWS Access Keys are rotated at least weekly, and c) The IAM Policy is tightly scoped so that it: i) Allows only access to only specific methods and targets and ii) Restricts access to the subnets on from which the resources will be accessed.	Yes	Yes	No	No	
1.13 AWS CloudTrail is enabled for all AWS accounts in every region	AWS CloudTrail must be enabled on all AWS accounts and in every region. Visibility into your AWS account activity is a key aspect of security and operational best practices. You can use AWS CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.	Yes	Yes	No	No	
1.14 AWS CloudTrail logs are stored in an Amazon S3 bucket owned by another AWS account	AWS CloudTrail logs must be emplaced in a bucket owned by another AWS account configured for extremely limited access, such as audit and recovery only.	Yes	Yes	No	No	
1.15AWS CloudTrail Amazon S3 log bucket has Versioning or MFA Delete enabled	AWS CloudTrail log bucket contents must be protected with versioning or MFA Delete.	Yes	Yes	No	No	
1.16 Amazon EC2 security groups are tightly scoped	All Amazon EC2 security groups should restrict access to the greatest degree possible. This includes at least 1. Implementing Security Groups to restrict traffic between Internet and Amazon VPC, 2. Implementing Security Groups to restrict traffic within the Amazon VPC, and 3. In all cases, allow only the most restrictive possible settings.	Yes	Yes	No	Yes	
1.17 Amazon S3 buckets within your account have appropriate levels of access	You must ensure that the appropriate controls are in place to control access to each Amazon S3 bucket. When using AWS, it's best practice to restrict access to your resources to the people that absolutely need it (the principle of least privilege).	Yes	Yes	No	No (unless partner solution running on AWS requires the S3 service)	
1.18 Amazon S3 buckets have not been misconfigured to	You must ensure that buckets that should not allow public access are properly configured to prevent public access. By default, all Amazon S3 buckets are private, and can only be accessed by users that have been explicitly granted access. Most use cases won't require	Yes	Yes	No	No (unless partner solution running on AWS	

allow public access.	broad-ranging public access to read files from your Amazon S3 buckets, unless you're using Amazon S3 to host public assets (for example, to host images for use on a public website), and it's best practice to never open access to the public.				requires the S3 service)	
1.19 A monitoring mechanism is in place to detect when Amazon S3 buckets or objects become public	You must have monitoring or alerting in place to identify when Amazon S3 buckets become public. One option for this is to use AWS Trusted Advisor. AWS Trusted Advisor checks buckets in Amazon S3 that have open access permissions. Bucket permissions that grant list access to everyone can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant Upload/Delete access to everyone create potential security vulnerabilities by allowing anyone to add, modify, or remove items in a bucket. The AWS Trusted Advisor check examines explicit bucket permissions and associated bucket policies that might override the bucket permissions.	Yes	Yes	Yes	No (unless partner solution running on AWS requires the S3 service)	
1.20 A monitoring mechanism is in place to detect changes in Amazon EC2 instances and Containers	Any changes to your Amazon EC2 instances or Containers may indicate unauthorized activity, and must at a minimum be logged to a durable location to allow for future forensic investigation. The mechanism employed for this purpose must at least: 1. Detect any changes to the OS or application files in the Amazon EC2 instances or Containers used in the solution. 2 Store data recording these changes in a durable location, external to the Amazon EC2 instance or Container. Examples of suitable mechanisms include: a. Deployment of file integrity checking via scheduled configuration management (e.g. Chef, Puppet, etc.) or a specialized tool (e.g. OSSEC, Tripwire or similar), or b. Extending configuration management tooling to validate Amazon EC2 host configuration, and alert on updates to key configuration files or packages with 'canary' (logged no-op) events configured to ensure the service remains operational on all in-scope hosts during runtime, or c. Deploying a Host Intrusion Detection System such as an open source solution like OSSEC with ElasticSearch and Kibana or using a partner solution. Note that the following mechanism does not meet this requirement: a. Frequently cycling Amazon EC2 instances or Containers.	Yes	Yes	No	No	
1.21 All data is classified	All customer data processed and stored in the workload is considered and classified to determine its sensitivity and the appropriate methods to use when handling it.	Yes	Yes	No	No	
1.22 All sensitive data is encrypted	All customer data classified as sensitive is encrypted in transit and at rest.	Yes	Yes	No	No	
1.23 Cryptographic keys are managed securely	All cryptographic keys are encrypted at rest and in transit, and access to use the keys is controlled using an AWS solution such as KMS or an APN Partner solution such as HashiCorp Vault.	Yes	Yes	Yes	Yes	
1.24 All data in transit is encrypted	All data in transit across a VPC boundary is encrypted.	Yes	Yes	Yes	Yes	
1.25 Security incident response process is defined and rehearsed	A security incident response process must be defined for handling incidents such as AWS account compromises. This process must be tested by implementing procedures to rehearse the incident response process, e.g. by completing a security game day exercise. A rehearsal	Yes	Yes	No	No	

	must have been held within the last 12 months to confirm that: a. The appropriate people have access to the environment. b. The appropriate tools are available. c. The appropriate people know what to do to respond to the various security incidents outlined in the plan.					
2.0 Reliability The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.						
2.1 Network connectivity is highly available	Network connectivity to the solution must be highly available. If using VPN or AWS Direct Connect to connect to customer networks, the solution must support redundant connections, even if the customers do not always implement this.	Yes	Yes	Yes	Yes	
2.2 Infrastructure scaling mechanisms align with business requirements	Infrastructure scaling mechanisms must align with business requirements, either by: 1. Implementing auto-scaling mechanisms at each layer of the architecture, by 2. Confirming that current business requirements, including cost requirements and anticipated user growth, do not require auto-scaling mechanisms and manual scaling procedures are fully documented and frequently tested.	Yes	Yes	No	Yes	
2.3 AWS and Application logs are managed centrally	All log information from the application, and from the AWS infrastructure, should be consolidated into a single system.	Yes	Yes	No	No	
2.4 AWS and Application monitoring and alarms are managed centrally	The application and the AWS infrastructure must be monitored centrally, with alarms generated and sent to the appropriate operations staff.	Yes	Yes	No	No	
2.5 Infrastructure provisioning and management is automated	The solution must use an automated tool such as CloudFormation or Terraform to provision and manage the AWS infrastructure. The AWS Console must not be used to make routine changes to the production AWS infrastructure.	Yes	Yes	No	No	
2.6 Regular data backups are being performed	You must perform regular backups to a durable storage service. Backups ensure that you have the ability to recover from administrative, logical, or physical error scenarios. Amazon S3 and Amazon Glacier are preferred services for backup and archival. Both are durable, low-cost storage platforms. Both offer unlimited capacity and require no volume or media management as backup data sets grow. The pay-for-what- you-use model and low cost per GB/month make these services a good fit for data protection use cases.	Yes	Yes	No	No	
2.7 Recovery mechanisms are being tested on a regular schedule and after significant architectural changes	You must test recovery mechanisms and procedures, both on a periodic basis and after making significant changes to your cloud environment. AWS provides substantial resources to help you manage backup and restore of your data.	Yes	Yes	No	No	
2.8 Solution is resilient to	The solution must continue to operate in the case where all of the services within a single availability zone have been disrupted.	Yes	Yes	No	Yes	

availability zone disruption						
2.9 Resiliency of the solution has been tested	The resiliency of the infrastructure to disruption of a single availability zone has been tested in production, e.g. through a game day exercise, within the last 12 months.	Yes	Yes	No	Yes	
2.10 Disaster Recovery (DR) plan has been defined	A well-defined Disaster Recovery plan includes a Recovery Point Objective (RPO) and a Recovery Time Objective (RTO). You must define an RPO and an RTO for all in-scope services, and the RPO and RTO must align with the SLA you offer to your customers	Yes	Yes	No	No	
2.11 Recovery Time Objective (RTO) is less than 24 hours	The baseline requirement is for the RTO to be less than 24 hours for core services.	Yes	Yes	No	No	
2.12 Disaster Recovery (DR) plan is adequately tested	Your DR plan must be tested against your Recovery Point Objective (RPO) and Recovery Time Objective (RTO), both periodically and after major updates. At least one DR test must be completed prior to approval of your AWS APN Advanced Tier application.	Yes	Yes	No	No	
2.13 Disaster Recovery (DR) plan includes recovery to another AWS account	Your DR plan must include a strategy for recovering to another AWS account, and your periodic recovery testing must test this scenario. You must have completed at least one full test of the DR plan, including at least recovery to another AWS account, within the last 12 months. Note: Although processes restoring data into test environments or exporting data for users are useful ways to verify backups, these processes do not fulfill the requirement to perform a full restore test to another AWS account.	Yes	Yes	No	No	
3.0 Operational Excellence The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include managing and automating changes, responding to events, and defining standards to successfully manage daily operations.						
3.1 Deployment of code changes is automated	The solution must use an automated method of deploying code to the AWS infrastructure. Interactive SSH or RDP sessions must not be used to deploy updates in the AWS infrastructure.	Yes	Yes	No	No	
3.2 Runbooks and escalation process are defined	Runbooks must be developed to define the standard procedures used in response to different application and AWS events. An escalation process must be defined to deal with alerts and alarms generated by the system, and to respond to customer-reported incidents. The escalation process must also include escalating to AWS Support where appropriate.	Yes	Yes	No	No	
3.3 AWS Business Support is enabled for the AWS Account	Business Support must be enabled. Business Support (or greater) is an AWS Partner Network requirement for Advanced Tier Technology Partners. To qualify for Advanced Tier, you must enable Business Support on at least one of your AWS accounts.	Yes	Yes	No	No	