# AWS Nonprofit Competency
## Technology Partner Validation Checklist

June 2018
Version 1.0

# Table of Contents

# Introduction

The goal of the AWS Competency Program is to recognize 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. The checklist provides the criteria necessary to achieve the designation under the AWS Competency Program. APN Partners undergo a validation of their capabilities upon applying for the specific Competency. 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 submitting an application for the AWS Competency Program, even if all of the prerequisites are met. If items in this document are unclear or require further explanation, please contact your Partner Development Representative (PDR) or 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 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 Nonprofit-competency-checklist@amazon.com

If you have any questions regarding the above instructions, please contact your APN Partner Development Representative/Manager.

AWS will review and aim to respond back with any questions within five (5) business days to initiate scheduling of your validation or to request additional information.

APN Partners should prepare for the validation by reading the checklist, completing a self-assessment, and gathering and organizing the necessary documentation.

AWS recommends that APN Partners have individuals who are able to speak in-depth to the requirements during the validation. The best practice is for the APN Partner to make the following personnel available for the validation: one or more highly technical AWS engineers/architects who can speak about the submitted case studies applicable to this competency, an operations manager who is responsible for the operations and support elements, and a business development executive to conduct the overview presentation.

# Program Participation and Benefits

AWS may revoke an APN Partner's status as an AWS Competency Partner if at any time AWS determines in its sole discretion that such APN Partner does not meet the AWS Competency Program requirements or otherwise fails to represent the high standards expected of AWS Competency Partners. If an APN Partner's status as an AWS Competency Partner is revoked, such APN Partner will (i) no longer receive, and will immediately cease taking advantage of, any AWS Competency Partner Program benefits, (ii) immediately cease use of all materials provided to it in connection with the AWS Competency Partner Program and (iii) immediately cease to identify itself or hold itself out as an AWS Competency Partner.

# Impact of Merger, Acquisition, and Divestiture Activity

The AWS Competency Program validates Partners solutions, as well as its business and delivery models. These business and delivery models are often significantly impacted in the process of mergers, acquisitions and divestitures. As a result, APN Partners may be required to reapply and complete a new validation based on the resulting businesses from their M&A activity. Please refer to the guidelines below.

**Acquisition/Merger**
Competency Partner acquires non-Competency Partner: No immediate action required. The Competency Partner should describe any impacts to its AWS Competency solution during any subsequent validation.

Non-Competency Partner acquires Competency Partner: New application and validation required for acquiring Partner to be recognized as an AWS Competency Partner. The new business and delivery models, as well as the integration of the acquired technical capabilities, must be validated through the third-party validation process. We recommend that this be done as soon as possible to ensure continued recognition in the AWS Competency Program.

Competency Partner acquires another Competency Partner: No immediate action required. The consolidated entity will be assessed during the renewal for either of the original entities (whichever date is soonest).

**Divestiture**
Competency Partner divests a portion of its business related to its AWS Competency practice: The divesting business should immediately disclose significant impacts to its AWS Competency that would materially impact its standing as a Competency Partner. Depending on the significance of the impact, the APN Partner will either be immediately removed from the program or will be required to highlight impacts to the business during the next renewal. The divested business will be required to apply to the Competency Program as a new APN Partner.

# Definitions

**Action Items (AIs):** Non-negotiable items that must be addressed by the Partner to be accepted into the AWS Competency Program.

**Case Study:** A written description of an individual customer solution and outcomes. This should include an introduction to the customer, overview of the challenge, details about the solution implemented, and outcomes realized by the customer. Individual AWS programs will provide details about specific requirements for a case study. 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 validation or demonstrating to AWS that Partner meets program requirements).

**Customer Reference:** A completed customer project that can be described for the purposes of demonstrating Partner success in a given practice area. Customer references may be documented in a written **case study** (see definition), white paper, blog post, etc., and may be publically referenceable or private.

**Partner Solution Landing Page:** Also referred to as a microsite; a website or page that highlights the Partner's capabilities and successes in a given solution. Page may include Competency use cases, technology partnerships, customer references, and any other relevant information highlighting the partnership with AWS.

**Donor Management and Marketing Tools:** APN Partners offer various solutions that focus on driving innovation and improving the philanthropic experience of donors and volunteers. These donor management and annual campaign tools include solutions that provide Nonprofit and charitable organizations clear visibility into their diverse network of donors and volunteers. APN Partners offer simple solutions for managing relationships, and strategically implementing external communication strategies.

**Fundraising and Operations Tools:** APN Partners offer various solutions and technology that empower Nonprofit organizations and charities to operate efficiently and maintain lean operations. These donation management and operations tools include fundraising applications and platforms that assist Nonprofit and Charity organizations in tracking and managing grants, donations, and other monetary and/or in-kind donations.

# AWS Nonprofit Technology Competency Categories

Nonprofit & Charity Partner Solutions deliver a set of user-friendly and cost-effective database, analytics, engagement, and fundraising services that enable philanthropic organizations to leverage technology to maximize efficiency in completing mission critical activities, and driving social change.

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 at least one of the following categories to achieve the AWS Nonprofit Competency.

| Category | Characteristics |
|---|---|
| **Donor Management and Marketing Tools** | APN Partners offer various solutions that focus on driving innovation and improving the philanthropic experience of donors and volunteers. These donor management and annual campaign tools include solutions that provide Nonprofit and Charitable organizations clear visibility into their diverse network of donors and volunteers. These Partners offer simple solutions for managing relationships, and strategically implementing external communication strategies. |
| **Fundraising and Operations Tools** | APN Partners offer various solutions and technology that empower Nonprofit organizations and Charities to operate efficiently and maintain lean operations. These donation management and operations tools include fundraising applications and platforms that assist Nonprofit and Charity organizations in tracking and managing grants, donations, and other monetary and/or in-kind donations. |

# AWS Nonprofit Competency Program Prerequisites

AWS Nonprofit Competency Partners provide solutions targeting one or more of the primary steps in discrete manufacturing or process industries: Product Design, Production Design, Production, and Operations. These specialized software solutions enable companies in process and discrete manufacturing industries to increase the pace of product innovation while decreasing production and operational costs in their value chain.

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 Membership | | Met Y/N |
|---|---|---|
| **1.1 Technology Partner Tier** | APN Partner must be an Advanced Tier APN Technology Partner before applying to the Nonprofit Competency Program. | |
| **1.2 Program Membership** | APN Partner must be a member of the Public Sector Partner Program (PSP) prior to applying for this competency: https://aws.amazon.com/partners/public-sector/ | |
| **1.3 Solution Category** | Partner to describe whether their AWS Nonprofit Solution is:<br>☐ **Multi-tenant SaaS:** Serve multiple customers from shared AWS infrastructure. All AWS accounts are managed by the APN Partner.<br>☐ **Single-tenant SaaS:** Serve multiple customers but have some infrastructure components deployed in AWS accounts dedicated to individual customers. All AWS accounts are managed by the APN Partner.<br>☐ **Managed Service:** Are deployed on AWS and serve a single customer. All AWS accounts are managed by the APN Partner.<br>☐ **Customer-Deployed:** Are deployed in a customer AWS environment. All AWS accounts are managed by the customer | |
| **2.0 AWS Case Studies** | | **Met Y/N** |
| **2.1 Nonprofit-Specific Case Studies** | APN Partner must have four (4) AWS Case Studies specific to a single Nonprofit solution under review.<br><br>For each AWS Case Study, the APN Partner must provide the following information:<br>▪ Name of the customer<br>▪ Customer challenge | |

| | | |
|---|---|---|
| | ▪ How the solution was deployed to meet the challenge<br>▪ Third party applications or solutions used<br>▪ Date the reference entered production<br>▪ Outcome(s)/results<br>▪ Specific Architecture Diagrams, Deployment Guides and other materials depending on the type of solution, as described in the next section.<br><br>This information will be requested as part of the Program Application process in APN Partner Central. The information provided as part of this AWS Case Study can be private, and will not be made public.<br><br>All four of the AWS Case Studies provided will be examined in the Documentation Review of the Technical Validation. The Case Study will be removed from consideration for inclusion in the competency if the Partner cannot provide the documentation necessary to access the reference against each checklist item, or if there were Critical Findings identified during the validation.<br><br>References must have been created or updated within the past 18 months, and must be for projects that are in production, rather than in a 'pilot' or proof of concept stage. | |
| **2.2 Publicly Available Case Studies** | Publicly available case studies are used by AWS upon approval into the Competency to showcase the Partner's demonstrated success with the solution and provide customers with confidence that the APN Partner has the experience and knowledge needed to develop and deliver solutions to meet their objectives.<br><br>Two (2) of the four (4) customer deployments associated with the AWS Case Studies must be publicized by the APN Partner as publicly available case studies. These publicly available case studies may 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., must be able to navigate to the case study from the Partner's home page, and the APN Partner must provide links to these publicly available case studies. | |
| | Publicly available case studies must include the following:<br>▪ References to the customer name, APN Partner name, and AWS<br>▪ Customer challenge<br>▪ How the solution was deployed to meet the challenge<br>▪ How AWS services were used as part of the solution<br>▪ Outcome(s)/results | |
| **2.3 Nonprofit Specific Solution Criteria** | The APN Partner solution used in the AWS Case Studies must be meet the following requirements:<br>▪ It must be a Nonprofit solution, targeting one or more of the following categories: Donor Management and Marketing Tools or Fundraising and Operations Tools.<br>▪ It must follow AWS best practices as defined in the AWS Well-Architected framework.<br>▪ It must be clearly differentiated from existing solutions. AWS Competency Solutions enable customers to do things that were previously impossible, too costly, or too difficult. These solutions must prove more than customer success and need to be a nonprofit specific solution based on the aforementioned criteria. | |
| **2,4 End of Project Customer Satisfaction Survey** | APN Partner asks for responses on the AWS Customer Satisfaction Survey at the end of the project. This is accomplished by searching for the Partner in the AWS Partner Solutions Finder and asking Customer to leverage the "Rate this Partner" feature.<br><br>Evidence must be in the form of a demonstration to show where the "Rate this Partner" feature is located on the AWS Partner Solutions Finder and proof of implementation of this process; including at least 10 customer responses. | |
| **3.0 AWS Nonprofit Web Presence and Thought Leadership** | | **Met Y/N** |
| **3.1 Partner AWS Landing Page** | An APN Partner's internet presence specific to their AWS Nonprofit Solutions provides customers with confidence about the APN Partner's Nonprofit capabilities and experience. | |

| | | |
|---|---|---|
| | APN Partner must have an AWS Landing Page that describes their AWS Nonprofit solution, public AWS Case Studies, technology partnerships, and any other relevant information supporting the Partner's expertise related to Nonprofit and highlighting the partnership with AWS.<br><br>This AWS-specific Nonprofit page must be accessible from the APN Partner's home page. The home page itself is not acceptable as an AWS Landing Page unless APN Partner is a dedicated Nonprofit Technology company and home page reflects APN Partner's concentration on Nonprofit. | |
| **3.2 Nonprofit Thought Leadership** | AWS Nonprofit Competency Partners are viewed as having deep domain expertise in Nonprofit, having developed innovative solutions that leverage AWS services.<br><br>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 Nonprofit. Links must be provided to examples of materials published within the last 12 months. | |
| **4.0 Business Requirements** | | |
| **4.1 Field-Ready Toolkits** | Partner has field- ready documentation and seller toolkits including a clear product value proposition that can be articulated to the AWS sales organization with all relevant information needed to determine fit for a customer opportunity (e.g., sales collateral, presentation, and customer use cases).<br><br>Evidence must be in the form of sales collateral including a presentation, one-pager, and use-case checklist. | |
| **4.2 Product Support/Help Desk** | Partner offers their own product and customer support via web chat, phone, or email support to customers.<br><br>Evidence in the form of description of support offered to customers for their product or solution. | |
| **4.3 Product is listed on AWS Marketplace.** | Partner makes solution available via AWS Marketplace.<br><br>☐ Yes<br>☐ No<br><br>Note: Response to this question does not affect the outcome of the validation. | |
| **4.4 Sales Compensation for AWS Deals** | Partner has sales compensation plans for their sellers regarding AWS deals.<br>☐ Yes<br>☐ No<br>☐ Explain: _____<br><br>Note: Response to this question does not affect the outcome of the validation. | |
| **4.5 Joint AWS/Partner Wins** | Partner has process to document and publicize joint wins.<br><br>Evidence in the form of verbal description of process. | |
| **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 to the requirements of the AWS Nonprofit Technology Partner Validation Checklist.<br>▪ APN Partner must complete all sections of the checklist.<br>▪ Completed self-assessment must be emailed to **competency-checklist@amazon.com** using the following convention for the email subject line: "[APN Partner Name], Nonprofit Competency Technology Partner Completed Self-Assessment."<br>▪ It is recommended that APN Partner has their Partner Solutions Architect or Partner Development Manager (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. | |

# Nonprofit Competency Technology Partner Validation Checklist

| Technical Validation | | Applies to: Multi-tenant SaaS | Single-tenant SaaS | Managed Service | Customer-Deployed: | Met Y/N |
|---|---|---|---|---|---|---|
| **Required Documentation**<br>The baseline review is a set of items from the AWS Well-Architected Review deemed critical for the success of a technology partner solution that is built on or integrated with AWS. | | | | | | |
| **Architecture Diagram** | ☐ Shows the major elements of the architecture, and how they combine to provide the Partner Solution to customers<br>☐ Shows all of the AWS services used, using the appropriate AWS service icons.<br>☐ Shows the how the AWS services are deployed, including, VPCs, AZs, subnets, and connections to systems outside of AWS.<br>☐ Shows the systems is highly available and that there are no single point of failures.<br>Includes elements deployed outside of AWS, e.g. on-premises components, or hardware devices. | Yes – one for the whole solution and one for each AWS Case Study. Must meet 100% of requirements. | Yes – one for the whole solution and one for each AWS Case Study. Must meet 100% of requirements. | Yes – one for each AWS Case Study. Must meet 100% of requirements. | Yes – one for each AWS Case Study. Must meet 100% of requirements. | |
| **Deployment Guides** | See "Baseline Requirements for Deployment Guides.docx" | No | No | No | Yes – one for the solution. Must meet 100% of requirements. | |
| **1.0 Baseline**<br>**The baseline review is a set of items from the AWS Well-Architected Review deemed critical for the success of a technology partner solution that is built on or integrated with AWS.** | | | | | | |
| **1.1 AWS Business Support is enabled for the AWS Account** | Business Support has not been enabled. Business Support (or greater) is an APN 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 | Yes | No | |
| **1.2 AWS account root user is not used for routine activities** | The AWS account root user must not be used for everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks. To view the tasks that require you to sign in as the AWS account root user, see AWS Tasks That Require Root User. For a tutorial on how to set up an administrator for daily use, see Creating Your First IAM Admin User and Group. | Yes | Yes | Yes | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **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 | Yes | Yes | |
| **1.4 Multi-Factor Authentication (MFA) has been enabled on the AWS account root user** | 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 | Yes | Yes | |
| **1.5 CloudTrail is enabled for all AWS accounts in every region** | 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 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 | Yes | No | |
| **1.6 CloudTrail S3 log bucket has Versioning or MFA Delete enabled** | CloudTrail log bucket contents must be protected with versioning or MFA Delete. | Yes | Yes | Yes | No | |
| **1.7 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 | Yes | No | |
| **1.8 IAM credentials are** | You must change your passwords and access keys regularly, and make sure that all IAM users in your account do | Yes | Yes | Yes | No | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **rotated regularly** | 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 so. For more information about rotating access keys for IAM users, see Rotating Access Keys. | | | | | |
| **1.9 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 | No | |
| **1.10 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 | Yes | No | |
| **1.11 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 | Yes | Yes | Yes | No | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions. | | | | | |
| **1.12 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 | Yes | |
| **1.13 All credentials are encrypted at rest** | The baseline requirement is to ensure the encryption of any credentials at rest. | Yes | Yes | Yes | Yes | |
| **1.14 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 ideal 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 | Yes | Yes | |
| **1.15 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 | Yes | Yes | |
| **1.16 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 | Yes | Yes | |
| **1.17 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 | Yes | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **1.18 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 | Yes | Yes | |
| **1.19 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 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 | Yes | Yes | |
| **1.20 S3 buckets have not been misconfigured to allow public access.** | You must ensure that buckets that should not allow public access are properly configured to prevent public access. By default, all S3 buckets are private, and can only be accessed by users that have been explicitly granted access. Most use cases won't require broad-ranging public access to read files from your S3 buckets, unless you're using 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. | Yes | Yes | Yes | Yes | |
| **1.21 A monitoring mechanism is in place to detect when S3 buckets or objects become public** | You must have monitoring or alerting in place to identify when S3 buckets become public. One option for this is to use Trusted Advisor. Trusted Advisor checks buckets in Amazon Simple Storage Service (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 Trusted Advisor check examines explicit bucket permissions and associated bucket policies that might override the bucket permissions. | Yes | Yes | Yes | No | |
| **2.0 Security**<br>The security pillar focuses on protecting information & 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. | | | | | | |
| **2.1 AWS Access Keys only used by interactive users** | No AWS Access Keys should be in use, except in the following cases:<br>1. Used by humans to access AWS services, and stored securely on a device controlled by that human.<br>2. Used by a service to access AWS services, but only in cases where: a) It is not feasible to use an EC2 instance | Yes | Yes | Yes | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | role, 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. | | | | | |
| **2.2 EC2 security groups are tightly scoped** | All 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 VPC, 2. Implementing Security Groups to restrict traffic within the VPC, and 3. In all cases, allow only the most restrictive possible settings. | Yes | Yes | Yes | Yes | |
| **2.3 A monitoring mechanism is in place to detect changes in EC2 instances and Containers** | Any changes to your 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 EC2 instances or Containers used in the solution. 2 Store data recording these changes in a durable location, external to the 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 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 EC2 instances or Containers. | Yes | Yes | Yes | No | |
| **2.4 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 | Yes | Yes | |
| **2.5 All sensitive data is encrypted** | All customer data classified as sensitive is encrypted in transit and at rest. | Yes | Yes | Yes | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **2.6 All data in transit is encrypted** | All data in transit across a VPC boundary is encrypted. | Yes | Yes | Yes | Yes | |
| **2.7 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 a partner solution such as HashiCorp Vault. | Yes | Yes | Yes | Yes | |
| **2.8 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 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. | Yes | Yes | Yes | No | |
| **3.0 Reliability**<br>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. | | | | | | |
| **3.1 Network connectivity is highly available** | Network connectivity to the solution must be highly available. If using VPN or 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 | No | |
| **3.2 Solution is resilient to availability zone disruption** | The solution must continue to operate in the case where all of the services within a single availability zone have been disrupted. | Yes | Yes | Yes | Yes | |
| **3.3 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 | Yes | Yes | |
| **3.4 Disaster Recovery (DR) plan includes recovery to another AWS account** | Your DR plan must include a strategy for recovering to another AWS account, and you 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 | Yes | No | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **4.0 Performance Efficiency**<br>The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve. | | | | | | |
| **4.1 Infrastructure scaling mechansims 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 | Yes | Yes | |
| **5.0 Operational Excellence**<br>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. | | | | | | |
| **5.1 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 to make routine changes to the production AWS infrastructure. | Yes | Yes | Yes | Yes | |
| **5.2 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 to must not be used to deploy updates in the AWS infrastructure. | Yes | Yes | Yes | Yes | |
| **5.3 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 | Yes | Yes | |
| **5.4 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 | Yes | Yes | |
| **5.5 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. | Yes | Yes | Yes | No | |

# AWS Resources:

AWS Well Architected Website
https://aws.amazon.com/architecture/well-architected/

AWS Whitepapers
https://aws.amazon.com/whitepapers/

APN Blog
https://aws.amazon.com/blogs/apn/

AWS Blog
https://aws.amazon.com/blogs/