AWS Foundational Technical Review Guide

September 2021

aws partner network

Table of Contents

Introduction

The AWS Foundational Technical Review (FTR) enables AWS Partners to qualify their software products that run on or integrate with AWS. It defines a set of required best practices based on the AWS Well-Architected Framework and standards for evaluating the systems architecture, operational practices, and AWS resource configurations of Partner offerings.

We recommend AWS Partners complete an FTR for all software products they sell that run on or integrate with AWS. After completing an FTR your offering will be listed in the AWS Partner Solutions Finder and you will have access to use AWS badging to promote your product. An FTR is also a prerequisite for many other AWS Partner Network (APN) programs such as AWS Competency and AWS Service Ready.

This guide provides guidance for reviewing your software products and detailed instructions for completing an FTR.

Process Overview

The process to complete an FTR consists of three high level steps.

Step 1: Review your architecture and operational practices

Step 2: Prepare the required documentation and assets

Step 3: Submit your request through AWS Partner Central

The specific activities and requirements for each of these steps depends on the architecture and deployment model of your product.

Using the AWS Well-Architected Framework

The requirements of the FTR are based on a subset of the best practices defined in the AWS Well-Architected Framework. The only mandatory requirements for completing an FTR are the ones defined in the FTR Validation Checklists; however, we strongly recommend that all AWS Partners review their architecture and operational practices against the entire Well-Architected Framework. You can complete an AWS Well-Architected Framework Review (WAFR) yourself using the AWS Well-Architected Tool available at no cost in the AWS Management Console, or you can engage a Well-Architected partner to help you implement best practices, measure the state of your workloads, and make improvements where assistance is required.

When conducting a review with the AWS Well-Architected Tool, you can use the FTR lens in order to include the specific FTR requirements for components you host in your review. If your software product is deployed and managed by the customer, you should consider the questions in the Well-Architected Framework from the perspective of your customers. Many questions (e.g. those about AWS account management) may not be applicable, but you should review your product and its documentation to determine how easily customers can follow the Well-Architected best practices when running your software.

Once you have completed an AWS Well-Architected Framework Review, you should remediate any issues related to the FTR requirements immediately. Prioritize addressing other issues identified based on your risk assessment and business needs.

Alternative Architectural Review Standards

Many Partners have also defined their own internal architectural standards tailored to the needs of their business. In these cases, we encourage you to review any gaps between your standard and the Well-Architected Framework and determine which best practices make sense to incorporate into your own reviews. The FTR does not require or expect you to do additional Well-Architected Framework Reviews if you already have a standard, documented process in place for reviewing your products against your own standard.

Offering Component Types

The specific process and requirements for the FTR will depend on how and where the components of your product are deployed and managed. For the purposes of the FTR, components are categorized based on the following attributes:

1. Who is responsible for deploying and managing the software (i.e. the AWS Partner or the customer)

2. Where the software runs (i.e. on AWS or in another environment)

Most software products have only a single component type. For example, a SaaS application running on AWS would be considered Partner Hosted on AWS even if that application has multiple microservices or APIs spread across multiple AWS accounts. Similarly, a product deployed on Amazon EC2 instances running in the customer's account that has multiple types of nodes and data stores would be considered a single Customer Deployed component.

In cases where your product consists of both partner hosted and customer deployed components, you will need to fulfill all requirements relevant to each component type as described below.

1. Partner Hosted on AWS

Partner Hosted on AWS components are deployed, owned, and managed by you, the AWS Partner. Typically, these are Software as a Service (SaaS) applications running in an AWS account you own, although any cases where you are deploying and running software you own on behalf of your customers falls into this category.

If you are deploying and managing software you do not own or did not write, your offering should be classified as a managed service. In these cases, you should not complete an FTR. Please contact your Partner Development Manager (PDM) to discuss the details of your offering.

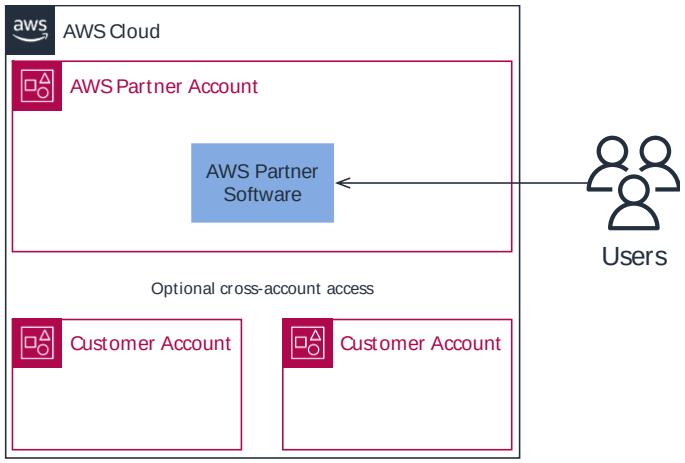

Figure 1 – Example Partner Hosted on AWS component

2. Partner Hosted outside AWS

Partner Hosted outside AWS components are deployed, owned, and managed by you, the AWS Partner on infrastructure running outside AWS. In all cases these components must directly integrate the customer's AWS environment by assuming a IAM role in the customer's account, serving as a SaaS Partner event source for Amazon EventBridge, or making direct network connections with customers' AWS resources.

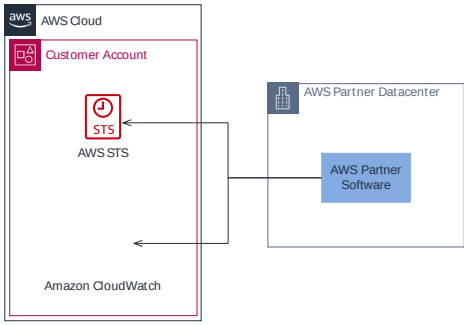

Figure 2 - Example Partner Hosted outside AWS component

3. Customer Deployed on AWS

Customer Deployed on AWS components run on instances, containers, or functions in a customer's AWS account. These may be Amazon Machine Images (AMIs) distributed through AWS Marketplace, or other packaged software that is licensed for customers to run on compute resources they own. The customer is responsible for deploying and operating the software, while you as the AWS Partner provide documentation on how to properly configure and run the software on AWS.

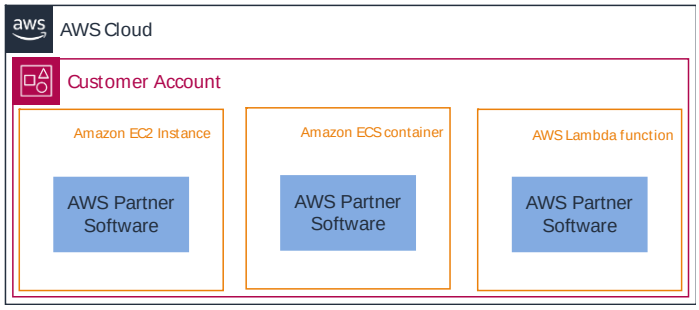

Figure 3 – Example Customer Deployed on AWS component

4. Customer Deployed outside AWS

These components are deployed and managed by the customer on infrastructure outside of AWS and integrate with AWS services or other components running on AWS either in the customer's or AWS Partner's account. Common examples of these types of components include software running on IoT devices that connect to AWS IoT and appliances that run in the customer's on-premises environments and synchronize data to AWS.

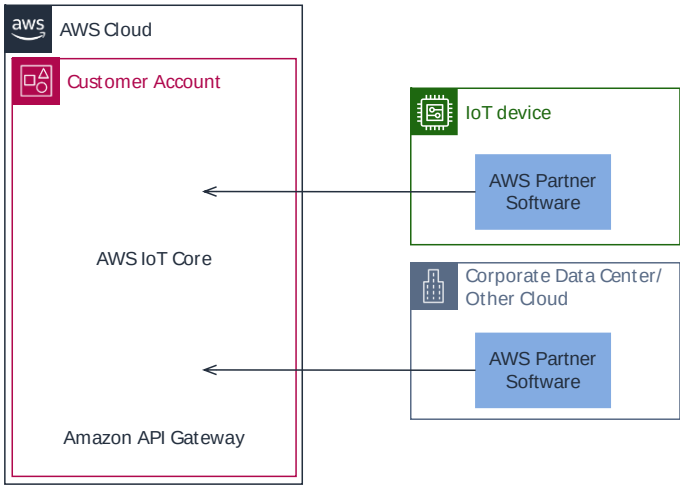

Figure 4 – Example Customer Deployed outside AWS component

Other Component Types

If you have a software product that does not have components that fall into one of the above categories, but you would still like to promote it through the APN and its programs, please contact your PDM in order to determine how best to proceed with an FTR.

Reviewing a Partner Hosted Component Running on AWS

You can view the technical requirements for completing your review in the FTR Partner Hosted Validation Checklist.

In order to complete an FTR for a software product that includes a Partner Hosted component running on AWS, you will provide two pieces of documentation: a security report from an automated tool and a completed self-assessment. Both the report and self-assessment should be scoped to all AWS accounts that you use to process customer data.

To complete the automated security report, we recommend you use an AWS Security Competency or AWS Cloud Management Tools Competency Partner Solution that supports the CIS AWS Foundations Benchmark such as nOps. nOps is an AWS Partner solution with a dedicated FTR feature that allows you to complete the automated and manual assessment components through a single interface. If you would like to use this tool, please follow the nOps FTR documentation. You can also use AWS Security Hub or any other tool that can evaluate your AWS accounts against the CIS AWS Foundations Benchmark.

After you submit your documents, AWS will review them offline and approve your FTR if you have met all the requirements. If there are any issues identified with your submissions we will provide feedback over email, and you can resubmit your documents after addressing any concerns.

Note
If you are unable to provide a CIS AWS Foundations Benchmark report for any reason, you can still request a review by submitting only the self-assessment. This will result in an AWS Partner Solutions Architect contacting you to schedule a live review call. The fastest way to complete an FTR is using the standard process described below, but you can follow the instructions in the Getting Help section below if you wish to have your software product manually reviewed.

Step 1: Review your AWS accounts against the CIS AWS Foundations Benchmark

You may use any tool that supports the CIS AWS Foundations Benchmark to complete the automated assessment of your AWS environment.

Using your own tooling

If you already have a tool in place that supports this standard, please use it to generate a report following these guidelines:

1. Include all of your Production AWS accounts and AWS Regions (i.e. any account and Region where customer data is stored or processed) in your report. It is ok to submit multiple files.
2. Include all of the required controls in your report.
3. Ensure all required controls are marked as passed before submitting your report.
4. If possible use the comma-separated values (CSV) format. We will accept other report formats, but it may take longer to process your review.
5. Only include CIS AWS Foundations Benchmark controls in the report you submit.

Using AWS Security Hub

If you are not using an AWS Partner solution and would like to use AWS Security Hub to generate the required report, please follow these instructions:

1. Complete all prerequisites for enabling Security Hub. Please note that the prerequisites include enabling AWS Config.
2. Enable Security Hub with the CIS AWS Foundations Benchmark security standard in each account and AWS Region where you handle customer data. It might take a few hours for Security Hub to complete its security checks. **Please note that enabling Security Hub will incur additional costs after the 30-day free trial window as indicated in the Security Hub pricing page.**
3. Once Security Hub completes its security checks, you can view a summary of your findings on the Summary page. Navigate to the 'Security standards' section and click on 'View results' for CIS AWS Foundations Benchmark. Review this summary against the list of required controls below.
4. If any of the required controls are marked as failed, follow the remediation instructions in the AWS Security Hub documentation.

5. Click on the 'Download' button located in the top right corner of the enabled controls list to download your Security Hub report in CSV format. You will be submitting this file along with your attestation worksheet. You will need to repeat this process in each account and AWS Region where you handle customer data.

Required CIS AWS Foundations Benchmark Controls

You must pass all of the following controls in order for your FTR to be approved:

1. CIS 1.1 - Avoid the use of the "root" account
2. CIS 1.13 - Ensure MFA is enabled for the "root" account
3. CIS 1.12 - Ensure no root account access key exists
4. CIS.2.1 - Ensure CloudTrail is enabled in all regions
5. CIS.2.2 - Ensure CloudTrail log file validation is enabled
6. CIS.1.2 - Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
7. CIS.1.4 - Ensure access keys are rotated every 90 days or less
8. CIS 1.22 - Ensure IAM policies that allow full "*:*" administrative privileges are not created
9. CIS1.5 - Ensure IAM password policy requires at least one uppercase letter
10. CIS1.6 - Ensure IAM password policy requires at least one lowercase letter
11. CIS1.7 - Ensure IAM password policy requires at least one symbol
12. CIS1.8 - Ensure IAM password policy requires at least one number

You can find more details about each of these controls in the AWS Security Hub documentation.

If there are cases where your report shows a control as failed, but you have implemented a compensating control, please provide an explanation in your self-assessment worksheet.

Step 2: Complete the Self-Assessment

In addition to the CIS AWS Foundations Benchmark report, you must submit a completed self-assessment worksheet that confirms you are following additional best practices that cannot be validated with a tool.

Note
If you are using nOps, you can complete the self-assessment directly in the tool and submit a single, consolidated report.

To complete the self-assessment

1. Download the self-assessment spreadsheet in Microsoft Excel format.
2. Complete all of the worksheets/tabs.
3. For each technical requirement row, indicate whether you have implemented or completed each of the best practices described using the response column. By answering 'yes' for a given row you are confirming that you are fully complying with the stated requirement for all accounts and environments that process customer data.

Please ensure you have met all requirements before requesting your FTR. If you need assistance remediating any of your issues, please see the Getting Help section below.

Step 3: Request an FTR through AWS Partner Central

After you have created a CIS AWS Foundations Benchmark report and completed the self-assessment, you can submit these documents to AWS for review using AWS Partner Central.

To request an FTR

1. Log in to your Partner Central account.
2. Choose **View My APN Account** on the left-hand side.
3. In the **Offerings** section find the Software Product offering you would like request an FTR for and choose **Edit**.
4. If the Offering does not exist, you can create it by choosing New at the top of the section and completing the required sections on the next screen.
5. In the **Validations** section of the offering, upload your completed self-assessment under **FTR Checklist** and your AWS CIS Foundations Benchmark report under **Security Tool Report**. You may upload multiple files in order to cover all accounts and AWS Regions where you process customer data.
6. If your software product includes a Customer Deployed component, follow the instructions for "Reviewing a Customer Deployed Component" below and upload the files associated with that component as well.
7. Choose **Request Foundational Technical Review**.

Note: The Request Foundational Technical Review button will be disabled until you have uploaded your self-assessment to the FTR Checklist field.

Step 4: Receive Feedback

After you request your review through AWS Partner Central, an AWS Partner Solutions Architect (PSA) will review your submitted documents and contact you via email. If all of your documents are complete and all requirements are met, your FTR will be approved. If there are any issues identified, the PSA will provide you with a list of remediations and guidance for how to complete your FTR. Once you have implemented all remediations and provided confirmation to the PSA, your FTR will be approved. You must complete remediations within 6 months. After 6 months you must submit a new request and meet all requirements on the latest version of the validation checklist. While you complete remediations your review will be marked as Declined.

Reviewing a Partner Hosted Component Running outside AWS

You can view the technical requirements for completing your review in the FTR Partner Hosted Validation Checklist.

The process for reviewing a Partner Hosted Component that runs outside AWS requires a live review with an AWS Partner Solutions Architect (PSA). Complete the following steps to review your product, request a review, and complete your FTR.

Step 1: Complete the Self-Assessment

To complete the self-assessment

1. Download the self-assessment spreadsheet in Microsoft Excel format.
2. Complete all of the worksheets/tabs.
3. For each technical requirement row, indicate whether you have implemented or completed each of the best practices described using the response column and provide a brief explanation of your implementation in the Response column. By answering 'yes' for a given row you are confirming that you are fully complying with the stated requirement for all environments that process customer data.

Step 2: Request an FTR through AWS Partner Central

After you have completed the self-assessment, you can request an FTR using AWS Partner Central.

To request an FTR

1. Log in to your Partner Central account.
2. Choose **View My APN Account** on the left-hand side.
3. In the **Offerings** section find the Software Product offering you would like request an FTR for and choose **Edit**.
4. If the Offering does not exist, you can create it by choosing New at the top of the section and completing the required sections on the next screen.
5. In the **Validations** section of the offering, upload your completed self-assessment under **FTR Checklist**.
6. If your software product includes a Customer Deployed component, follow the instructions for "Reviewing a Customer Deployed Component" below and upload the files associated with that component as well.
7. Choose **Request Foundational Technical Review**.

Note: The Request Foundational Technical Review button will be disabled until you have uploaded your self-assessment to the FTR Checklist field.

Step 3: Complete a live review with an AWS Partner Solutions Architect

After you request your review through Partner Central, a PSA will contact you via email to schedule a review of your software product. During the review they will discuss each of the items on the validation checklist and provide feedback on any identified issues. If there are any issues you will be given guidance on how to remediate those problems. Once you have implemented all remediations and provided confirmation to the PSA, your FTR will be approved. You must complete remediations within 6 months. After 6 months you must submit a new request and meet all requirements on the latest version of the validation checklist. While you complete remediations your review will be marked as Declined.

Reviewing a Customer Deployed Component

You can view the technical requirements for completing your review in the following validation checklists:

- Customer Deployed on AWS FTR Validation Checklist
- Customer Deployed outside AWS FTR Validation Checklist

The FTR for Customer Deployed components evaluates how your software product supports being deployed within a customer's environment. Much of the review is based on the product documentation you provide to customers that explains how to deploy and manage your software on AWS or in another environment. In cases where your software runs outside AWS, the review also evaluates how it integrates with AWS services. While the customer is ultimately responsible for properly configuring and securing their AWS resources, your product must provide the features and documentation that enable customers to implement AWS Well-Architected best practices when deploying your software.

Offerings with AWS Quick Starts

Quick Starts are automated reference deployments built by Amazon Web Services (AWS) solutions architects and AWS Partners. Quick Starts help customers deploy popular technologies on AWS according to AWS best practices. The standards enforced when publishing a Quick Start align to the FTR which means all recently published or updated Quick Starts fulfill all FTR requirements.

If you have an AWS Quick Start for deploying your software product on AWS that was published or updated within the last two years, your FTR can be automatically approved. Please ensure you have the AWS Quick Start URL field completed on the Offering listing in Partner Central and contact your PDM to request that an FTR be created and approved on your behalf.

Partner led deployments in customer environments

In cases where your product is only allowed to be deployed by your own professional services staff, you do not need to provide a customer-facing deployment guide; however, you are expected to have internal documentation, runbooks, or automated deployment scripts that ensure deployments are delivered consistently and in accordance with the FTR requirements. Please provide your internal documentation for review in these cases.

Step 1: Complete the Self-Assessment

To complete the self-assessment

1. Download the self-assessment spreadsheet in Microsoft Excel format.
2. Complete all of the worksheets/tabs.
3. For each technical requirement row, indicate whether you have implemented or completed each of the best practices described using the "Met?" column and provide a direct link or page number reference to the section of your documentation that addresses the requirement.

Step 2: Request an FTR through AWS Partner Central

After you have completed the self-assessment, you can request an FTR using AWS Partner Central.

To request an FTR

1. Log in to your Partner Central account.
2. Choose **View My APN Account** on the left-hand side.
3. In the **Offerings** section find the Software Product offering you would like request an FTR for and choose **Edit**.
4. If the Offering does not exist, you can create it by choosing New at the top of the section and completing the required sections on the next screen.
5. In the **Validations** section of the offering, upload your completed self-assessment under **FTR Checklist**.
6. If your customer deployment guide or other documentation is not available at a publicly accessible URL, upload the relevant documentation under **Customer Deployment Guide**.
7. If your software product includes a Partner Hosted component, follow the instructions for "Reviewing a Partner Hosted Component" above and upload the files associated with that component as well.
8. Choose **Request Foundational Technical Review**.

Note: The Request Foundational Technical Review button will be disabled until you have uploaded your self-assessment to the FTR Checklist field.

Step 3: Receive Feedback

After you request your review through AWS Partner Central, an AWS Partner Solutions Architect (PSA) will review your submitted documents and contact you via email. If all of your documents are complete and all requirements are met, your FTR will be approved. If there are any issues identified, the PSA will provide you with a list of remediations and guidance for how to complete your FTR. Once you have implemented all remediations and provided confirmation to the PSA, your FTR will be approved. You must complete remediations within 6 months. After 6 months you must submit a new request and meet all requirements on the latest version of the validation checklist. While you complete remediations your review will be marked as Declined.

Prior Reviews and Exceptions

Completion of an AWS Well-Architected Framework Review or any other technical validation led by AWS does not guarantee your FTR will be approved. However, if you have recently conducted an architectural review for your software product with an AWS Partner Solutions Architect (PSA) you may be able to work with them to complete an FTR based on the work you have already done. Please contact the PSA who conducted the review to discuss an alternate FTR process.

Getting Help

If you have issues completing the review or remediating any issues you discovered while conducting your self-assessment and would like to meet with an AWS Partner Solutions Architect (PSA), you can request a review through AWS Partner Central even if you have not yet met all the requirements.

To request a review by a PSA:

1. Complete the self-assessment based on the types of components in your software product. Please provide details about any items you would like additional guidance on in the "Response" column.
2. Log in to your Partner Central account.
3. Choose **View My APN Account** on the left-hand side.
4. In the **Offerings** section find the Software Product offering you would like request an FTR for and choose **Edit**.
5. If the Offering does not exist, you can create it by choosing New at the top of the section and completing the required sections on the next screen.
6. In the **Validations** section of the offering, upload your completed self-assessment under **FTR Checklist**.
7. (Optional) Upload an architecture diagram representing how your software product is deployed on AWS under **Architecture Diagram**.
8. Choose **Request Foundational Technical Review**.

After you request the review through AWS Partner Central, a PSA will contact you via email and provide an option to schedule a live review of your product.