AWS Foundational Technical Review Guide

Nov 2024

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 solutions.

An FTR is not required to list a partner solution in AWS Marketplace. However, we recommend that AWS Partners complete an FTR for all software products they want to co-sell with AWS and join ISV co-sell program (ISV-Accelerate), as well as those that run on or integrate with AWS. Completing an FTR allows your solution to be listed in the AWS Partner Solutions Finder and grants you access to AWS badging to promote your product. Additionally, an FTR is a prerequisite for many AWS Partner Network programs, including AWS Competency, Service Ready Specializations, and ISV- Accelerate. If you are not interested in these programs and benefits, you do not need to complete an FTR. The FTR is valid for three years from the approval date.

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

AWS Foundational Technical Review (FTR)

Overview

What is an FTR?

An FTR's primary purpose is to ensure Software products offered by AWS Partners have implemented a basic set of architectural, security, and operational best practices. The FTR defines a set of objective criteria based on the AWS Well-Architected framework. This serves as a gate to ensure the products AWS endorses to customers have appropriate mitigations for the most common risks that impact end customers.

What are the benefits of doing an FTR?

Completing an FTR is one of the primary requirements for Partners to move to the Validated stage within the AWS Partner Network Software Path. After receiving FTR approval, Partners are eligible to go to market with AWS.

FTR is a self-service review that is valuable at any stage of your cloud journey. Partners can leverage FTR process to help identify and remediate risks for the benefit of your end customer.

Software Path Validated Partner Benefits

COMPLETE A FOUNDATIONAL TECHNICAL REVIEW FOR YOUR SOFTWARE FOR ACCESS TO:

ACE

ACE Referrals
APN Ambassador
AWS Competency
AWS Partner badge
Sponsor packages*
Press Release eligibility
Qualified software badge
Partner Discovery Portal listing
Partner Opportunity Acceleration funds
Partner Solution Finder listing
Marketing Central partner ready campaigns

Programs

AWS Service Ready
ISV Accelerate
ISV Workload Migration
Public Sector Partner
Well-Architected Partner

How can I conduct FTR?

To conduct an FTR, Partners must submit a self-assessment checklist and security tool report (if applicable). A security report is only required for Partner Hosted solutions, and it can be generated automatically using AWS SecuityHub or other tools. Please review the FTR Guide for complete requirements and instructions for conducting FTR.

Getting Started

- ❑ Allocate a technical resource who is familiar with your AWS environment.
- ❑ Download FTR checklist and User Guide.
- ❑ Request an FTR.
  - ❑ Login to Partner Central > Build> Solutions > View Details of existing or Create solution > Request validation. Upload the self-assessment checklist & Security Tool Report (if applicable) to request a FTR.
- ❑ The system will review your submitted documents and provide a result in 30 minutes. If a CIS benchmark report and Architecture Diagram (required) are provided, and all requirements in the self-assessment are met, the FTR will be approved automatically. Otherwise, a Partner Solutions Architect will contact you to provide details on the outcome and will work with you to remediate issues.

What are the next steps?

Step 1

Identify the **appropriate** FTR checklist to conduct a self-assessment for an solution

Step 2

Request technical owner(s) in your company to **answer checklist questions**

Step 3

Submit a completed self-assessment checklist in Partner Central, and also upload an architecture diagram (required) and CIS benchmark report.

Step 4

If the FTR is not auto-approved, an AWS PSA will get in touch with you **via email for next**

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.

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.

FTR WAFR Waiver: **If you have completed an AWS WAFR led by an AWS employee in the past 12 months which shows zero outstanding high-risk issues (HRIs) in the Security, Operational Excellence, and Reliability pillars, you do not need to complete all FTR controls.** Please complete a self-assessment spreadsheet affirming your compliance with the HOST-001, SUP-001, WAFR-001, and WAFR-002 requirements and upload an exported WAFR report. Your FTR renewal date will be set to 36 months from the data of the WAFR.

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.

Process Overview

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

Step 1

Review your architecture and operational practices using the latest FTR checklist. Requirements have changed

Step 2

Prepare the required documentation and assets. Previous documentation cannot be provided by AWS.

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.

FTR Renewal Guidance

Partners are required to submit a new FTR in order to renew their "Approved" FTR status every 3 years. Partners on the Software Path must have at least one current FTR in order to remain in the Validated+ stage of the Software Path. If your account does not have any solutions with an active Approved FTR, you may lose APN benefits including, but not limited to:

- *Qualified Software* solution badge
- solution listed in the Partner Solution Finder (PSF), and Partner Discovery Portal (PDP) *
- ACE Eligibility
- Impact to co-sell and inability to receive AWS Originated Opportunities

  Note: Both ACE and ISVA have additional entrance criteria beyond a valid FTR
- Access to AWS ISV Accelerate Program
- Access to AWS Competencies and Service Ready Specializations

We've streamlined the FTR process to make it even more partner-friendly. If you conducted the FTR or Technical Baseline Review (TBR) process two years ago, we kindly request that you revisit this review to ensure alignment with the latest requirements.

*Partner Discovery Portal is an internal discoverability for AWS Sellers to find and understand your product/solution and match to AWS customer opportunities

FAQs

Will I be notified about expiring FTRs?

Yes, we will notify the Alliance Lead registered in Partner Central 90, 60, 30 days before FTR expires.

Do I need to submit a full FTR for renewal?

Yes, you must submit a completed self-assessment that covers all current requirements for the FTR. This is to confirm your solution continues to meet all existing and new requirements in the current version of the checklist.

When should I initiate FTR renewal?

AWS recommends that you begin working on the renewal at least 90 days prior to FTR expiry. This ensures you have enough time to remediate any findings identified during self-assessment and AWS review.

What happens if my FTR has expired?

Partners who no longer have a valid FTR are at risk of losing APN benefits associated with their participation in programs, such as ISV Accelerate.

solution 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 on the AWS Partner on AWS. All critical application components must be hosted on AWS. You may use external providers for edge services such as content delivery networks (CDNs) or domain name system (DNS), or corporate identity providers. 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 solution 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 solution.

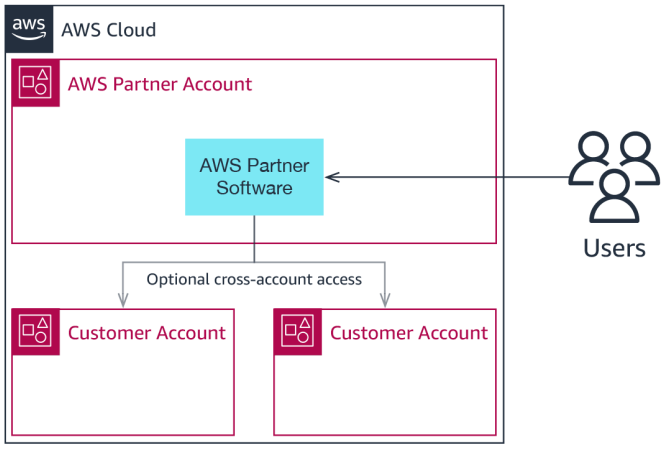

Figure 1 – Example Partner Hosted on AWS component

2. Partner Hosted outside AWS

Partner Hosted outside AWS components are deployed, owned, and managed by you, the AWS Partner using infrastructure you own and manage (e.g., hosted in a data center you own or a co-location facility) in addition to AWS services. In all cases, these components

must directly integrate the customer's AWS environment by assuming an 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.

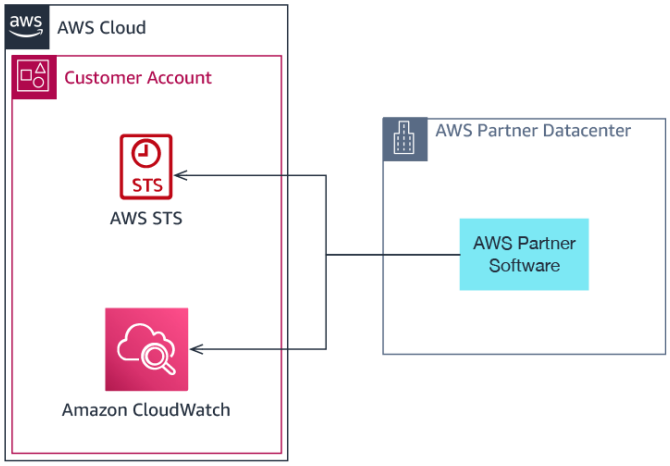

Figure 2 - Example Partner Hosted outside AWS component

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.

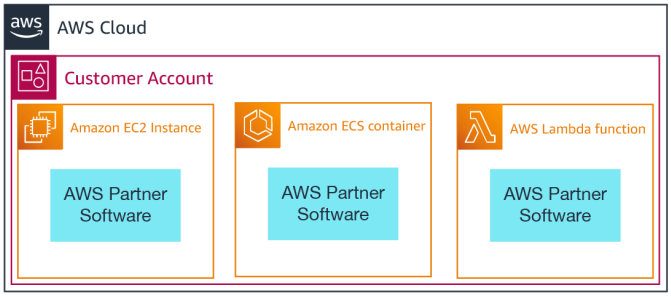

Figure 3 – Example Customer Deployed on AWS component

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.

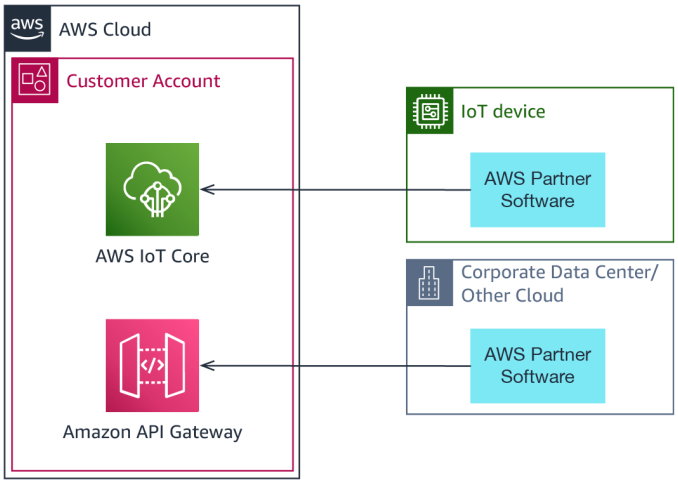

Figure 4 – Example Customer Deployed outside AWS component

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 AWS Partner Network 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. You can 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.

Partner Hosted Solutions on AWS Marketplace

Partner Hosted solutions on AWS Marketplace must follow the standard FTR process for Partner Hosted component described in the Partner Hosted Component section.

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

You may use any tool that supports the CIS AWS Foundations Benchmark 1.4 or 3.0 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 okay 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.

NOTE: In order to use AWS Security Hub to generate an CIS AWS Foundations Benchmark report, you must also enable resource recording in AWS Config which will incur costs. Review the AWS Config pricing page and the AWS Security Hub pricing page before enabling these services. Please also consider only enabling recording for the resource types required for CIS Controls if you want to minimize costs.

Required CIS AWS Foundations Benchmark v3.0 Controls

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

1. CIS 1.5/Security Control IAM.9 - Ensure MFA is enabled for the 'root' user account
2. CIS 1.4/Security Control IAM.4 - Ensure no 'root' user account access key exists
3. CIS 1.10/Security Control IAM.5 - Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
4. CIS 1.14/Security Control IAM.3 - Monitor and secure static AWS Identity and Access Management (IAM) credentials
5. CIS 5.3/ Security Control EC2.54 and CIS 5.2/ Security Control EC2.53- Implement the least permissive rules for all Amazon EC2 security groups.
6. CIS 1.8/Security Control IAM.15 - Ensure IAM password policy requires minimum length of 14 or greater
7. CIS 1.9/Security Control IAM.16 - Ensure IAM password policy prevents password reuse
8. CIS 5.3/Security Control EC2.2 - Ensure the default security group of every VPC restricts all traffic
9. CIS 1.2/ Security Control Account.1 - Configure AWS account contacts.

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.

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. On the top navigation, choose **Build -> Solutions**.
3. In the **Solutions** section, find the Software Product solution you would like request an FTR for and check the circle, then click **View details**.
    a. If the solution does not exist, you can create it by choosing **Create solution** at the top right of the section and completing the required sections on the next screen.
4. In the **Request validation** section of the solution, 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.
5. 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.
6. Choose **Request Validation**.

NOTE: The Request Validation button will be disabled until you have uploaded files.

Step 4: Receive Feedback

After you request FTR validation through AWS Partner Central, the system will review your submitted documents and provide status in 30 minutes. If a CIS benchmark report and Architecture Diagram are provided, and all requirements in the self-assessment are met, the FTR will be approved automatically and the FTR status will be updated accordingly.

If any clarification is needed from your application, an AWS Partner Solutions Architect (PSA) will review your submitted documents and contact you via email. 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 Remediation in progress.

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.
4. In the **Request validation** section of the solution, upload your completed self-assessment under **FTR Checklist.**
5. 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.
6. Choose **Request Validation**.

NOTE: The Request Validation button will be disabled until you have uploaded files.

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 your Partner Central account.
2. On the top navigation, choose **Build -> Solutions**.
3. In the **Solutions** section, find the Software Product solution you would like request an FTR for and check the circle, then click **View details**.
    a. If the solution does not exist, you can create it by choosing **Create solution** at the top right of the section and completing the required sections on the next screen.

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.

AMI and Container Based Products on AWS Marketplace

AMI and Container based products listed on AWS Marketplace (AWS MP) are validated against AWS MP requirements before listing. An FTR for these products will be approved upon request with no further validation. Please submit an FTR using the self-assessment on this checklist for these products.

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 from the validation checklist appropriate for your workload.
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. On the top navigation, choose **Build -> Solutions**.
3. In the **Solutions** section, find the Software Product solution you would like request an FTR for and check the circle, then click **View details**.
    a. If the solution does not exist, you can create it by choosing **Create solution** at the top right of the section and completing the required sections on the next screen.
4. In the **Request validation** section of the solution, upload your completed self-assessment under **FTR Checklist.**
1. If your customer deployment guide or other documentation is not available at a publicly accessible URL, upload the relevant documentation under **Customer Deployment Guide**.
2. 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.
3. Choose **Request Validation**.

NOTE: The Request Validation button will be disabled until you have uploaded files.

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.

Reviewing Data and Machine Learning Products on AWS Marketplace

Data and Machine Learning Products on AWS Marketplace are validated against AWS MP requirements before listing and meet all the requirements for FTR. FTR for these products will be approved upon request with no further validation. Please submit an FTR request using the self-assessment on this checklist for these products.

Reviewing AWS Direct Connect Products

Direct connect products are reviewed using this checklist. Please submit an FTR request using the self-assessment on this checklist for Direct Connect products.

Best Practice to Expedite FTR Review

Tip 1: Upload Architecture diagram in your FTR submission

Tip 2: Submit FTR with architecture diagram in jpeg / png format and security report csv file against CIS AWS Foundations Benchmark will accelerate automated 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. On the top navigation, choose **Build -> Solutions**.
4. In the **Solutions** section, find the Software Product solution you would like request an FTR for and check the circle, then click **View details**.
    a. If the solution does not exist, you can create it by choosing **Create solution** at the top right of the section and completing the required sections on the next screen.
5. In the **Request validation** section of the solution, upload your completed self-assessment under **FTR Checklist**.
6. Upload an architecture diagram representing how your software product is deployed on AWS under **Architecture Diagram (required),** and also upload a CIS Benchmark Report under Security tool report
7. Choose **Request Validation.**

NOTE: The Request Validation button will be disabled until you have uploaded files.

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.

Thank you!