# Assessment

The assessment phase is also referred to as Discovery & Insights. This phase has been designed to standardize how Microsoft delivery resources engage with customers to get insights from several Azure critical areas by leading a set of customer interviews, workload insights, and (where applicable) whiteboarding sessions. The Well-Architected Assessments target a specific Azure workload and share a common delivery approach with focus on specific critical areas within the specific tenant (cost, reliability, operations, security) of the framework.

In addition to the interview sessions, Microsoft delivery resources will use the Azure Monitor security workbook template, and potentially other tools as applicable, to gain critical insights into customer strengths and improvement areas for the in-scope workload.

At the end of the Discovery & Insights delivery, Microsoft delivery resources will build an improvement plan of activities for future work based on identified recommendations and optimizations (fit/gap analysis).

## \*\*Engagement Start\*\*

The start of the assessment should include:

- Round-table introductions

- Re-hash parts of the scoping call to ensure participants are clear on delivery flow, logistics, expectations, special topics of interest, and deliverables

- The customer should provide the CE an overview of the scoped workload to understand its purpose and its architecture in Azure

- Azure Monitor workbook deployment and filtering

Use the `Well-Architected Security Assessment - Kickoff.pptx` deck from the [IPKit](https://aka.ms/waf/wasa) as a back-drop for the below activities.

### \*\*Round-table Introductions\*\*

At the beginning of the assessment phase, kick off the engagement by introducing yourself, the assigned CSA, and CSAM. Seek introductions from the customer stakeholders to understand who is responsible for what aspect of IT operations and the workload being assessed. Be mindful of the number of customer stakeholders in the call and forgo these intros for the sake of time if needed.

### \*\*Re-hash parts of the scoping call\*\*

Spend a short amount of time to re-hash parts of the scoping call to ensure participants are clear on delivery flow, logistics, expectations, special topics of interest, and deliverables. This is also an opportunity to reiterate the expected customer stakeholders needed to respond to the Q&A.

### \*\*(Optional) Well-Architected Framework Overview\*\*

A set of slides are provided to give an overview of WAF, the security pillar of WAF and how this assessment aligns to its guidance. Consider spending a short amount of time grounding the customer in the theory and design principals WAF security. Educate that WAF is an inside-out lens focusing on the workload architecture and that its only part of the story of how well architected a workload is.

### \*\*(Optional) Enterprise Scale / Landing Zones Overview\*\*

A set of slides are provided to give an overview of Enterprise-scale landing zones. Consider spending a short amount of time grounding the customer to the outside-in lens on the role and importance of WAF/CAF and landing zones for workload architecture (Enterprise Scale). This part will give context when the question comes up in the survey on whether customer designed and deployed landing zone for the workload being reviewed.

### \*\*Workload Overview\*\*

The customer should provide the CE an overview of the scoped workload to understand its purpose and its architecture in Azure. Take the time to open the shared architecture document (if there is one to understand the application purpose, architecture, authentication and data flows). Ask questions and take notes as applicable to familiarize yourself with the scoped application/workload. If the customer can't provide an architecture diagram, consider whiteboarding the workload design with them (high level).

### \*\*Azure Monitor workbook deployment and filtering\*\*

As part of this assessment, the WAF Security workbook has to be deployed. Walk the customer through filtering the report pages to zero in on the scoped workload. This will depend on how the workload is architected across resources, resource groups, and subscriptions. Filtering on resource tagging may be needed to ensure the recommendations surfaced by Advisor and Microsoft Defender for Cloud are for the scoped workload.

#### Workbook Pre-requisites

The following Azure resource providers must be registered on the in-scope subscriptions:

- Microsoft.Advisor

- Microsoft.ResourceHealth

- Microsoft.Security

A cloud account with Built-in Reader role assigned to all in-scope subscriptions, or their parent management group.

[Optional] Monitor Contributor role to save workbook from template.

> [!NOTE]

> Saving the workbook is not required to view and export the insights it surfaces. Monitor Contributor role to save workbook from template if customer wants to continue using the workbook post engagement.

#### Workbook Deployment Guide

The following resources can be used to deploy the workbook into Azure monitor:

- [JSON Deployment guide](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/workbooks-automate#azure-resource-manager-template-for-deploying-a-workbook-in) - A guide to create workbooks using a \*\*JSON Template\*\*.

- [ARM Template Deploy Guide](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/workbooks-automate#azure-resource-manager-template-for-deploying-a-workbook-instance) - A guide to deploy the workbook as an \*\*ARM Template\*\*.

- [Security WorkBook.json](https://microsoft.sharepoint.com/teams/ASDIPRelease/IP%20Release/Forms/AllItems.aspx?viewid=971b6985%2D5ac6%2D47e5%2Da6dc%2D5c0664b149a9&id=%2Fteams%2FASDIPRelease%2FIP%20Release%2FSecure%20Infrastructure%2FAssessment%20Program%2FWell%2DArchitected%20Security%20Assessment%2F4%2DDelivery%20Artifacts%2F1%2DAzureMonitorWorkbook) - This workbook will present various security related details from Microsoft Defender for Cloud and Azure Advisor.

#### Optional Network Security Dashboard Workbook

The IPKit also contains a link to the [Network Security Dashboard](https://aka.ms/DeployNetSecWorkbook) workbook on GitHub. This additional workbook may be used to get additional insights into network related workload resources. However, this workbook \*\*does not provide filtering capabilities\*\* like the WASA Security workbook. If you decide to use it make sure to \*\*focus only on the workload resources that are in scope\*\*. This workbook may provide additional value and benefit for the customer.

## Azure Well-Architected Review Survey

Examine your workload through the lenses of the security pillar. To conduct the assessment, please visit the [Azure Well-Architected Review](https://docs.microsoft.com/assessments) website.

Interviews are a critical part of the engagement, where the main goal is to get as much information and insights from the customer for the scoped Azure workload as possible. It’s important to have the correct customer stakeholders to ensure accurate responses to collect rich and meaningful responses for the Azure Well-Architected Review.

The spirit of these customer interviews is to have open conversations about each of the critical areas instead of trying to ask a bunch of questions to get binary answers that might miss a lot of other important details. Try to identify strengths, challenges, and opportunities.

Do not just read the assessment questions/choices line by line. Ask them in your words. Extend them with examples, provide context and background information why this question does matter and what the impact is. Drive open-ended questions to engage the customer to speak and share the details of the Azure workload. Encourage the customer to use the whiteboard to visualize their explanation.

Look for hard and easy decisions to make – both extremes can be the result of organizational issues. Ensure to timebox the topics and use `parking lot` for challenging discussions.

> [!NOTE]

> There can be situations where the necessary stakeholder is not available to answer a question and delivery continues forward without responding to a question. Ensure all questions are responded to before submitting the survey.

### Perform the assessment and generate the csv report

- Navigate to the [Azure Well-Architected Review](https://docs.microsoft.com/assessments) website.

- When prompted, login with your B2B account (if you have one) or have the customer login with their credentials. You may have to create an account if one doesn't already exist.

- Once you are logged in, under available assessments, select the Azure Well-Architected Review.

- Upon doing this, you will be presented with 2 options - Create a new assessment or create a milestone. Select create a new assessment.

- Give the assessment an appropriate name or continue with the default name that is provided.

- [Optional - \*\*see Important call out below\*\*] In the Azure Advisor section, sign in with the Azure credentials and select the Azure subscriptions in scope for the Well-Architected review. Perform this step only if you wish to include all Azure Advisor recommendations from an Azure subscription into the reports.

- Select the security pillar.

- Spend time with the customer on each section and options presented within the section. You can capture any relevant notes from this discussion in the note text box below. (Try to capture these notes in OneNote or another system as these notes are not yet exposed in the reports)

- After submitting the assessment, you will be presented with the assessment results and scores.

- Locate the Export to CSV option to download the csv report for the assessment.

> [!NOTE]

> There may not be sufficient time to go into every recommendation with the customer, so use your discretion on how many recommendations in each category to review and annotate.

> [!IMPORTANT]

> Azure Advisor integration is supported for Azure commercial cloud tenant accounts \*\*only\*\* and may bring efficiencies into the reporting part of the delivery with the automatic inclusion of recommendations into the CSV output report. This integration should only be considered when the workload scope can be filtered successfully using the limited filtering levers in this integration feature.

## Insights Days 1-2

The Insights Days are intended to provide ample time for the Microsoft resource and the customer to dig into the insights from both Azure Well-Architected Review and the Azure Monitor security workbook. Each well-architected assessment has its own critical areas of focus aligned to the specific tenant in the Microsoft Azure Well-Architected Framework. The following subsections provide more specifics on the discovery and insights days to ensure a successful delivery.

### Discovered Data Analysis

The first activity as part of the Insights phase is to analyze the collected data from the Azure Well-Architected Review. The Azure Well-Architected Review assessment results are structured and organized for identifying optimizations opportunities and broken down into categories in the CSV export. Each category is sorted based on the achieved score. Explain each recommendation to the customer and how they should proceed with mitigating the identified issues.

When a recommendation involves enabling an Azure security solution (e.g., Microsoft Defender for Cloud, Azure Policy, Azure Blueprints, Azure Firewall, Web Application Firewall, etc.), take the time to demo or illustrate these technologies and capabilities to ensure the customer understands their value and place in improving workload security.

## Azure Monitor Security Workbook

The Azure Monitor security workbook deployment and workload filtering should have been completed in the kick-off session. There are multiple report pages to review with the customer. The delivery resource should focus in on the dashboards and report pages that contain the most relevant insights for the assessment.

The workbook contains the following pages that provide important insights for this assessment:

#### Security and Compliance

- Review overall secure score and subscription secure score.

- Explain how secure score is calculated [Secure score in Microsoft Defender for Cloud | Microsoft Docs](https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls).

- Review each control area and resource compliance against the included policies for each control area.

- Review, share, discuss the connection from recommendations to control areas and their impact on secure score. [Security controls and their recommendations | Microsoft Docs](https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations).

- Export insights for Q&A session and reporting.

#### Microsoft Defender for Cloud Alerts

Alerts require Microsoft Cloud Defender enabled on the in-scope subscriptions.

- Review each group and resources with active alerts.

- Review, share, discuss alerts against resources in the workload. [Alerts Reference](https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference).

- Export alerts for Q&A and reporting.

#### Regulatory Security and Compliance

Control Frameworks require Microsoft Cloud Defender to be enabled on the in-scope subscriptions before those control frameworks besides Azure-Security-Benchmark can be added.

- Review each compliance standard relevant to the workload.

- Review, share, discuss regulatory compliance for resources in the workload [Tutorial: Improve your regulatory compliance](https://docs.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard).

#### Advisor

- Explain the Advisor page has full inventory of all active recommendations whether they are part of secure score control areas or not.

- Review, share, discuss recommendations not already covered on the Security and compliance page.

- Export insights for Q&A session and reporting.