# Scoping

The Scoping component includes a scoping email and a scheduled \*\*30 minute\*\* call with the customer at least two weeks or more prior to the delivery. This phase is important to ensure expectations are set, prerequisites are met, stakeholders identified, and outputs are clear.

A key element in this phase is to ensure customer stakeholders are available for the Q&A portion of the delivery.

Scoping phase:

- Scoping email

- Scoping call

- Azure Monitor workbook prerequisite validation

## Scoping email

The scoping email is sent by the dispatched delivery resource to the primary customer point of contact(s), Customer Success Account Manager (CSAM), Cloud Solution Architect (CSA), and Microsoft account team as applicable.

The customer point of contact should be the representative responsible to coordinate logistics, requirements, and stakeholders. Typically the scoping email recipients are the stakeholders that will participate in the assessment. There is a separate email template per Well-Architected Assessment which can be obtained in the scoping folder in the respective assessment [IPKit](https://aka.ms/waf/ipkits).

\*\*View Scoping Email template [here](https://microsoft.sharepoint.com/:u:/r/teams/ASDIPRelease/IP%20Release/Secure%20Infrastructure/Assessment%20Program/Well-Architected%20Security%20Assessment/3-Scoping%20Call%20Artifacts/CUSTOMER%20NAME%20Well-Architected%20Security%20Assessment.oft?csf=1&web=1&e=rtfaYP)\*\*

> [!NOTE]

> The email should be sent as soon as a scoping call is scheduled with customer, CSAM, and delivery resource. Ideally this is several business days prior to the scoping call to give the customer time to complete pre-reqs for resource provider registration.

The purpose of this email is as follows:

- Conveys the date and time of the scheduled scoping call.

- Provides a high level agenda for the scoping call.

- Provides technical requirements for the Azure Monitor workbook including step-by-step to meet the requirements.

## Scoping Call

During the call the delivery resource explains the delivery flow and what topics will be reviewed. The Well-Architected Security Assessment covers the following categories for workload security:

- Application Design

- Health Modelling

- Networking and Connectivity

- Security and Compliance

- Operational Procedures

- Deployment and Testing

- Operational Model and DevOps

- Identity and Access Control

The scoping call provides an opportunity to ask questions such as:

- What do you expect from the assessment?

- What specific Azure workload will be assessed?

- Are there specific topics of interest?

- Executive briefing intended audience and scheduling

The Well-Architected Assessments are focused on a \*\*specific production Azure workload\*\*. A `workload` or `application` is a resource or collection of resources that provide end-to-end functionality to one or multiple clients (humans or systems). Another way to think of it; workload as an \*\*end-to-end scenario\*\* (a process) and the IT infrastructure supporting it. It can be one application, it can be multiple apps, APIs and databases working together \*\*to deliver a specific functionality\*\*.

\*\*Examples:\*\*

\*\*\*Example 1:\*\*\*

The Azure resources of ticket ordering workload would be:

1. The client web application, used by consumers to book tickets.

2. The payment gateway used to process credit card transactions.

3. The backend API handling communication.

4. The database where everything is stored.

5. The gateway to on-premises systems handling capacities and available seats.

6. The admin web application.

7. The shared AAD supporting authentication for administrators across the organization... etc.

\*\*\*Example 2:\*\*\*

A data processing pipeline, which runs every night:

1. Pumps data from SAP and other on-premises systems.

2. Runs data analytics workbooks on Data Bricks.

3. Stores results into Storage

4. Is accessed by a desktop application.

5. Only for authenticated users from the organization.

The guidance here is to have the customer pick a business critical run-state workload and its supporting resources/services (if not already identified during pre-scoping). When customers struggle with picking a single workload for security review (`but we have so many apps in Azure, which one should we choose?`), it's recommended to pick either the most exposed and sensitive one, possibly with recent breaches, or the most representative one – if the company is running 90% web apps, doesn’t make sense to analyze data processing workload, unless there’s a specific reason for it (breach).

> [!IMPORTANT]

> If the customer is unable to define a specific workload or the defined workload is not configured in a manner that is easily surfaced (subscription, resource group, tags) by the Azure Monitor workbook, modifying the existing workload to include resource tags is required. If tagging is needed, it is recommended to follow the [Recommended naming and tagging conventions](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/naming-and-tagging) guidance in the Azure Cloud Adoption Framework.

> [!NOTE]

> Request workload architecture diagrams to be shared in advance of the delivery. Diagrams provide delivery resource with valuable information on the architecture of the scoped workload that can be used to lead the customer in the Q&A discussions.

A key component of the scoping and setup phase is to ensure the customer gets the prerequisites in place for the Azure Monitor workbook.

Other topics to include in the call:

- Engagement logistics

- Azure Monitor workbook prerequisites

- Specific topics of interest

- Has workload been assessed before?

- Customer stakeholder expectations

- Core output of an agreed upon improvement implementation plan

|Assessment|Stakeholders|

|-------|------------|

|Well-Architected Security Assessment |Cloud Architect, SecOps, IAM, Network engineering, Solution owner, DevOps manager, Governance, risk, compliance manager |

>[!Important]

> It is important for the correct stakeholders to be available at the outset of the assessment both for accuracy of responses to the discovery phase and to ensure no time is lost due to unavailable stakeholders.

> Establishing customer stakeholder expectations during the scoping phase provides the customer with an opportunity to line up the correct resources well in advance of the assessment delivery.

> [!NOTE]

> There are valuable insights only available via Azure Defender being enabled on the in-scope subscriptions. Security alerts and regulatory compliance dashboard reports are only available with Azure Defender for example. Encourage customer enable Azure Defender, even if in trial mode, on the in-scope subscriptions.

>[!Important]

> It is important for the customer to ensure Azure Monitor Workbook prerequisites are in-place going into the delivery. Followup with the customer contact via email after scoping and prior to the delivery to ensure this step is completed.