# Overview of Well-Architected Security Assessment Delivery

This delivery guide is aimed at helping delivery engineers understand what the Well-Architected Security Assessment is and how to get the best delivery experience for our customers.

# What is a Well-Architected Security Assessment?

The Well-Architected Security Assessment is aimed to assess an Azure workload implementation across the security pillar of the Microsoft Azure Well-Architected Framework.

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 main goal of this delivery is to provide a comprehensive end-to-end review of an existing application or workload to identify critical security optimizations. This assignment is designed to:

- Cover a range of technical topics from Application Design, Health Modelling, Customer Operational procedures (DevOps) etc., but always through a focused security lens.

- Identify critical security risks to scoped applications on Azure.

- Provide the customer with actionable feedback

## Domain Areas covered in the Well-Architected Security Assessment

- Application Design

- Health Modelling

- Operational Procedures

- Networking & Connectivity

- Security & Compliance

- Deployment & Testing

- Identity & Access Control

- Operational Model & DevOps

# What will be assessed

1. A single run-state workload. This workload will be used for security assessment.

2. Evaluate workload against best practices for application design, health monitoring, security & compliance, etc.

3. Collect data and provide recommendations around the configuration of your Azure tenant and supporting infrastructure.

# Delivery Out of scope

1. Remediation during the assessment delivery

2. Customization of Azure Monitor workbook

# Delivery Phases

Their are 6 different stages involved with delivering this assessment. These stages are:

1. Pre-scoping: An internal call with the Microsoft account team, CSAM, CSA and CE to discuss what's involved in this delivery.

2. Scoping: A call with the customer to outline what will be delivered as part of this MIP and to ensure the customer meets the requirements (A single workload that is identifiable within Azure).

3. Assessment: This stage includes the kick-off meeting (use the PPT presentation), walking through the customers architecture and completing the WAF security assessment in the PNP portal.

4. Reporting: During this stage the engineer will review their findings from the assessment stage and begin creating the `Well-Architected Security Assessment - Recommendations and Optimizations Executive Summary` PPT (combining the dynamic + static presentations).

5. Pre Close Out: Once the report is complete, a meeting needs to be organized to present and review the findings with the CSA, CSAM and the account team (as required).

6. Close Out: The final stage is where the report will be presented to the customer.

# Next Steps

1. [Customer Delivery Scoping](wasa-scoping.html)

# Important References

1. [Well-Architected Security Assessment IP Kit](https://aka.ms/waf/wasa)