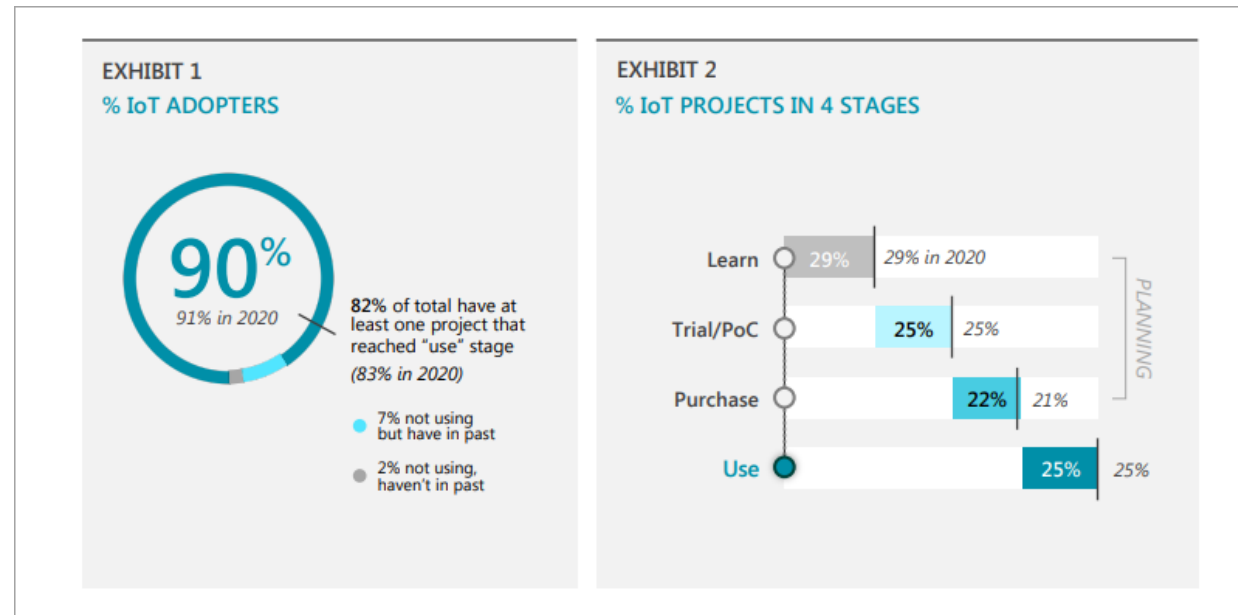


Azure Well-Architected Framework for IoT Overview

- Gordon Smith
- Sr. Technical Specialist / Microsoft
- May 2022

Azure Well-Architected Framework for IoT

Motivation



IoT Signals Edition 3 – October 2021

- IoT Projects are complex, many fail in the POC stage
 - Primary causes cited:
 1. Lack of knowledge
 2. Technical complexity cited as causes

Azure Well-Architected Framework for IoT

Introduction

- Built by a deeply technical team of architects, consultants, developers
- Goal: synthesize experience into actionable recommendations for customers
- Approach: leverage existing Azure Well-Architected Framework and extend for IoT workloads

Baseline: What is the Azure Well-Architected Framework?

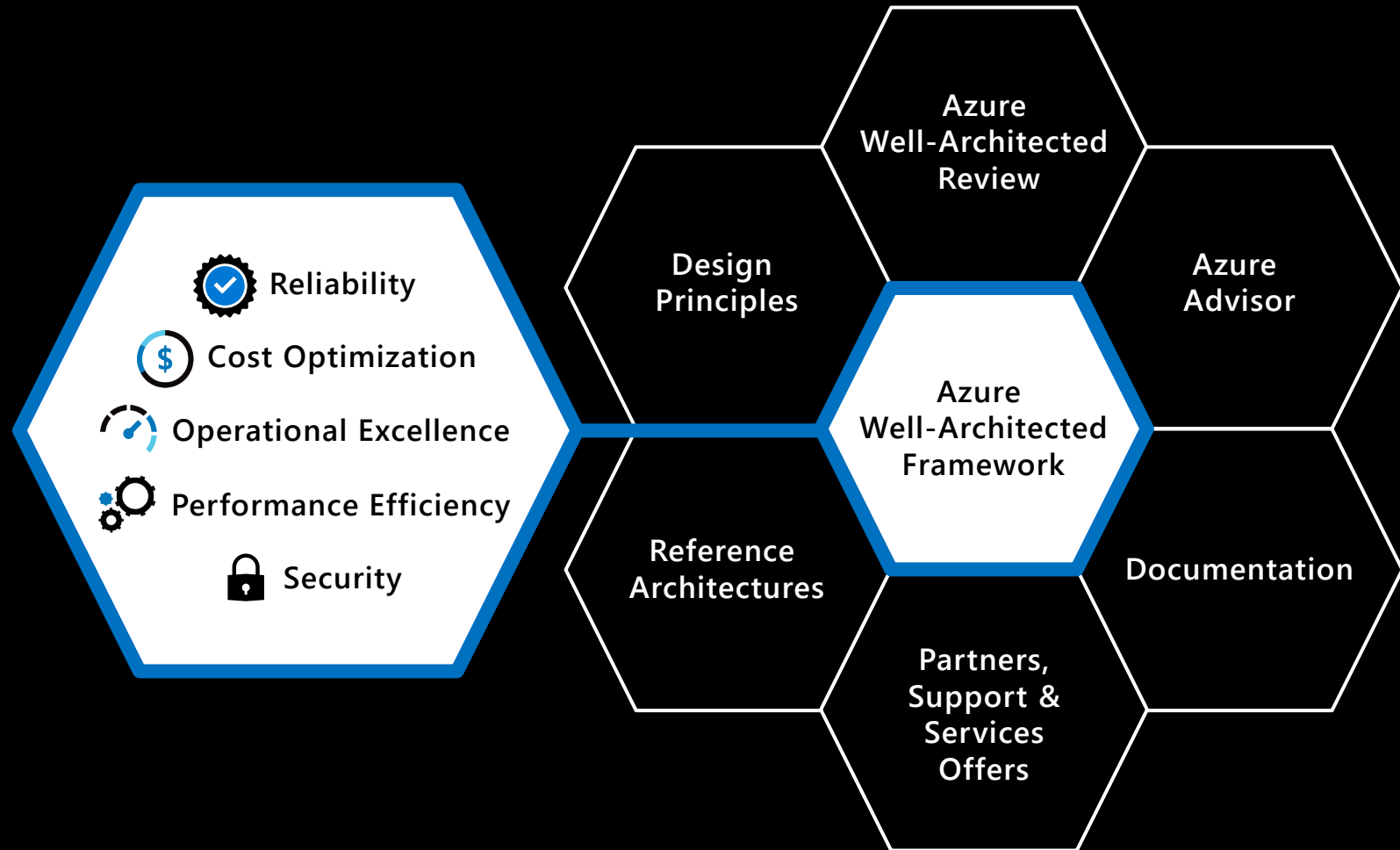
Azure Well-Architected

Build and manage high-performing workloads

Build workloads with **confidence** with proven best practices

Design **high-performing** workloads using deep technical guidance

Optimize workloads with actionable focus areas



What are WAF “workload” deliverables?

(1) Written overview and guidance

The screenshot shows the Microsoft Azure documentation page for 'Security in a hybrid workload'. The page is part of the 'Azure Architecture Center (AAC) resources' and is titled 'Security in a hybrid workload'. It includes a sidebar with a navigation menu for 'Azure / Architecture' and a search bar. The main content area discusses the importance of security in hybrid and multicloud environments, mentioning Azure Security Center, Azure Sentinel, and Azure Arc. It also provides links to 'Principles', 'Design', and 'Monitor' sections.

(2) Assessment questionnaire and implementation resources

The screenshot shows the Microsoft Azure Well-Architected Review assessment questionnaire. The page is titled 'Azure Well-Architected Review' and is part of the 'Assessments' section. It includes a sidebar with a navigation menu for 'Assessments' and a search bar. The main content area is titled 'Reliability' and contains a list of questions and checkboxes for assessing reliability targets and metrics. The questions include: 'What workload type do you want to evaluate?', 'Which pillars do you want to evaluate?', 'What reliability targets and metrics have you defined for your application?', 'How have you ensured that your application architecture is resilient to failures?', 'How have you ensured required capacity and services are available in targeted regions?', 'How are you handling disaster recovery for this workload?', 'What decisions have been taken to ensure the application platform meets your reliability requirements?', 'What decisions have been taken to ensure the data platform meets your reliability requirements?', 'How does your application logic handle exceptions and errors?', 'What decisions have been taken to ensure networking and connectivity meets your reliability requirements?', 'What reliability allowances for scalability and performance have you made?', 'What reliability allowances for operations have you made?', 'How do you test the application to ensure it is fault tolerant?', 'How do you monitor and measure application health?', 'Security', 'Have you done a threat analysis of your workload?', 'What considerations for compliance and governance did you make in this workload?', 'What practices and tools have you implemented as part of the development cycle?', 'Have you adopted a formal secure DevOps approach to building and maintaining software?', 'Is the workload developed and configured in a secure way?', and 'How are you monitoring security-related'.

Using the Azure Well-Architected Review

This web-based assessment helps improve the quality of a workload by

- **Examining the workload** across the 5 pillars of the Azure Well Architected Framework (Reliability, Cost Optimization, Security, Operations Excellence, and Performance Efficiency)
- **Providing specific guidance** to improve architecture and overcome detected hurdles effectively
- **Proactively focusing** on the pillar where most attention is needed
- **Driving consistency** into customer discussions.

Microsoft Azure Well-Architected Review

Examine your workload through the lenses of reliability, cost management, operational excellence, security and performance efficiency [20 minutes].

Assessment name *

Microsoft Azure Well-Architected Review - workload #1

Choose your interests

☐ Cost Optimization

An effective architecture achieves business goals and ROI requirements while keeping costs within the allocated budget.

☐ Operational Excellence

To ensure that your application is running effectively over time, consider multiple perspectives, from both an application and infrastructure angles. Your strategy must include the processes that you implement so that your users are getting the right experience.

☐ Performance Efficiency

Prioritize scalability as you design and implement phases. Scalability leads to lower maintenance costs, better user experience, and higher performance.

☐ Reliability

In a cloud environment to prevent all failures.

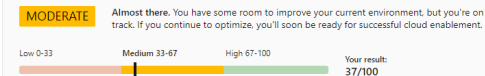
☐ Security

Security is one of the pillars of the Azure Architecture Framework. It provides assurances against threats that could negatively impact your workload. In the following sections, we will apply to Azure.

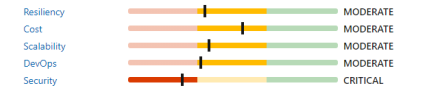
Recommendations for your workload

Actionable items to consider implementing to improve your workload across the five pillars of the Azure Architecture Framework

Your overall results



Categories that influenced your results



You can find out how to improve on individual categories by reviewing the recommendations below in the report.

Next Steps

Review the 'pillars of a great Azure architecture' learn module

You want to build great things on Azure, but you're not sure exactly what that means. Using key principles throughout your architecture regardless of technology choice, can help you design, build, and continuously...

[Visit Microsoft Learn >](#)

Review the Azure Architecture Framework

A successful cloud solution implementations requires focus on these five pillars of architecture excellence: Cost, DevOps, Resiliency, Scalability, and Security.

[Visit Azure Architecture Center >](#)

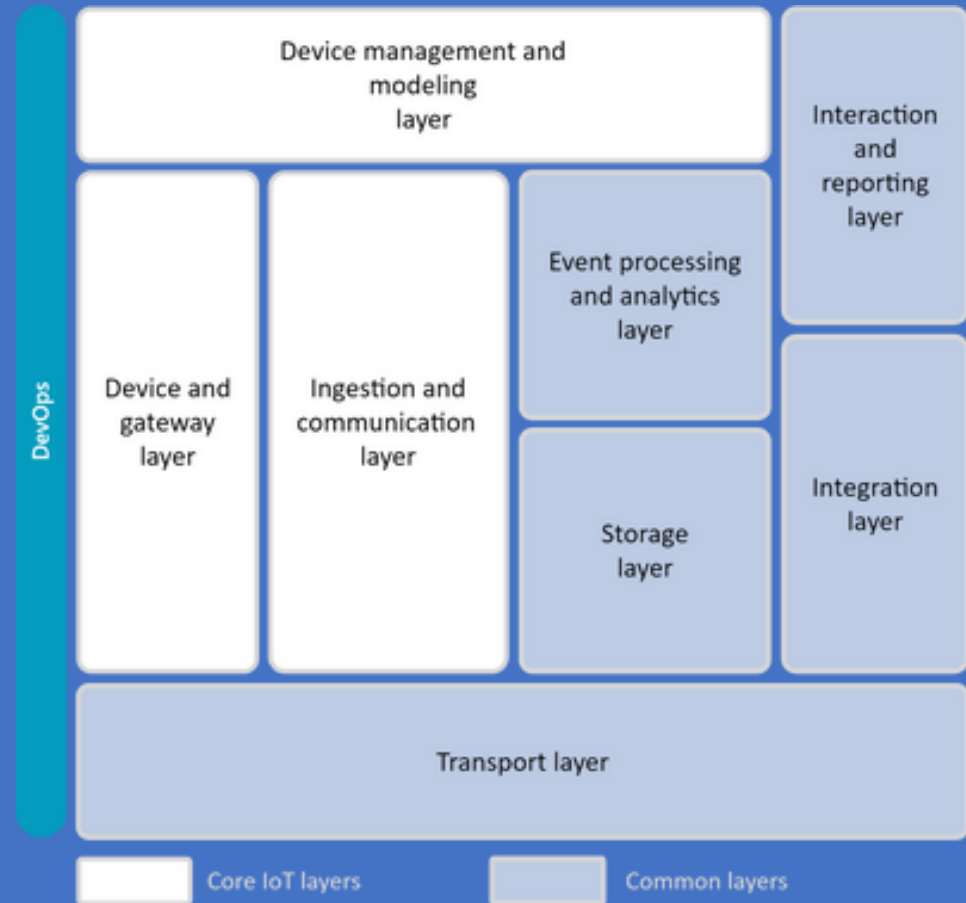
Review the 'how to incorporate security into your architecture design' learn module

Learn how to incorporate security into your architecture design, and discover the tools that Azure provides to help you create a secure environment through all the layers of your architecture.

[Launch the design for security >](#)

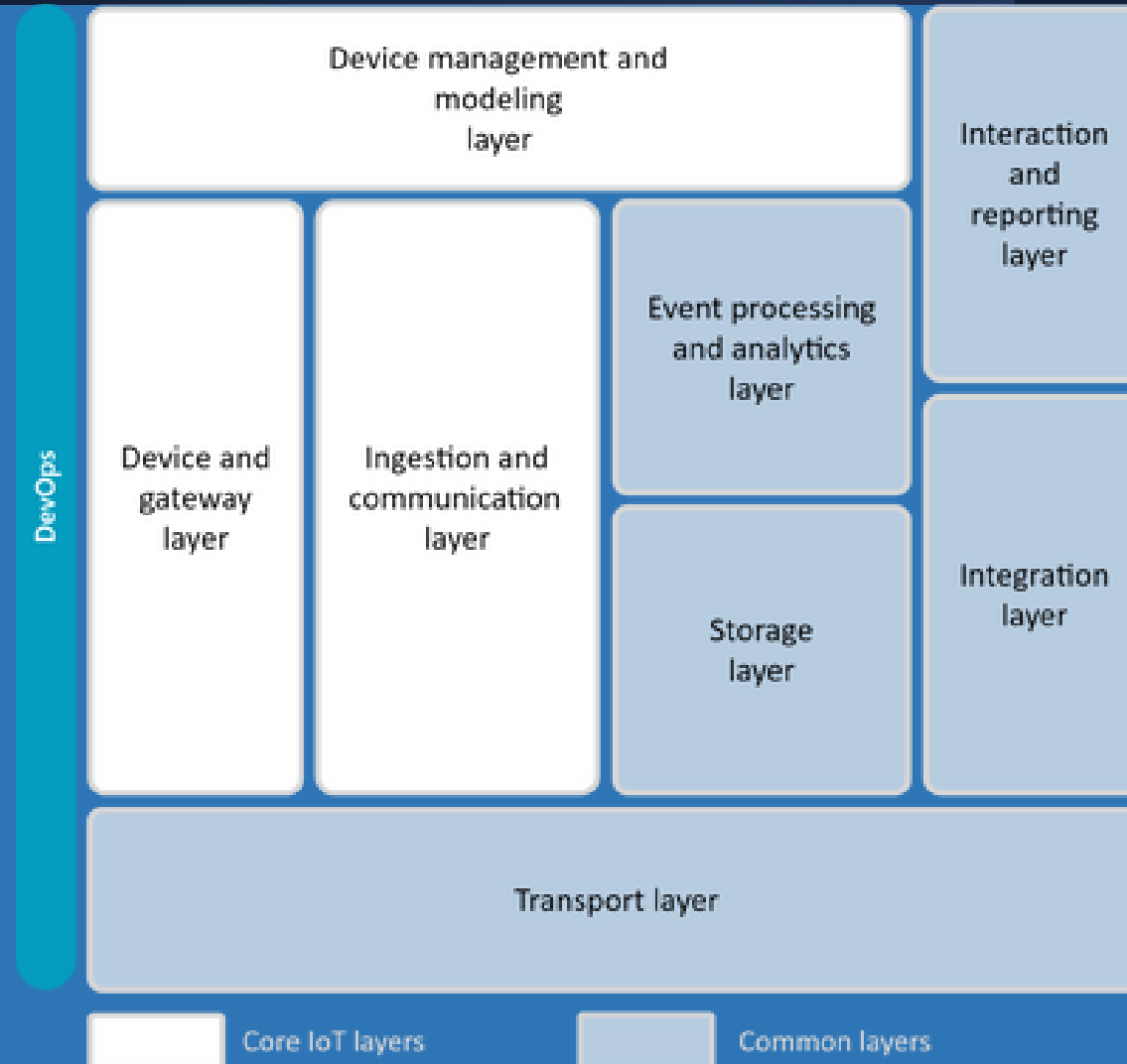
Azure Well-Architected Framework for IoT

1. Written Guidance
2. Well-Architected Review for IoT



Azure Well-Architected Framework for IoT

Architecture Layers



Azure Well-Architected Framework for IoT

IoT Workload Guidance

Outlines core principles

- Heterogeneity: different types of hardware and software
- Security: security and privacy measures
- (Hyper-) Scalability: support millions of connected devices and events
- Flexibility: built upon a principle of composability
- Serviceability: maintain and repair the components, devices, and other elements
- Intermittent connectivity: handle periods of offline and low-bandwidth connectivity
- Hybridity: on-premises, edge, and multi-cloud environments

Choosing the right architectural approach / pattern

- Connected Products - apply core principles
- Connected Operations - apply core principles

Provides recommendations for the 5 pillars of WAF

Resource: <https://aka.ms/waf/iot>

Azure Well-Architected Framework for IoT

IoT Workload Assessment

- Web based assessment tool
- Designed to help evaluate your workload against Azure best practices
- Provides actionable guidance
- Tailors recommendations to IoT project needs (considers tradeoffs among pillars)
- Repeat anytime during your development process (pre-deployment, refining architecture for pillars, etc.)

Resource: <https://docs.microsoft.com/en-us/assessments>

Azure Well-Architected Framework for IoT

IoT Workload Assessment

Azure Well-Architected Review
Azure Well-Architected Review - Apr 11, 2022 - 4:30:19 PM

[View guidance](#) 2 of 87 pages complete

WAF Configuration

- ✓ What workload type do you want to evaluate?
- ✓ Which pillars do you want to evaluate?

IoT - Reliability

- * Q1. Do you use Device Provisioning Service to discover the corresponding IoT Hub for the device to connect to?
- * Q2. How does your device handle transient network errors at connection time?
- * Q3. Do you have a repeatable process for deploying your device or edge agent and have you automated it?
- * Q4. How do you deploy firmware or application updates to your device?
- * Q5. How do you manage device state information including metadata, configurations, device connectivity state, heartbeat, and device conditions?
- * Q6. Have you defined uptime goals in accordance with the chosen failover approach (Microsoft initiated or manual) for your IoT solution starting with IoT Hub?
- * Q7. Have you performed a failure mode analysis and chaos engineering for your solution?
- * Q8. Have you defined appropriate policies to reconfigure dependencies when you failover the IoT Hub service from a primary to a secondary IoT hub?
- * Q9. Have you documented and tested your HA/DR procedures?
- * Q10. Have you ensured that your IoT Hub service has the appropriate scale level and units provisioned?

IoT - Reliability

Q1. Do you use Device Provisioning Service to discover the corresponding IoT Hub for the device to connect to?

As your IoT solution grows, so does the need to automate the process to connect devices to different IoT hubs that may exist across multiple regions. The connection process should be done in a secure and scalable manner with as few touch points as possible.

- ☐ You use Device Provisioning Service (DPS) with multiple regional IoT hubs linked to DPS and have enabled appropriate allocation policy ⓘ
- ☐ You don't use the Device Provisioning Service. You've implemented a custom provisioning service ⓘ
- ☐ Devices are statically configured to connect to the same IoT hub ⓘ
- ☐ None of the above.

[← Back](#)[Next →](#)

Add a note here.

Azure Well-Architected Framework for IoT

IoT Workload Assessment

Improve your results

Our recommendations for improving your results are organized by category below.

IoT - Security MODERATE

20 recommended actions

Results breakdown

Critical 0-33

Moderate 33-67

Excellent 67-100

Your result:
64/100

- [Q1] Use Azure Well Architected Framework to address security pillars.
- [Q11] Check your solution uses secure credentials and protocols.
- [Q11] Prioritize vulnerability remediation.
- [Q11] Assess your compliance configuration against a defined posture.

- [Q5] Renew operational certificates automatically.
- [Q5] Provision operational certificates from a trusted PKI with an appropriate lifetime.
- [Q4] Use IoT gateways to enforce strong identity patterns for less capable devices.
- [Q4] Use password-less authentication for device identity.

Azure Well-Architected Framework for IoT

Resources

Well-Architected Framework for IoT – Guidance

<https://aka.ms/waf/iot>

Well-Architected Framework – MSLearn (leads to AZ-305 certification)

<https://docs.microsoft.com/en-us/learn/paths/azure-well-architected-framework/>

Well-Architected Review – aka “WAF assessment”

<https://aka.ms/architecture/review>

IoT Signals Report

[IoT Signals Report | Microsoft Azure](#)

Let's take a look!



Thank you!