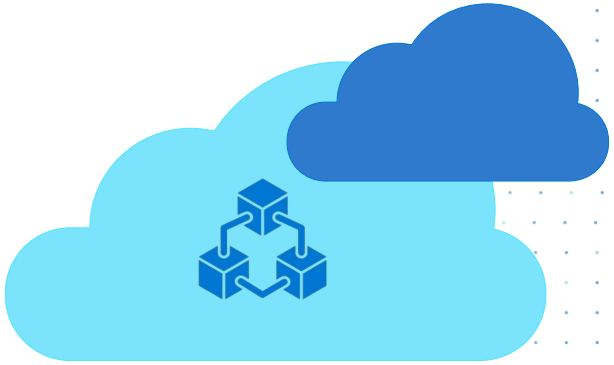
Microsoft

Microsoft Azure Well-Architected Workshop



<Name>
<Title>

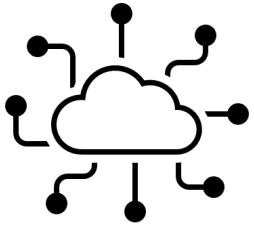
Agenda

- What is the Well-Architected Framework?
- Well-Architected Reviews
  - Cost optimization
  - Operations Excellence
  - Performance
  - Reliability
  - Security
- Remediation
- Expected outcome

Software Design & Development vs Architecture

Functional Requirements

What the application should do

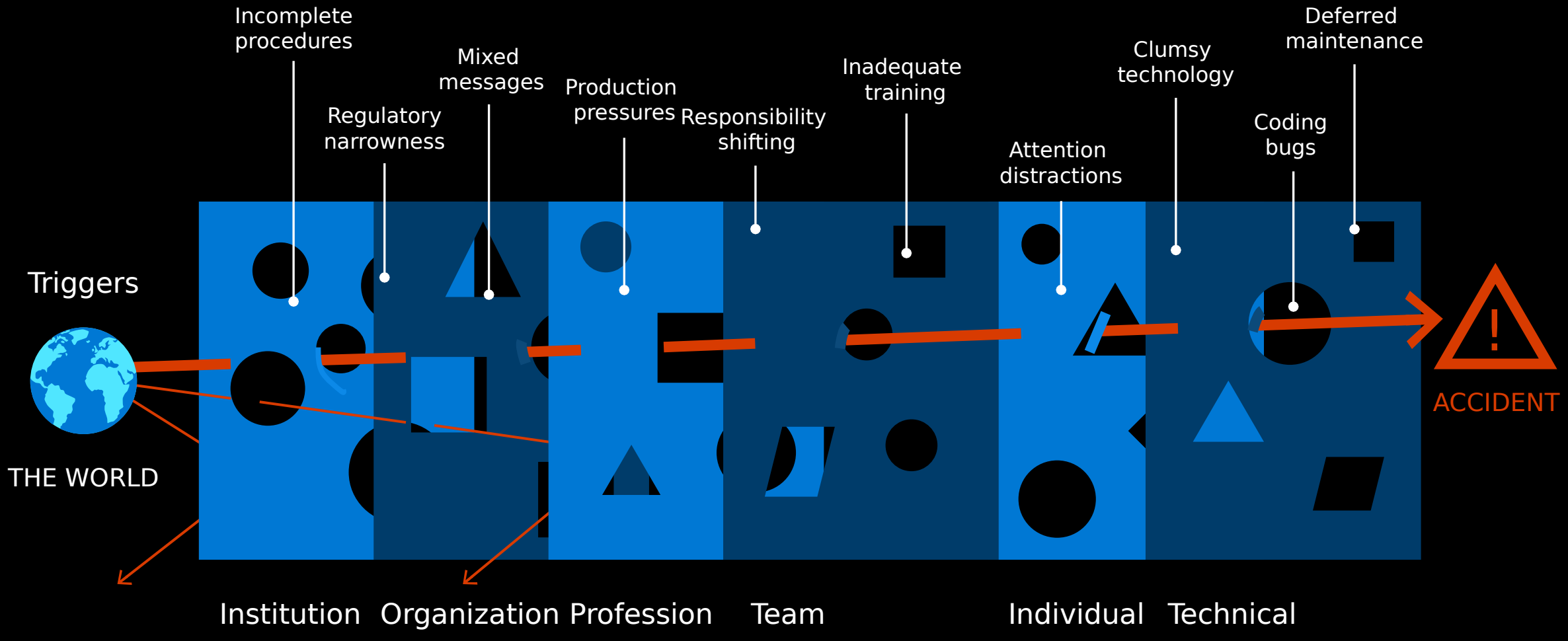


Architecture characteristics

Operational and design criteria for success

Why do bad things happen?

Modified from **Reason, 1991**



Proven guidance to support your cloud journey

Meeting different persona needs at different altitudes

Central IT

Workload Owners

Portfolio	Landing zones	Cloud Platforms	Workloads	Assets

Define strategy → Plan → Ready → Adopt

Define business justification and expected outcomes

Align actionable cloud adoption plan to business outcomes

Prepare people, process and environment for change

Migrate or Innovate

Govern ← Manage

Comply, control and secure

Operate and optimize

Cloud Adoption Framework and MCS Portfolio alignment: https://aka.ms/CAFServices

Well-Architected Framework

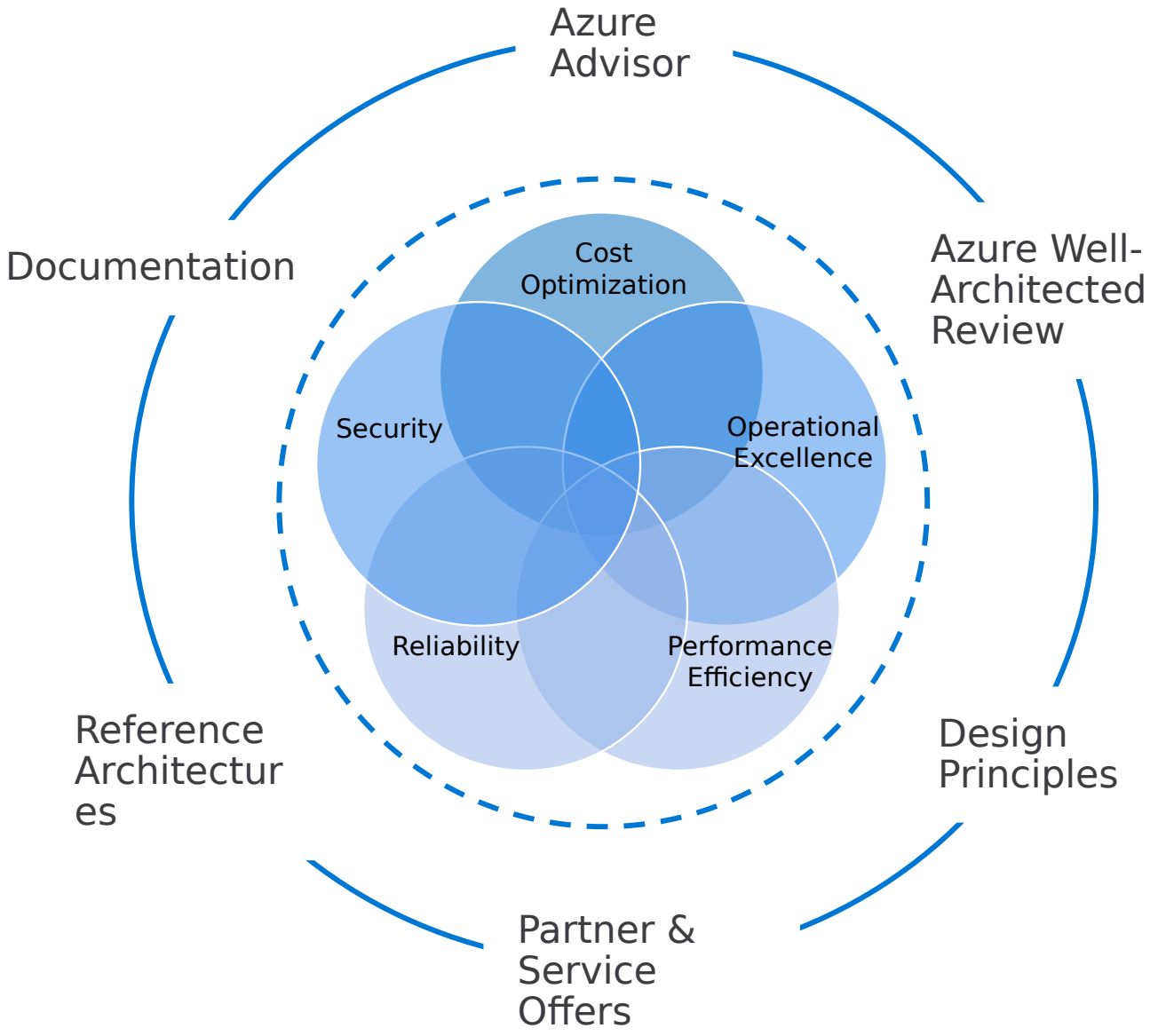
*Guidance to help design, build and optimize **workloads** in Azure*

Microsoft Azure Well-Architected

The Azure Well-Architected Framework is a set of guiding tenets to improve the quality of a workload.

The framework consists of five pillars of architecture excellence :

- Cost optimization
- Operational excellence
- Performance efficiency
- Reliability
- Security

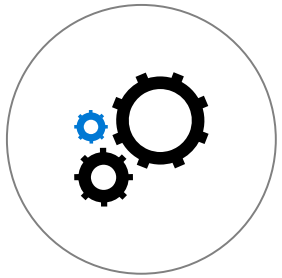


Best practices to drive workload quality

Cost Optimization

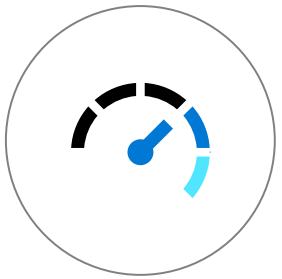
- ✓ Monitor and forecast
- ✓ Cost controls
- ✓ Azure Hybrid Benefit
- ✓ Reserve Instances
- ✓ Shutdown
- ✓ Resize
- ✓ Move to PAAS

Operational Excellence



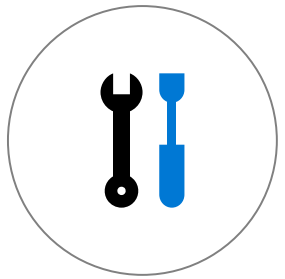
- ✓ DevOps
- ✓ Deployment
- ✓ Monitor
- ✓ Processes and cadence

Performance Efficiency



- ✓ Design for scaling
- ✓ Monitor performance

Reliability



- ✓ Define requirements
- ✓ Test with simulations and forced failovers
- ✓ Deploy consistently
- ✓ Monitor health
- ✓ Respond to failure and disaster

Security

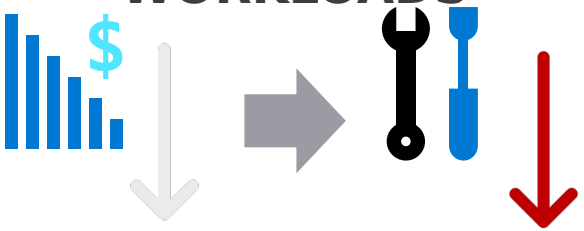
- ✓ Identity and access management
- ✓ Infra protection
- ✓ App security
- ✓ Data encryption and sovereignty
- ✓ Security operations

https://aka.ms/architecture/framework

Doing business means making trade-offs

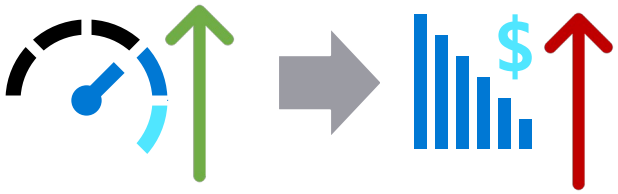
Business requirements influence workload architecture decisions

DEVELOPMENT WORKLOADS



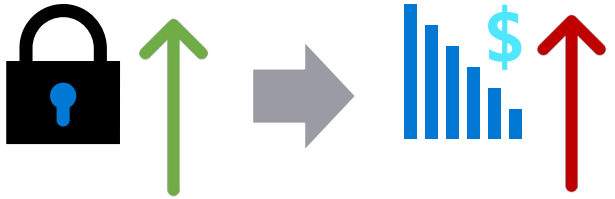
Optimizing costs in dev workloads may be the right approach, even when it may impact reliability, if it is in line with business expectations

MISSION-CRITICAL WORKLOADS



Improving performance for a mission-critical workload may be the right business decision, even at the expense of increased costs.

SECURING ALL WORKLOADS



Surge in cyber attacks drive workload security investments, as organizations attempt to protect their most valuable asset: data

https://aka.ms/architecture/framework

Building well architected systems is a **shared responsibility**

Scope of **Well-Architected Reviews**

Customer application

Customer **app** or **workload**, built on the Azure platform.

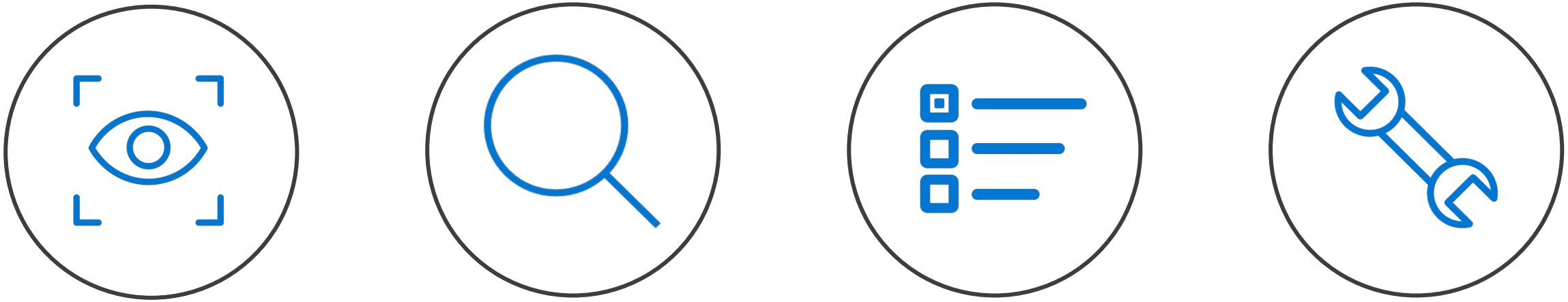
Platform features

Optional Azure capabilities **a customer enables** – to ensure security, reliability, operability, performance.

Platform foundation

Core capabilities **built into the Azure platform** – how the foundation is designed, operated, and monitored.

Well-Architected workshop process



1. Discover → 2. Analyze → 3. Prioritize → 4. Optimize

Review

Remediate

Example
Customer Stakeholders

- ❑ Solution Owner
- ❑ Solution Architect
- ❑ Cloud Architect
- ❑ Network Architect
- ❑ Data Architect
- ❑ Security Architect
- ❑ DevOps / SRE Lead
- ❑ Project Manager

Key Outcomes

Identify key risks to the design and implementation of the application

Propose actionable and prioritized recommendations to address identified risks

P0 – Critical short-term remediation
P1 – Strongly recommended mid-term improvements
P2 – Long-term sustainability recommendations

Capture key findings and associated recommendations in a Well-Architected report focused on the reviewed application

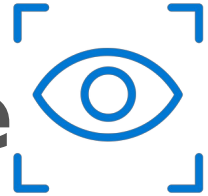
Provide guidance for implementing critical short-term recommendations

Microsoft

Well Architected Review

Discovery

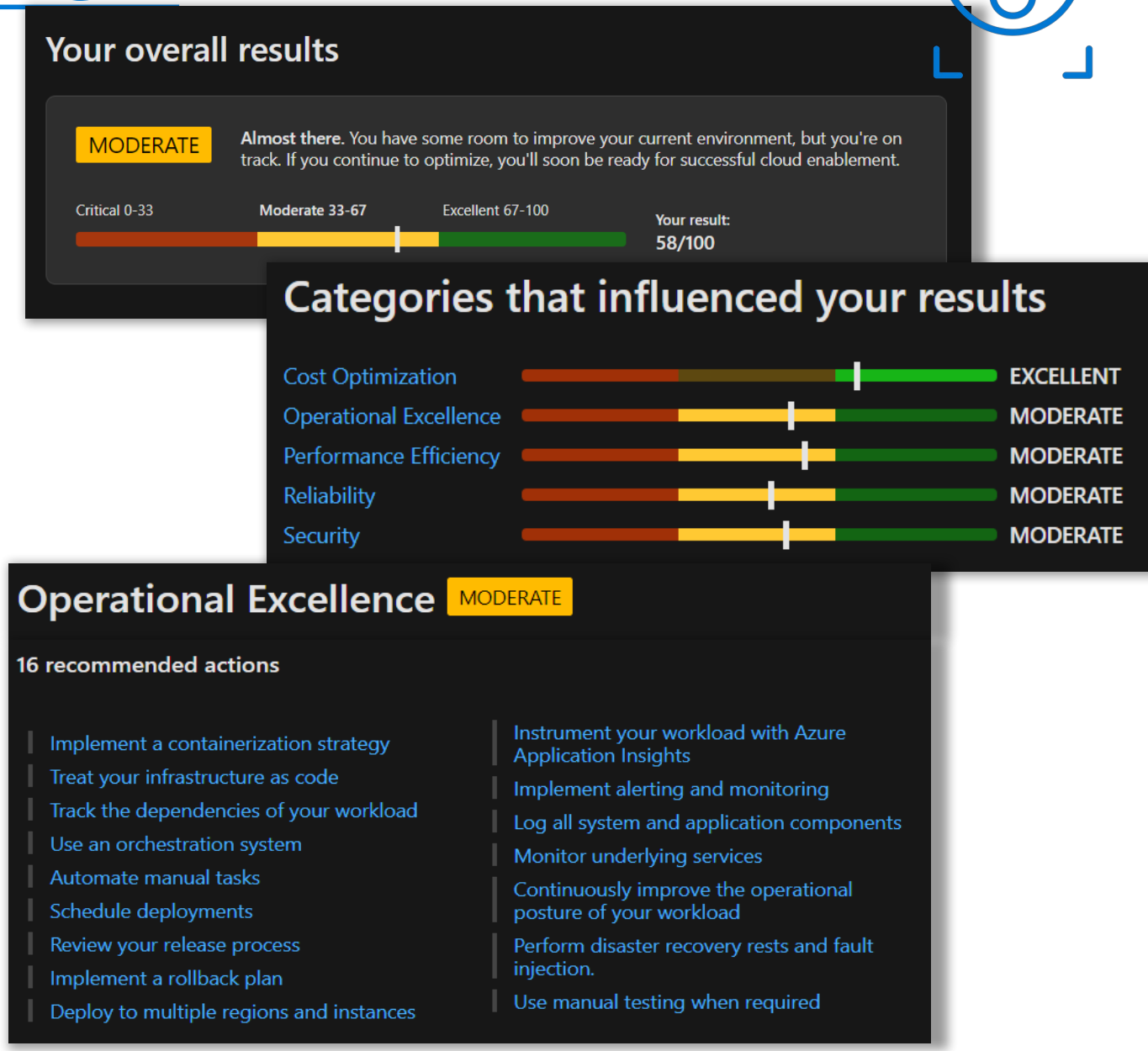
Discovery – Understand the current state



- Use the Well-Architected Review online questionnaire to have more insight on the customer’s cloud adoption maturity
- Understand the workloads profile (Customer facing app, internal application, IoT Solution…)
- Review with the customer the Architecture Diagram
- Azure Resources Walkthrough

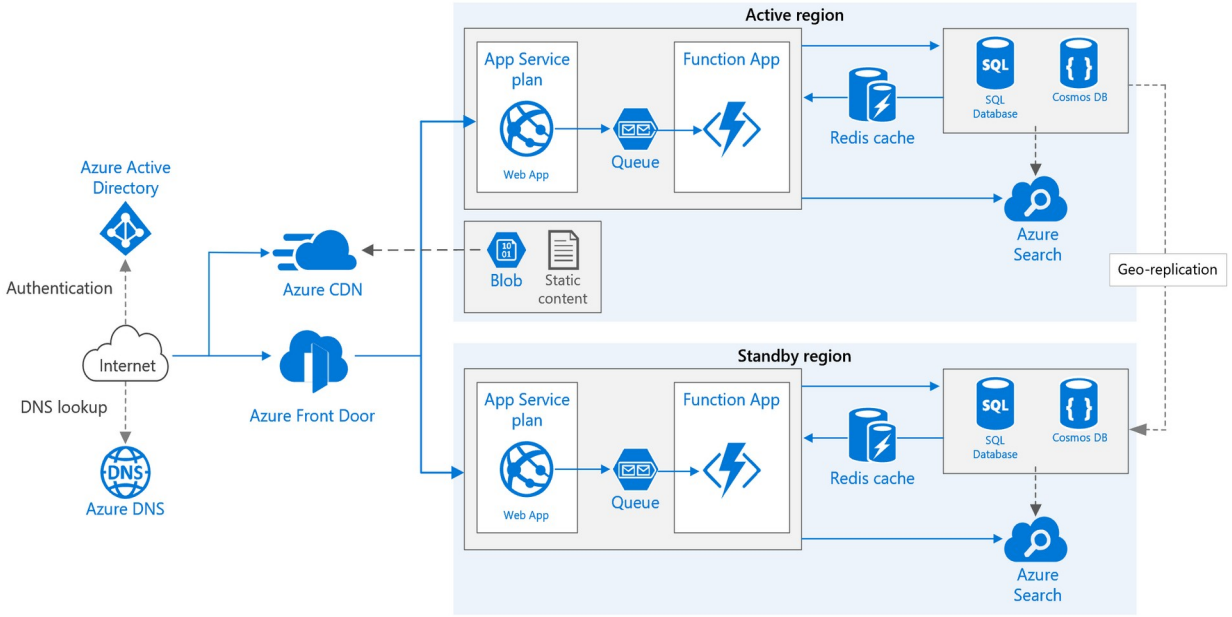
Well Architected Review

- The 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



Discovery - Architecture diagram

- Plays a critical role in understanding the customer deployments
- Ask the customer to provide an architecture walkthrough and design decisions
- Specific design pain points will be addressed further down the line in the review



Discovery - Azure Walkthrough

- Review the current state of Azure resources
- Resource walkthrough through the Portal by the customer
- Gather initial information on Governance and Resource structure

Useful links

Azure portal
Resource organizatio
Resource Explorer
Tagging convention

Discovery - Workload Profile

- Key Production workloads overview and key usage scenarios.
- How the production workloads are deployed, operated, measured, and monitored.
- Available usage data (CCO dashboard or existing cost details).
- Issues and experience degradations (is it related to platform services, application architecture, or process).

Discover – Tools

Use a data driven approach to optimize your Azure resources

- Azure Advisor
- CCO Dashboard
- Cloudockit
- AZGovViz
- WellArchitected Tools

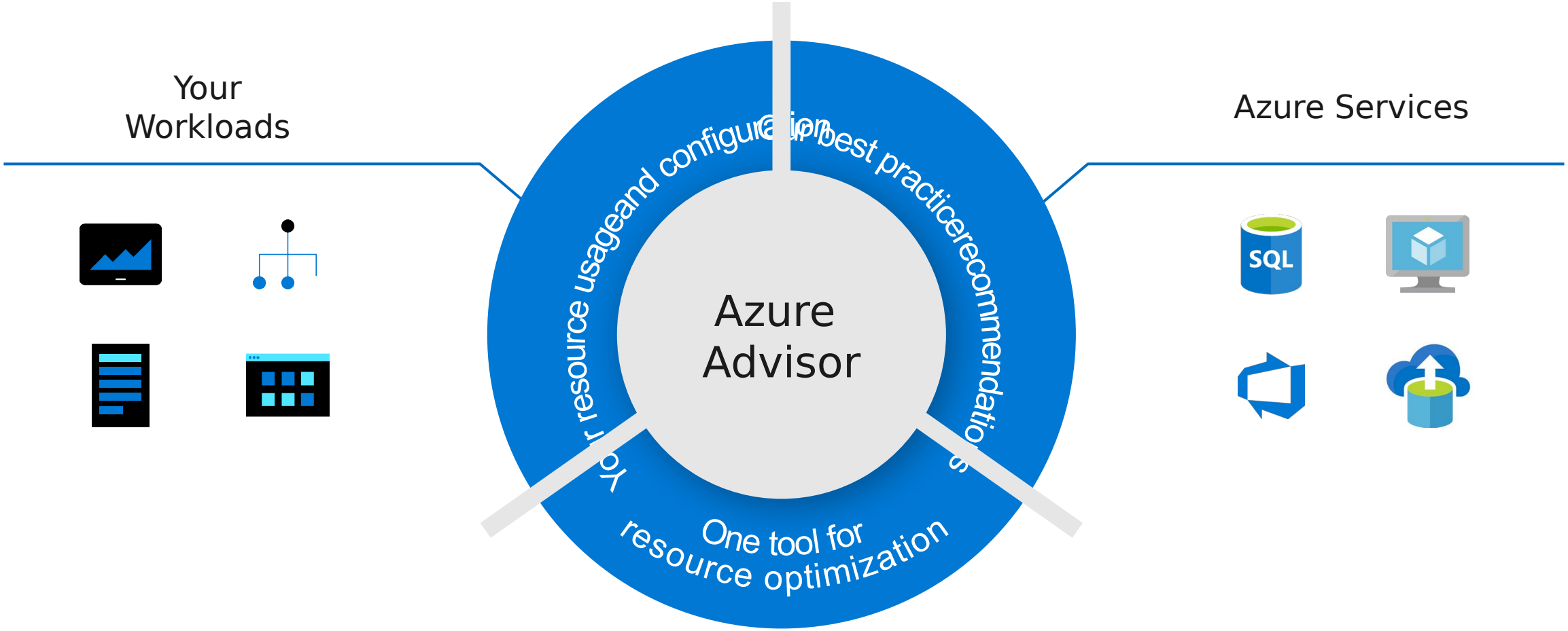
Azure Advisor

Personalized guide to Azure best practices

- Best practices to set up and optimize your Azure workloads
- Simple, step-by-step guidance and quick links
- One place to review and act on recommendations across Azure
- Alerts to notify you about new recommendations

Cost	Security	Performance	High availability	Operational excellence
Maximize the return on your Azure investment	Protect your Azure resources from security threats	Boost speed and responsiveness of your resources	Increase uptime of your business-critical apps	Process and workflow efficiency and manageability

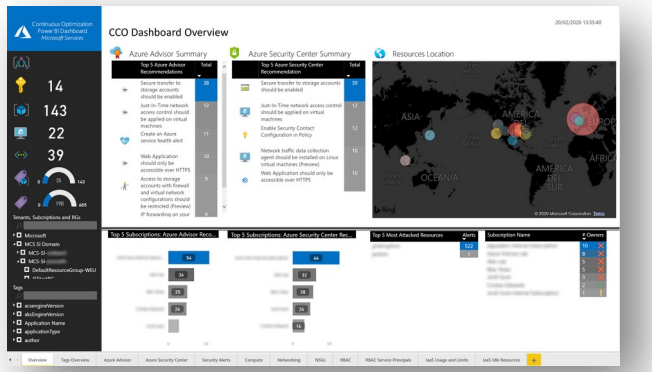
How Advisor works

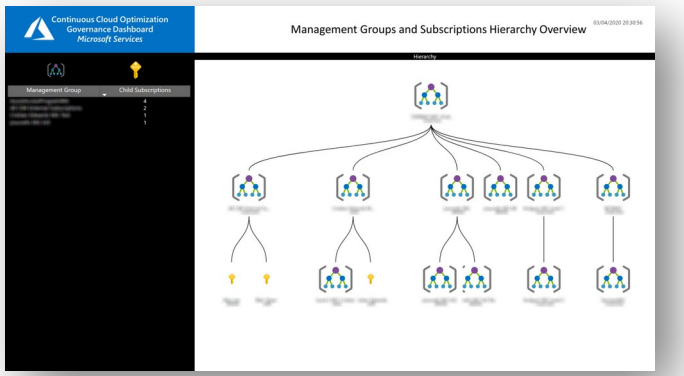


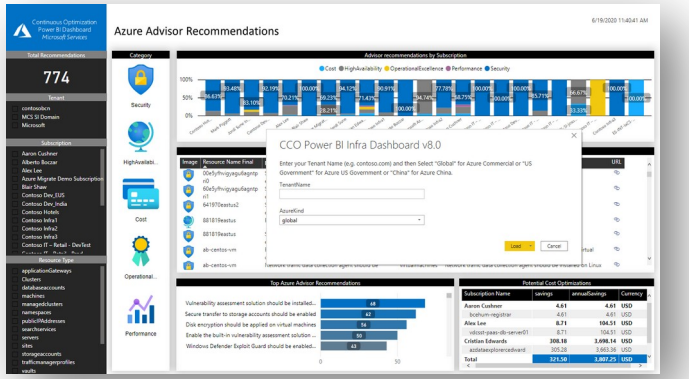
Continuous Cloud Optimization Power BI Dashboards

The Continuous Cloud Optimization Power BI Dashboards project is a set of Power BI Dashboards developed using Power Query M language and DAX, that pulls information directly from different Azure and Graph REST APIs and enables monitoring, operations and infrastructure teams to quickly gain insights about the existing Azure Platform footprint and resources. The current set of CCO Dashboards includes 3 different Dashboards to discover information about different Azure critical design areas:

CCO Azure Infrastructure Dashboard: Get insights about Azure Identity and RBAC, Security of your resources, Networking, Compute, Idle resources and Subscriptions Quotas and Limits
CCO Azure Governance Dashboard: Get insights Azure Governance aspects like Management Groups and Subscriptions hierarchy, Azure Policies, Azure Blueprints and Azure resources Regulatory Standards Compliance
CCO Azure Infrastructure Dashboard with AKS: Get all the insights from the infrastructure Dashboard plus AKS information







Source: https://github.com/Azure/ccodashboa

Why should we use the CCO Dashboard? Azure Portal already has most of the information natively.

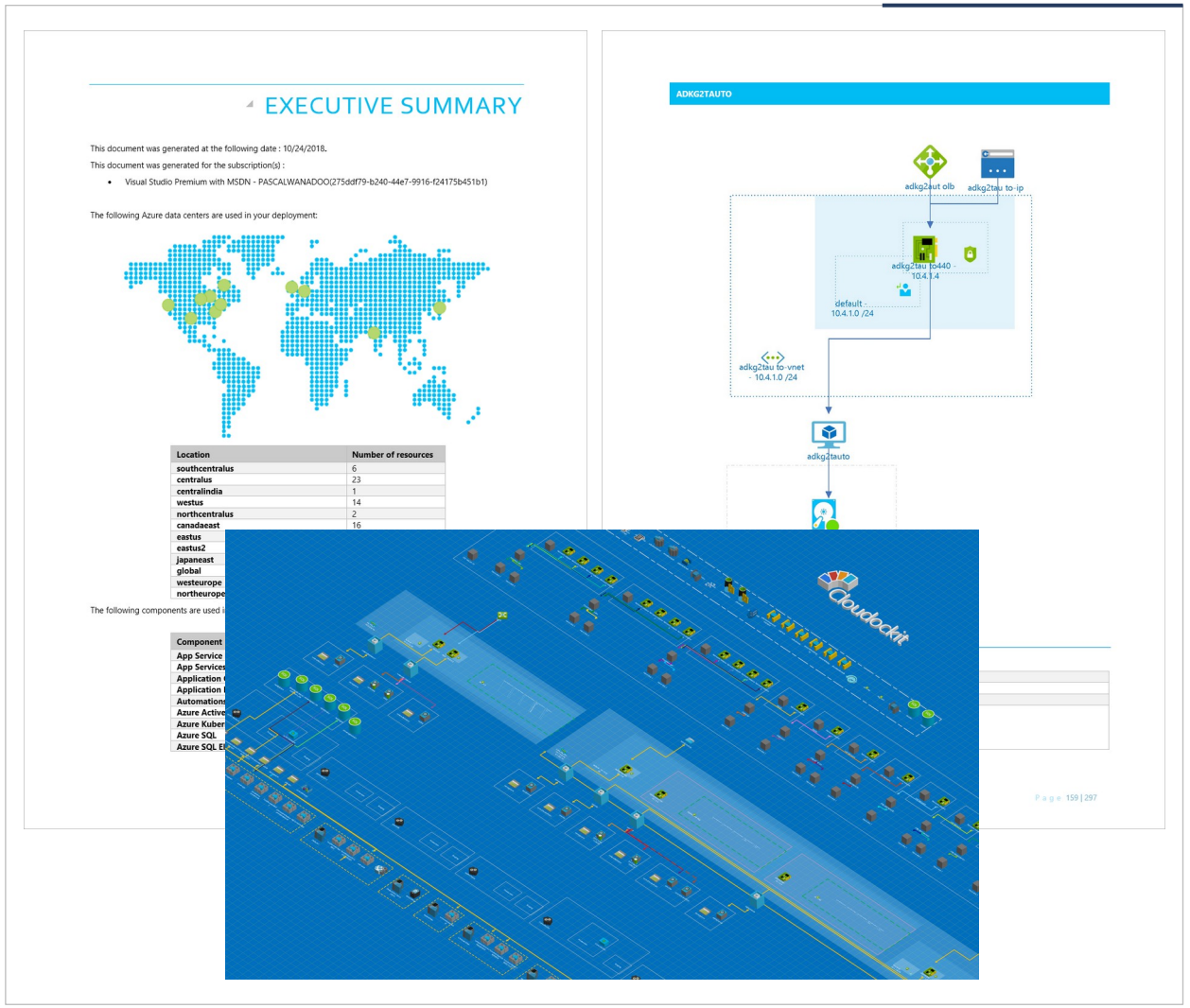
- Not all the customer stakeholders have access to the Portal. As Microsoft, we recommend to limit the access to the portal as much as we can. The CCO Dashboards enables customers to track their existing Azure footprint deployment with a rich, filterable and quick interface to multiple audiences.
- It provides or can provide an Executive Summary to customer C-x levels stakeholders
- The Portal does not include all the filters and data mappings natively. The Dashboard improves or expand some data no exposed in the portal. For example, Compliance state against different regulatory standards without the need of deploying them…
- It can provide segmented reporting to different customer teams (Security, Operations, Identity…)
- It is free
- It is easy to deploy and use.

How CCO Dashboard collects data

GitHub CCO Power BI Dashboard	Azure Account Credentials	Azure Subscriptions Access based on Azure Account permissions	REST API and Web Calls	REST APIs and web sites used as data source	Aggregated Customer Subscriptions Data
Continuous Cloud Optimization Power BI Dashboard Template execution	Customer Azure Account Credentials Request	Azure Subscription 1 Azure subscription Azure Subscription 2 Azure subscription Azure Subscription x Azure subscription	Azure REST API Calls API Management Azure AD Graph REST API Azure Active Directory	Azure Management Groups Azure Subscriptions Azure Resource Groups Azure Resources Azure Virtual Networks Azure Network Interface Azure Virtual Machines Azure Network Security Groups Azure Public IPs Azure Advisor Azure Security Center Azure Regions Azure AD Graph docs.microsoft.com	Continuous Cloud Optimization Power BI Dashboard  

What is CloudDockit

- It is a 3rd Party solution
- Is a SAAS solution that automatically generates technical documentation from Azure Subscriptions, including complete Visio diagrams, dependencies, track changes,
  best practices warnings, billing info (CSPs and Eas included)and more
- It works in both environment, classical and ARM
- It gives the ability to receive emails that contain executive information and changes since the last document generation
- Microsoft Services SI domain has licenses to use the tool
- It requires to have a user id in the customers AAD tenant with read-only permissions access to the subscriptions you want to analyze
- Customer Data and logging information is not stored on CloudDockit servers. Refer the customer to their security guidance
- A new offline version (CloudDockit Desktop) has been released if the customer does not want to use the SAAS solution



Source: https://www.cloudockit.com/cloudockit-security/

AzGovViz

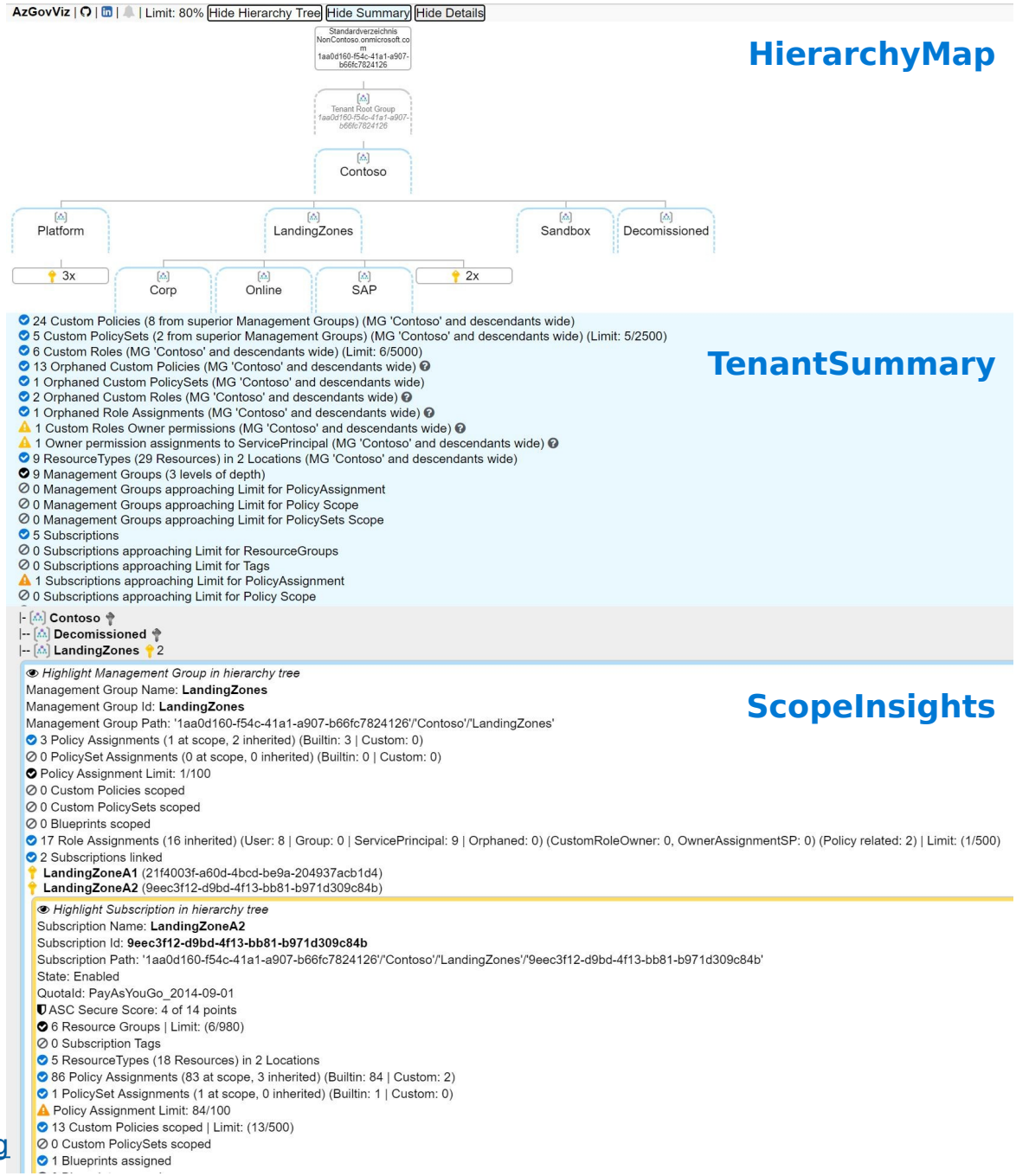
AzGovViz is a PowerShell based script that iterates your Azure Tenant´s Management Group hierarchy down to Subscription level.

It captures most relevant Azure governance capabilities such as Azure Policy, RBAC and Blueprints and more.

From the collected data AzGovViz provides visibility on your **HierarchyMap**, creates a **TenantSummary** and builds granular **ScopeInsights** on Management Groups and Subscriptions.

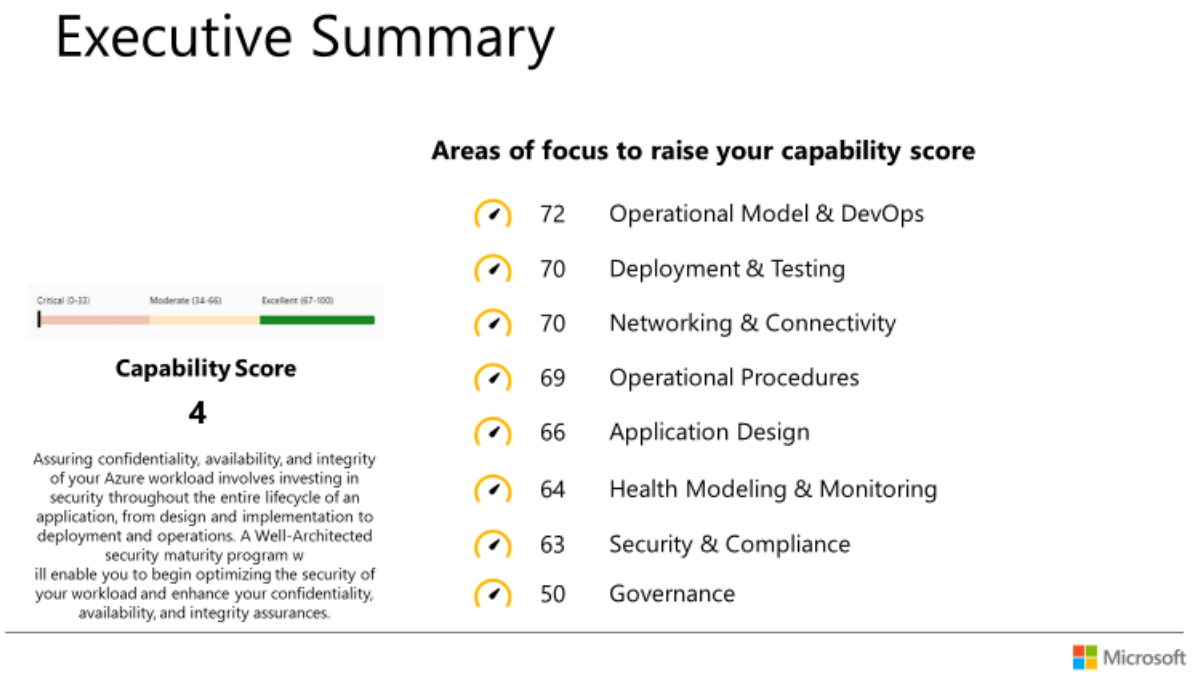
The technical requirements as well as the required permissions are minimal.

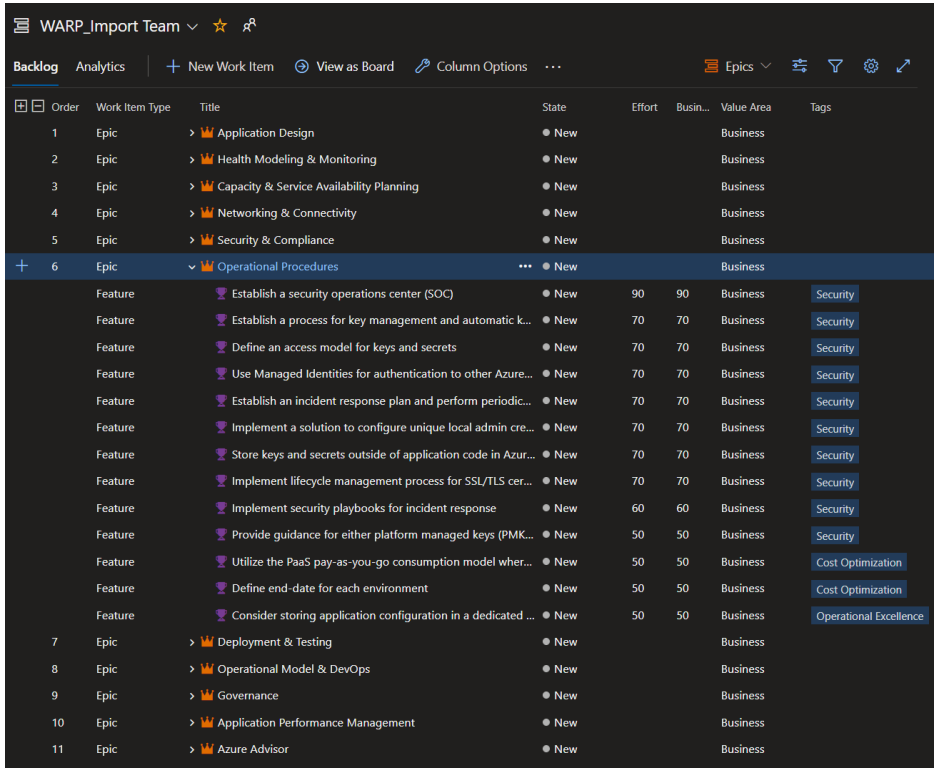
https://github.com/JulianHayward/Azure-MG-Sub-Governance-Reporting



Azure/WellArchitected-Tools

https://github.com/Azure/wellarchitected-tools





Microsoft

Well Architected Review

Analyze

The Microsoft Azure Well-Architected Framework Pillars

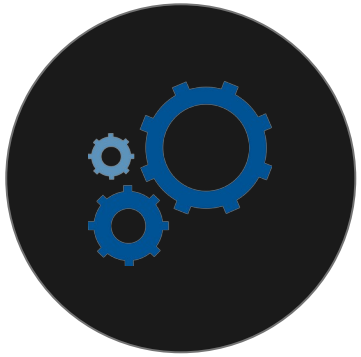
Learn more https://aka.ms/architecture/framework

Architecture guidance and best practices created for architects, developers, and solution owners, to ***improve the quality of their workloads, based on 5 aligned and connected pillars…***

Cost Optimization

- ✓ Keep within the cost constraints
- ✓ Aim for scalable costs
- ✓ Pay for consumption
- ✓ Right resources, right size
- ✓ Monitor and optimize

Operational Excellence

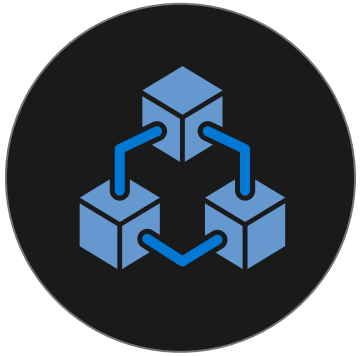


- ✓ Design for operation
- ✓ Automation
- ✓ Testing
- ✓ Safe deployment
- ✓ Monitoring

Performance Efficiency

- ✓ Design for performance
- ✓ Test for performance
- ✓ Monitor and optimize
- ✓ Capacity planning
- ✓ Data driven

Reliability



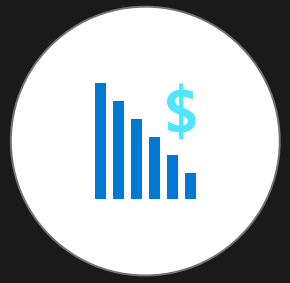
- ✓ Define requirements
- ✓ Design for resilience
- ✓ Resilience test
- ✓ Monitor and alert
- ✓ BCDR plan and test

Security

- ✓ Design for security
- ✓ Drive simplicity
- ✓ Build a comprehensive strategy
- ✓ Assume zero trust
- ✓ Educate and incentivize security

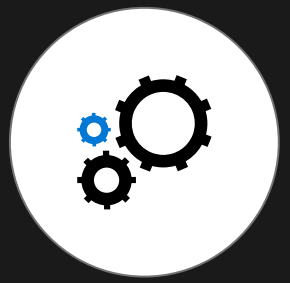
Overcoming workload quality inhibitors

Cost Optimization



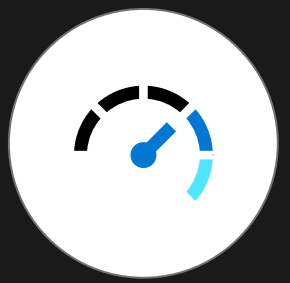
- No cost and usage monitoring
- Unclear on underused or orphaned resources
- Lack of structure billing management
- Budget reductions due to lack of support for cloud adoption by LT/board

Operational Excellence



- Lack of rapid issue identification
- No deployment automation
- Absence of communication mechanisms and dashboards
- Unclear expectations and business outcomes
- No visibility on root cause for events

Performance Efficiency



- No monitoring new services
- No monitoring current workloads health
- No design for scaling
- Lack of rigor and guidance for technology and architecture selection

Reliability

- Unclear on resiliency features/capabilities for better architecture design
- Lack of data back up practices
- No monitoring current workloads health
- No resiliency testing
- No support for disaster recovery

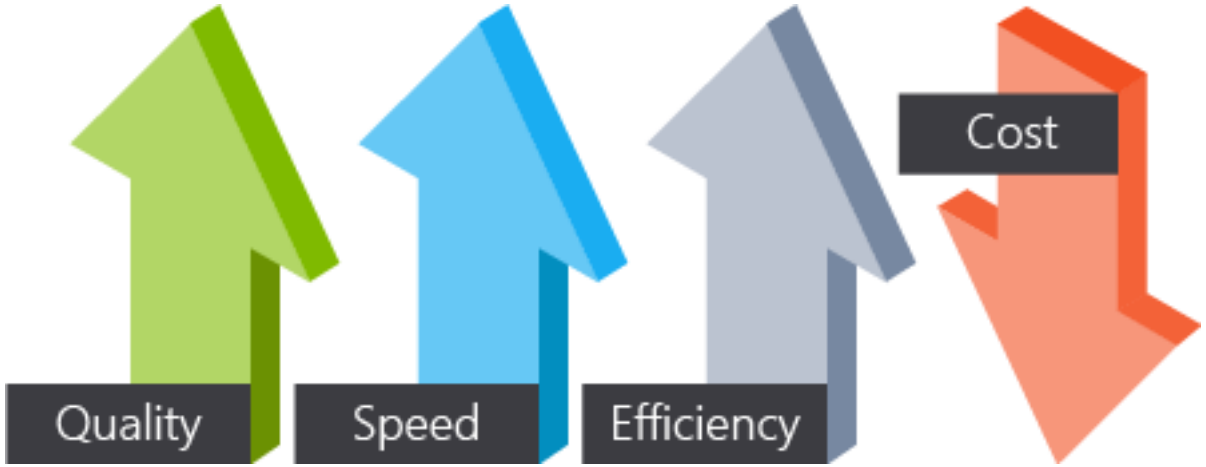
Security

- No access control mechanism (authentication)
- No security thread detection mechanism
- Lack of security thread response plan
- No encryption process

https://aka.ms/architecture/framework

WAF Pillars – Cost Optimization

You'll want to design your cloud environment so that it's cost-effective for operations and development. Identify inefficiency and waste in cloud spending to ensure you're spending money where you can make the greatest use of



WAF Pillars – Cost Optimization – Level 1

1

Cost Management

Start with Advisor recommendations

Review cost over 12 months and identify outliners (Cost analysis)

Review budget and alerts configuration

Operational costs

2

Sizing and plans

Review services sizing against usage pattern

Review SKU and VM classes

Utilization patterns (Auto-shutdown, scaling, spot)

3

Reservations and Licenses

Reserve instances and capacities

Dev/Test vs Prod

Hybrid benefits / Licensing

WAF Pillars – Cost Optimization – Level 2

4

Unused resources

Identify unused resources

Environment on Demand (DevTest Labs, Infra as Code)

Review retention settings (Backup, logs, storage)

5

Location / performances

Region location

Egress traffic charges, VNet peering, Gateways

Disk performances, replication configuration

Content Caching

6

Architecture changes

Architecture design patterns to reduce cost

Workers, Queuing, Caching, Sharding

Compression, code optimization

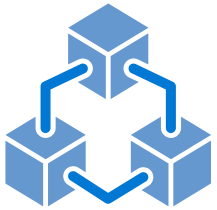
PaaS / Containers

Reservations

Azure Reservations help you save money by committing to one-year or three-years plans for many Azure resources.

- App Service
- Azure Cache for Redis
- Cosmos DB
- Databricks
- Data Explorer
- Disk Storage
- Dedicated Host
- Software plans
- Storage
- SQL Database
- Azure Database for PostgreSQL
- Azure Database for MySQL
- Azure Database for MariaDB
- Azure Synapse Analytics
- Virtual machines
- Log Analytics

WAF Pillars – Reliability



Start with the business requirements – how critical is the application?

- What would happen if the application went down

Is it a custom solution or a solution provided by a software vendor?

What are the SLAs target?

Does the customer have a risk analysis?

SLA targets

SLA	Downtime per week	Downtime per month	Downtime per year
99%	1.68 hours	7.2 hours	3.65 days
99.9%	10.1 minutes	43.2 minutes	8.76 hours
99.95%	5 minutes	21.6 minutes	4.38 hours
99.99%	1.01 minutes	4.32 minutes	52.56 minutes
99.999%	6 seconds	25.9 seconds	5.26 minutes

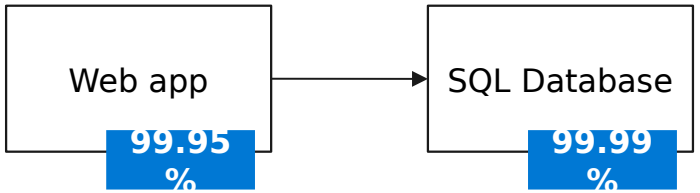
Evaluate the HA capabilities of the application

Focus on **single points of failure** and critical components that would have a large impact on the application if they were unreachable, misconfigured, or started behaving unexpectedly.

Evaluate the HA capabilities of dependent applications

If you are committing an uptime to your customers of 99.9%, but a service your application depends on only has an uptime commitment of 99%, this could put you at risk of not meeting your SLA to your customers.

Composite SLA

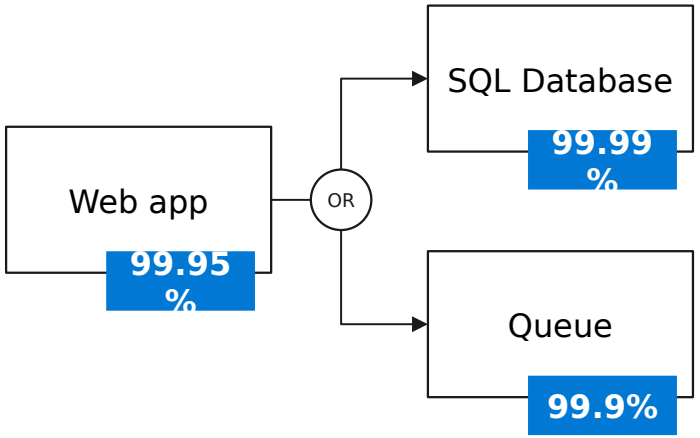


(A) Web App SLA: 99.95%

(B) SQL Database SLA: 99.99%

P(A Failure or B Failure) = P(A) +P(B) = 0.05% + 0.01% = 0.06%

Service A + B: 99.95% x 99.99% = 99.94% SLA



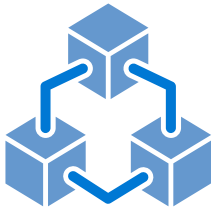
(C) Queue SLA: 99.9%

P(B and C) = P(B) · P(C) = (0.01% x 0.1%) = 0.00001%

(99.99999% SLA)

Web and (database or queue): 99.95% x 99.99999% = ~99.95%

WAF Pillars – Reliability – Level 1



1

Architecture review

Identify type of architecture

Look for single point of failure

Calculate the composite SLA of the application

Discuss redundancy strategy (Zone, Region)

2

Audit SPOF

Load balancing / scale-set

Stateless vs stateful

Chaos Engineering – what happens if X is down

Discuss application level resiliency

3

HA

Review HA requirements

Can the application support HA?

Cost vs Resiliency tradeoff

Data residency ?

WAF Pillars – Reliability – Level 2

4

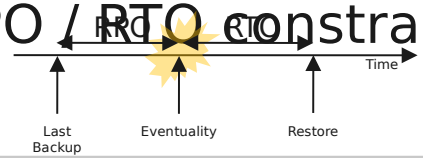
BCDR

Backup strategy

Disaster Recovery Plan

DR Drill / process in place

RPO / RTO constrains



5

Detection & Response

Are health checks in place?

Monitoring and Alerting

Traffic routing configuration

6

Design Patterns

Retry

Fallback

Timeout

Circuit-breaker

Bulkhead

WAF Pillars – Performance

“The application is slow…sometimes”

A user

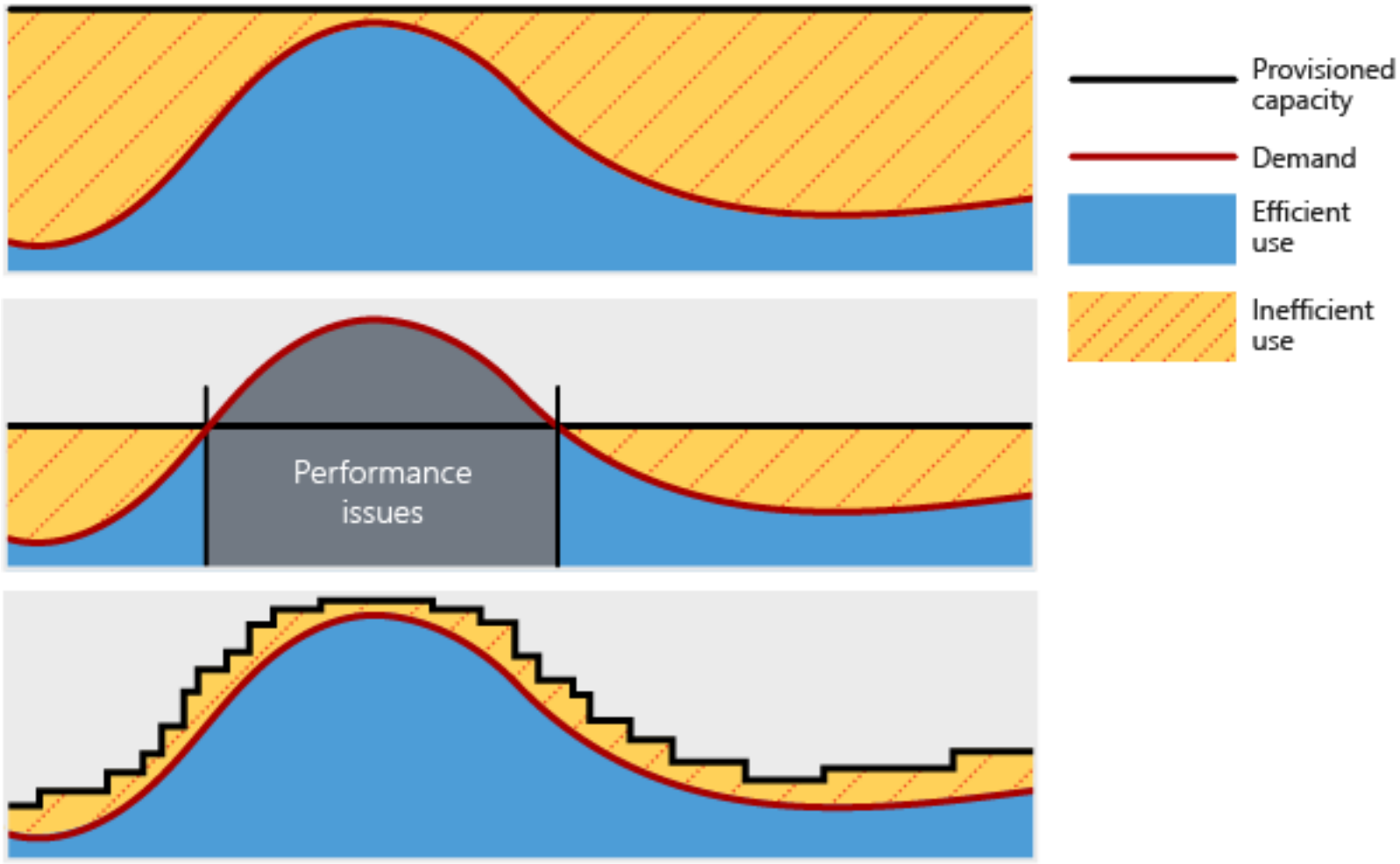
WAF Pillars – Performance

Application performance is tricky but also the most interesting part of Well Architected Review

How a user perceives your performance is as important, or perhaps more important, than any objective statistic, but it's subjective, and not as readily measurable. **Perceived performance is user perspective, not a metric.**

Capture as much data (raw performances) but always include end-users

WAF Pillars – Performance



WAF Pillars – Performances – Level 1

1

Raw performances

VM sizing

Disk IOPS / Throughput

CPU/Mem

Response time

Resource hogging

2

Networking

Network bandwidth

Latency and user distribution

Network path / boundary

CDN

Compression

3

Scaling

Vertical Vs horizontal scaling option

Multi geo-deployment

Scale as independent units

WAF Pillars – Performances – Level 2

4

Backing services

Database performances

Slow queries analysis

Replication and read replicas

Consistency requirements

Data caching /

5

Application design

Queuing and Async processing

Batch / background tasks

Review chatty interactions between components and services

6

Data sharing

Review client affinity

Partitioning and sharding capabilities

Shared-nothing architecture

Review data structure and database type

WAF Pillars – Security

Security is one of the most important aspects of any architecture.

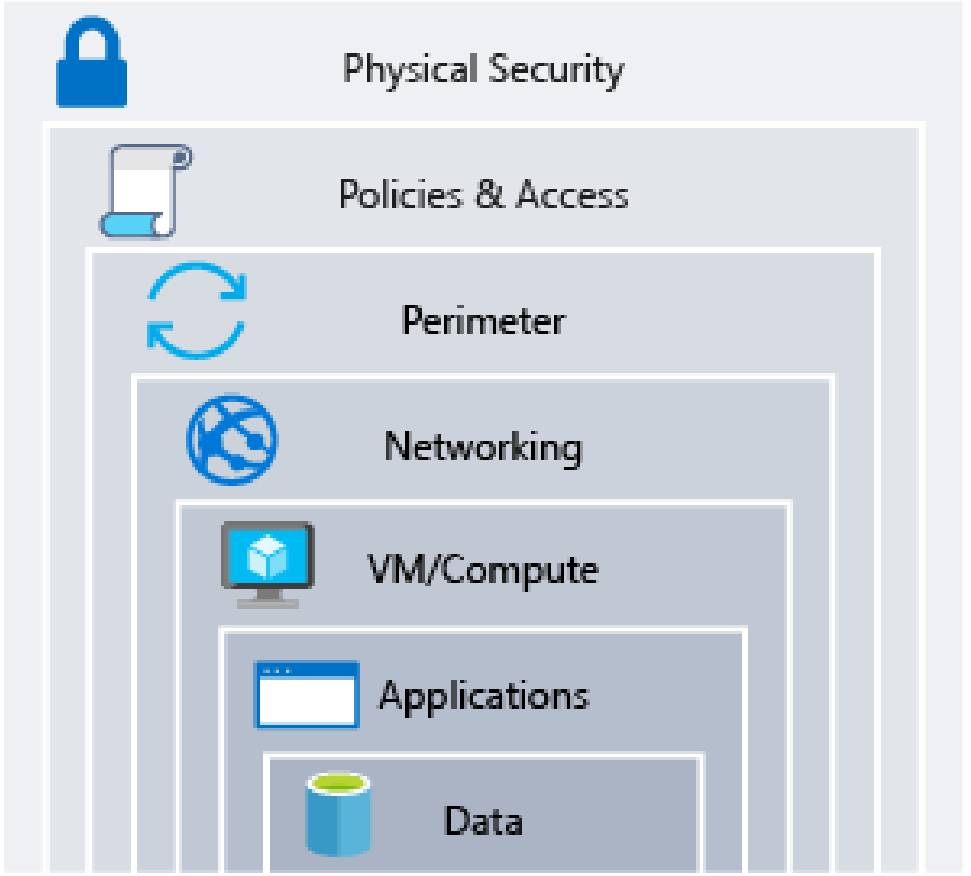
It provides confidentiality, integrity, and availability assurances against deliberate attacks and abuse of your valuable data and system.

Security of complex systems depends on understanding:

- Business context
- Social context
- Technical context

WAF Pillars – Security

A multi-layered approach to securing your environment will increase the security posture of your environment. Commonly known as *defense in depth*, we can break down the layers as in the diagram



Defense in-depth security layers

WAF Pillars – Security – Level 1

1

Identity

How are authentication / authorization managed for App / Resources

Protocols in use

MFA

Managed Identity

2

RBAC

Roles and responsibilities

Access management

Controls in place to access Azure

AD Sync

3

Encryption

Encryption requirements

Server side

OS

Client

WAF Pillars – Security – Level 2

4

Networking

Network perimeter / NSG

Bastion

End-to-end Encryption

WAF & Firewall

Connectivity / public access

5

Keys & Secret

Keys, Secrets and Certificates mgmt

Key rotations and lifecycle

Access policies

BYOK

6

Tools & Processes

Monitoring / Auditing

Vulnerability detection

SIEM / SOAR

Patch & configuration Management

Endpoint Protection

WAF Pillars – Security – Level 3

7

Application

Development lifecycle

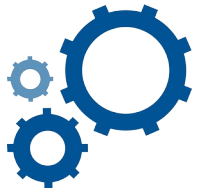
Code scanning and vulnerability assessment

Deployment

Oauth / OpenID

- Azure Security Benchmark
- Azure Security Benchmarks documentation

WAF Pillars – Operational Excellence



Operational excellence is about ensuring that you have full visibility into how your application is running, and ensuring the best experience for your users

1. DevOps and continuous integration in mind
2. Use monitoring and analytics to gain operational insights
3. Use automation to reduce effort and error
4. Test

WAF Pillars – Operational Excellence – Level 1

1

Monitoring

Metrics

Logs

Dashboarding

Alerts

Resource dependencies

2

Resources

Resource organization

Naming convention

Subscription

Management groups

Tenant

3

Deployment

Deployment strategy

Automation tools

Rollback process

Infra as Code

Config Management

WAF Pillars – Operational Excellence – Level 2

4

Testing

Unit Tests

Integration Tests

Code coverage

A main tenet of a DevOps practice to achieve system reliability is the ***shift left*** *principle.*

If your process for developing and deploying an application is depicted as a series of steps that are listed from left to right, your testing should be ***shifted as much as possible toward the beginning of your process (e.g. to the left)****, and not just at the very end of your process (e.g. to the right).*

WAF Pillars – Operational Excellence – Level 3

5

BCDR

Backup strategy

DR strategy

DR Drills

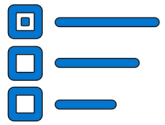
App prioritization

RPO / RTO

Microsoft

Well Architected Review

Prioritize



Prioritization of next steps and recommendations

Provide workload owners a prioritization of “Next Steps” and “Recommendations” so they know what to address **immediately** vs. what is **less urgent**.

1. Clarify the difference between “Next Steps” and “Recommendations.” If “Next Steps” are the first priority tasks, make that very clear, visually and textually.
2. Within both Next Steps and Recommendations, prioritize the order of actions/considerations for the workload owner based on the assessment. Which actions are going to have the biggest impact on cost optimization? What areas are critically underperforming that need to be addressed immediately?
3. Relating the Next Steps/Recommendations back to the question that prompted these suggestions. This will help the solution owner to understand WHY—what are the benefits and

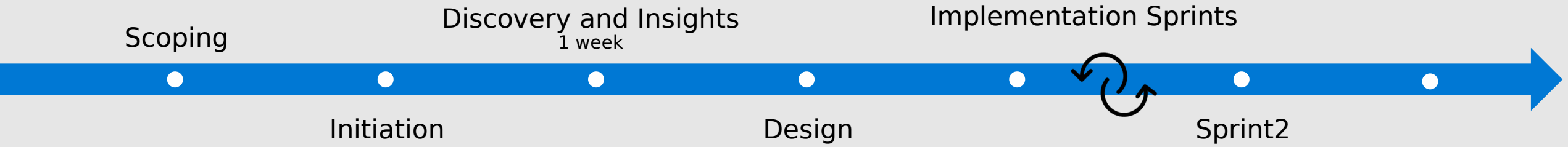
Next Steps

Insights

- Organize and analyze the information you've shared.
- Review the data collected during the discovery workshop. The outcome of this review is an initial design proposal showing how our proven practices address your requirements.

Design

The design workshop begins with a review of the insights from the discovery phase, and the initial design proposal. The design workshops continue to explore the design proposal, highlighting critical areas, and showing how the design elements address your requirements.



Impact and success metrics

Beyond prioritization of ”Next steps” and “Recommendations” provide to the customer key insights on:

- Disruption to production environments
- Estimate on time to complete the remediations
- People and resources in the organization that will need to be involved
- Potential risks identified

Finally agree on success metrics and indicators before the remediation

Review Summar

Scope

The WAF **review phase** is designed to help us better understand customer’s production workloads and platform to identify optimization opportunities and backlog:

- The discussions will be heavily driven on customer scenarios.
- It will be important to understand customers’ priorities from a business perspective. This will guide our optimization proposal.
- will support to run the toolset to capture and document recommended optimizations.

Next phases

Discovery will enable the following activities in the following phases

After this workshop, organize and analyze the information shared by the customer:

- Prepare the initial backlog of optimizations (in Azure DevOps)
- Prioritize with the customer what optimization will be implemented during the following sprints

Microsoft

Well Architected Remediation

Remediation steps

Review → Backup → Communicate → Document
Fix
Test → Validate

Backup

Before any changes – have your checklist ready:

1. All items are backed-up
2. Risk and impact fully documented
3. Rollback procedure is ready, you can return to the previous state

Communicate

Communicate with the stockholders – make a clear RACI

1. Business team / users – any planned disruption
2. Development team – Application changes required / Rollout needed / additional monitoring metrics
3. Ops Team – Changes in cloud resources
4. Security Team – Identity, role, policy changes

Remediate

Remediate items in the prioritized backlog

1. Preferably one item at the time
2. Document and test each remediation
3. Validate the outcome before moving to the next item

At the end of the remediation process review the outcome against agreed KPIs for each of the 5 pillars (Cost, SLAs, response time, time to production…)

Deliverables examples

- Recommendations and Optimizations Plan
- Architecture diagram
- Infra as Code, PowerShell Script, Pipelines
- Azure Monitor Workbook

Questions

Resources

Documentation

- Azure Well-Architected Framework documentation
- Microsoft Learn course
- Architecture center
- Azure Security Benchmark

Tools

- Azure Well-Architected Review
- CCO Dashboard
- AzGovViz
- Cloud adoption Framework tools
- Well-Architected Tools

Microsoft

Thank you

Your Feedback is important!

Link to the presentation:
http://bit.ly/WAFWorkshop

https://forms.office.com/r/z7ZHa7S595

Juan Manuel Servera
Cloud Solution Architect

Based on the work of Nicolas Yuen