



Project Journey

Azure Migration Enablement Program

8 Sept 2020 – 11 Nov 2020

APAC

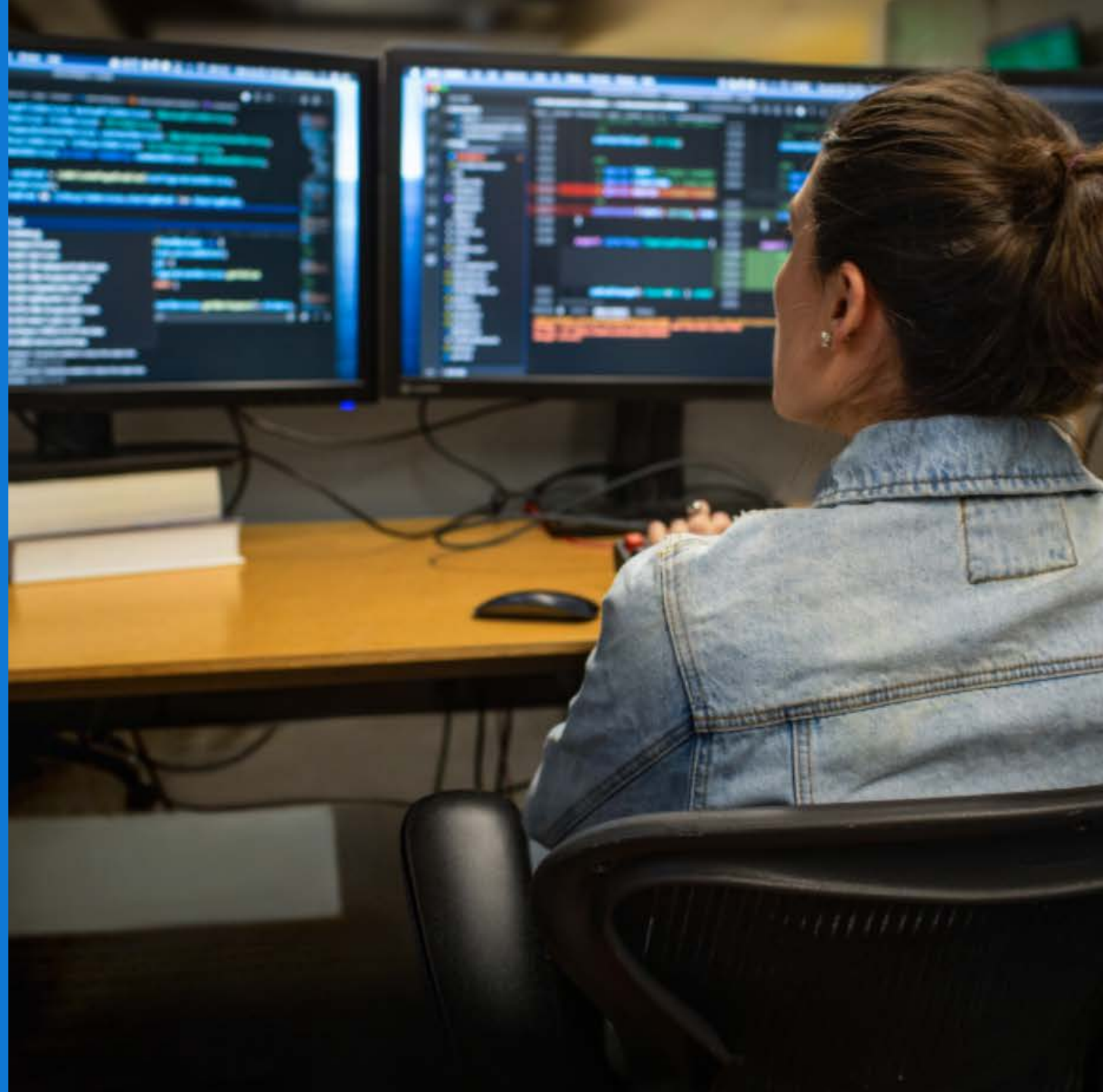
Today's Session

Module 5 – Tuesday 10 November 2020

Please hold while we get the event ready...
Session will start at 10:15am SGT

IMPORTANT NOTICE:

- If you choose to participate in this session using Microsoft Teams, your name, email address, phone number, and/or title may be viewable by other session participants.
- Please note that the training will not and cannot be recorded in alignment with Microsoft's policies



Azure Migration / Project Journey

Module 5 – Continuing the Journey

Jenzus Hsu - Cloud Solution Architect

Nick Westbrook - Cloud Solution Architect

Agenda

Cloud Adoption Framework: Govern

- Governance methodology overview
- Defining initial governance state

Cloud Adoption Framework: Manage

- Establish management baseline
- Advanced operations and design principals

Your feedback is important

Tell us what you think



Nick Westbrook



Jenzus Hsu



Nicolas Yuen



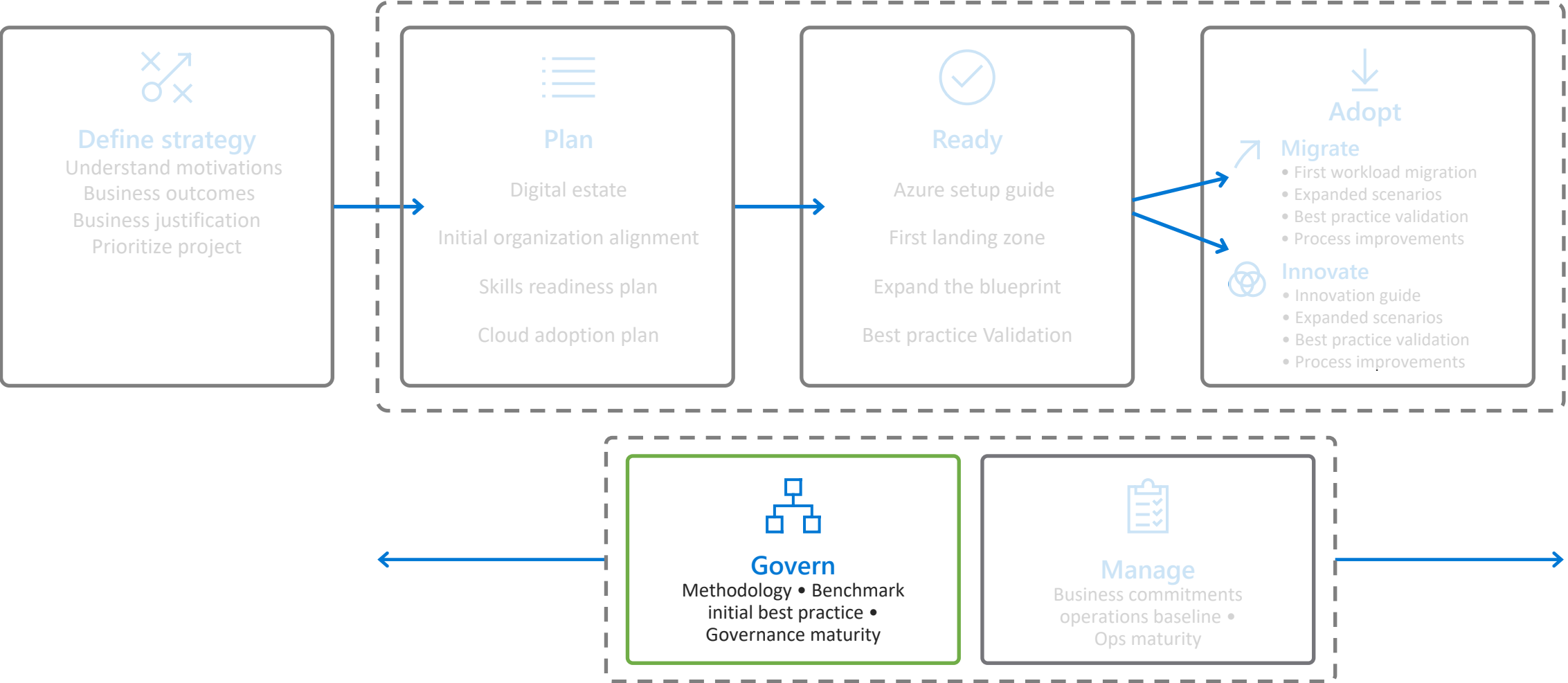
Inseob Kim



<https://aka.ms/JourneySurvey>

Governance with Cloud Adoption Framework

Microsoft Cloud Adoption Framework for Azure



Governance Methodology

Governance Model

Governance End State that fosters trust and builds confidence

Govern <https://aka.ms/adopt/Gov>

Define Corporate Policy



Five Disciplines of Cloud Governance



Cost management

Establish controls and processes to ensure proper allocation of cost across business units, implement cost guardrails, and analyze the cost of applications

Define:

Enterprise Enrollment Hierarchy Process and RACI
Azure Cost Management Budgets and Alerts + RACI
Cost Management RBAC Model

Define **Cost Management Policies**

- Tagging
- Allowed VM SKUs
- Allowed Storage SKUs
- Allowed Networking SKUs
- Allowed Database SKUs

Azure tools and services

- Azure Policy
- Azure Cost Management PBI Application in Azure Market place
- Azure Advisor
- Azure Portal
- Azure EA Content Pack

Security baseline

Establish policies to protect your network, assets, and data—
residing on cloud provider platform(s)

Document risks, business tolerance, and mitigation strategies related to the security of:

- **Data and assets** - develop clear, simple, and well-communicated guidelines to identify, protect, and monitor the most important data assets
- **Network** - control and monitor any allowed communication between on-premises environment and cloud workloads.

Implement these best practices for corporate policy:

- **Network requirements** - on-premises networks must be secured against potential unauthorized access from cloud-based resources.
- **Hybrid identity strategies** - a key factor in structuring cloud-based identity services is the level of integration required with existing on-premises identity infrastructure.
- **Encryption** - encryption mechanisms vary in cost and complexity, and both technical and policy requirements and can influence decisions on how encryption is applied and how to store and manage critical secrets and keys
- **Security Baseline policies** - processes that manage updates to security policy based on inputs from stakeholders. (e.g., initial risk assessment and planning, deployment planning and testing, and quarterly review and planning)

Azure tools and services

- Azure Policy
- Azure Security Center
- Azure Sentinel
- Subscription Design
- Encryption
- Hybrid Identity
- Azure Networking
- Azure Automation

Resource consistency

Implement the foundation for governance best practices—
with correct resource organization

Define Azure Management Groups & Subscriptions model and RACI

- To reflect security, operations and business/accounting hierarchies
- To group similar resources into logical collections

Define resource consistency roles & responsibilities

- To further group applications or workloads into deployment and operations units

Define Resource Consistency Policies

- Naming Conventions
- Tagging
- Allowed Locations
- Allowed Resource Types
- Allowed Extensions
- Auditing

Azure tools and services

- Azure Policy
- Azure Monitor
- Azure Advisor
- Resource Manager Templates
- Resource Graph
- Management Groups

Identity baseline

Protect your data and assets in the cloud—
implementing identity management and access control.

Define Azure RBAC Model –

- Using RBAC can segregate duties within a team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in an Azure subscription or resources, only certain actions with narrow scope can be allowed.

Define Azure Access Management Process and RACI

- Several options are available for managing identity in a cloud environment which vary in cost and complexity.
- A key factor in structuring your cloud-based identity services is the level of integration required with existing on-premises identity infrastructure.

Operationalize Azure Privileged Identity Management

- Cloud-based identity management is an iterative process.

Azure tools and services

- RBAC
- Azure AD
- Azure AD B2B
- Azure AD B2C
- Directory Federation
- Directory Replication

Deployment acceleration

Establish policies to govern asset configurations or deployments—manual, or automated through DevOps best practices

The DevOps practices in this discipline include

Infrastructure as Code

- Stand up environments in the fastest means possible.
- Remove the human element and reliably and repeatably deploy every time.
- Improve environment visibility and improve developer efficiency
- Store infrastructure definitions alongside application code.

Continuous Integration and Continuous Deployment

- Accelerate delivery through automation
- Simple and easy to use
- Global community for actions

Azure services that enable deployment acceleration include Azure Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Azure tools and services

- Resource Manager Templates
- Azure PowerShell
- Azure CLI
- Azure Policy
- Resource Grouping & Tagging
- Azure DevOps
- Github – Azure Github Actions
- Azure Automation

Making Governance Actionable with Native Tools

Govern <https://aka.ms/adopt/Gov>

Define Corporate Policy

Business Risks

Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality

Policy & Compliance

Convert Risk decisions into policy statements to establish cloud adoption boundaries.

Process

Establish processes to monitor violations and adherence to corporate policies.

Five Disciplines of Cloud Governance



Cost Management

Evaluate & monitor costs, limit IT spend, scale to meet need, create cost accountability



Security Baseline

Ensure compliance with IT Security requirements by applying a security baseline to all adoption efforts



Resource Consistency

Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability



Identity Baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments



Deployment Acceleration

Accelerate deployment through centralization, consistency, and standardization across deployment templates

Azure Monitor

- Azure Blueprints
- Azure Policy
- Azure Cost Management
- Azure Advisor
- Azure Portal
- Azure EA Content Pack

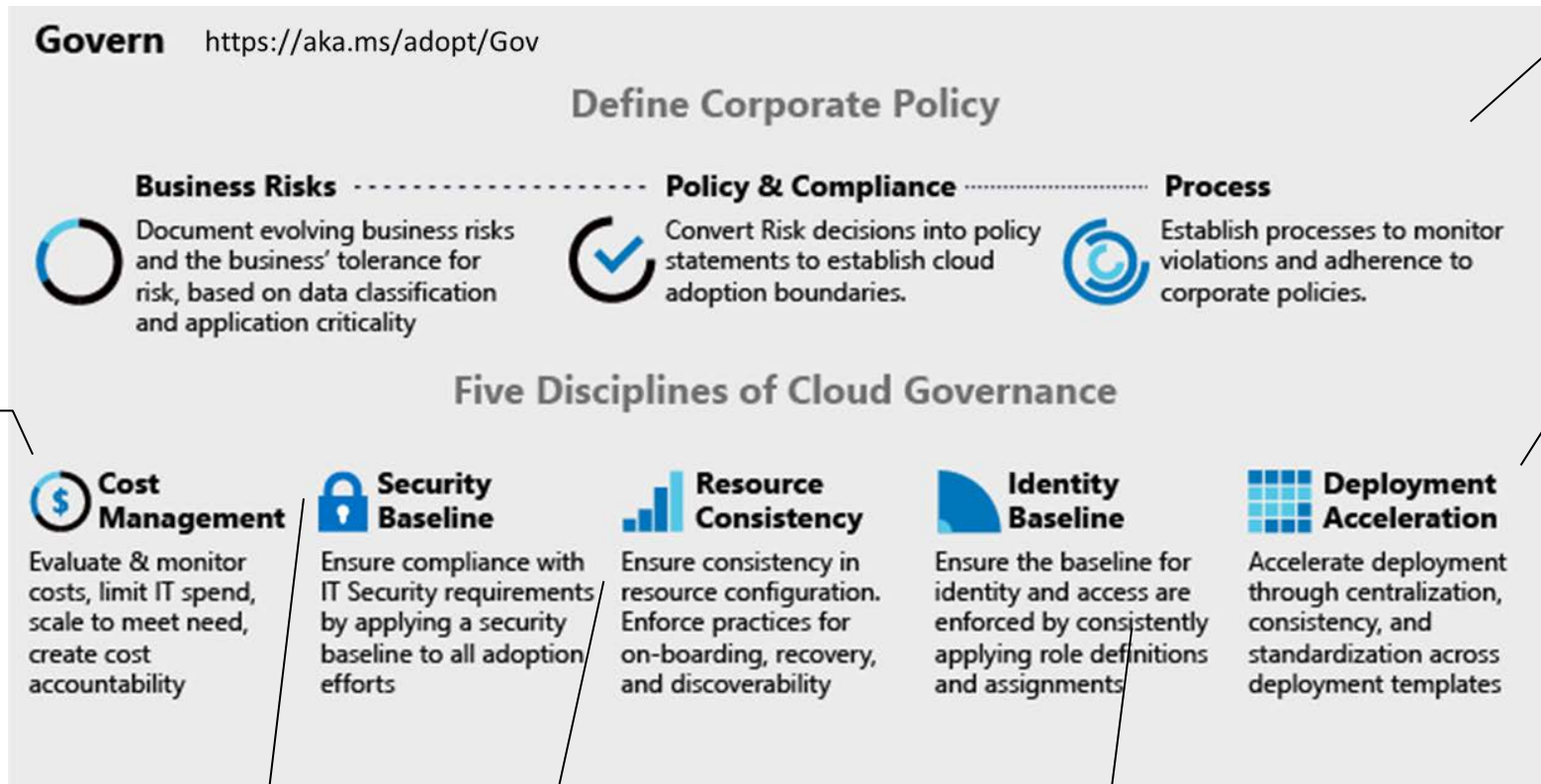
- Azure Blueprint
- Azure Policy
- Resource Grouping & Tagging
- Resource Manager Templates
- Azure Advisor
- Azure DevOps
- Azure Site Recovery
- Azure Backup
- Azure Automation

- Azure Blueprints
- Azure Policy
- Azure Security Center
- Azure Sentinel
- Subscription Design
- Encryption
- Hybrid Identity
- Azure Networking
- Azure Automation

- Azure Blueprints
- Azure Policy
- Azure Monitor
- Azure Advisor
- Resource Manager Templates
- Resource Graph
- Management Groups

- Azure Blueprints
- RBAC
- Azure AD
- Azure AD B2B
- Azure AD B2C
- Directory Federation
- Directory Replication

Integrating 3rd Party Tools



Cost Management 3rd parties

- HashiCorp Terraform (ROI tools)
- Cloudcheckr

Monitoring 3rd parties

- OpsCompass
- Splunk
- AppDynamics
- Solarwinds
- New Relic
- Data Dog

Deployment 3rd parties

- Nagios
- HashiCorp Terraform
- devops tools like Chef, Puppet, Ansible, Zabix

Security baseline 3rd parties

- Splunk
- HashiCorp Vault
- F5
- Gemalto
- Palo Alto
- CheckPoint
- Dome9

Discovery, onboarding, and recovery 3rd parties

- ServiceNow
- HashiCorp Terraform

3rd party identity providers

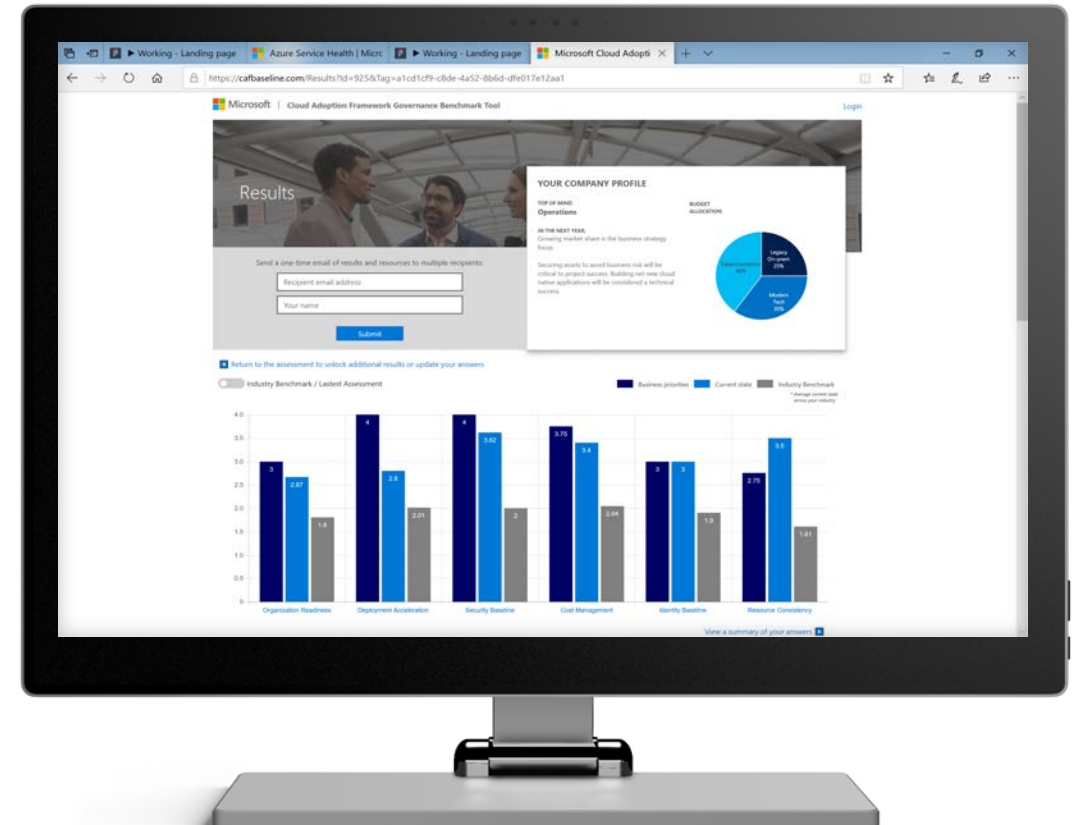
- HashiCorp Vault
- RSA
- Omada
- Ping Identity
- SailPoint

Benchmark your governance state

Make governance **actionable** with **processes and policies**—

Use the **Governance benchmark tool**—

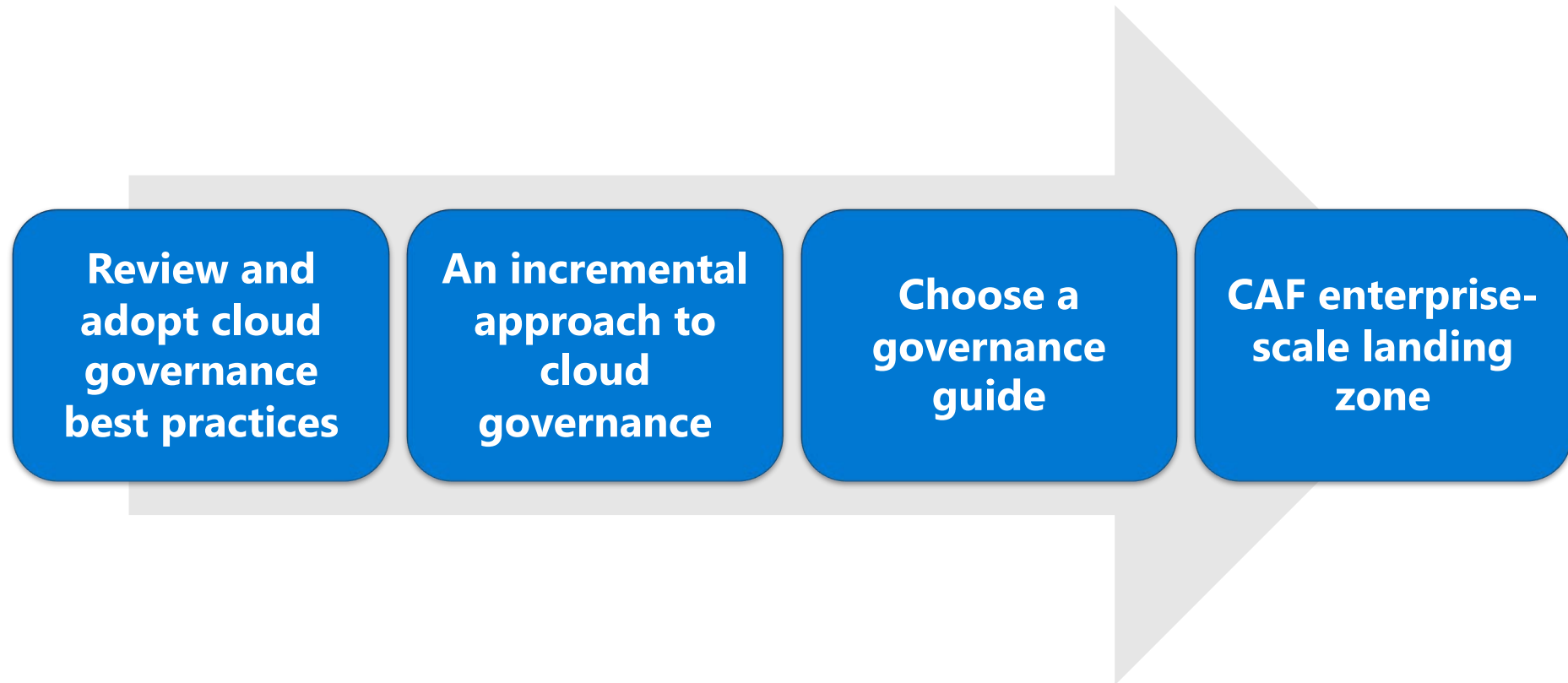
- Establish a governance baseline **and recommended starting-point**
- Understand gaps **between your desired and current governance state, using the Cloud Adoption Framework.**
- Remove blockers **with curated guidance on how to build a proper Governance foundation.**



<https://cafbaseline.com/>

Demo: Governance Benchmark Tool

Cloud governance guides

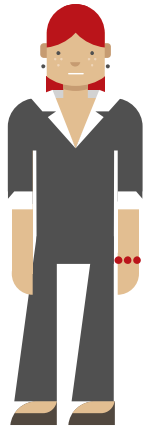


Resource Consistency

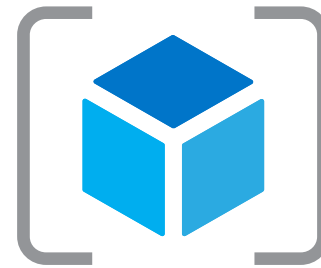
Resource Groups, Tags and RBAC

Finance/Business

Need to be able to break out costs by various dimensions such as Customer, Cost Center, Environment



Create Roles with
Appropriate
Permissions



Always Tag!

- Owner
- Dept.
- Environment
- Application
- (Cost Center)



Resources in a RG should
be tagged as needed



Best Practices on using Resource Tags: <https://azure.microsoft.com/documentation/articles/resource-group-using-tags/>
Custom RBAC Roles: <https://azure.microsoft.com/documentation/articles/role-based-access-control-custom-roles/>
Manage tag governance with Policy: <https://docs.microsoft.com/azure/governance/policy/tutorials/govern-tags>

Resource Consistency



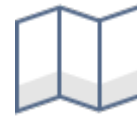
[Resource Consistency discipline template](#)
Download the template for documenting a Resource Consistency discipline.



[Policy adherence processes](#)
Suggested processes for supporting policy compliance in the Resource Consistency discipline.



[Business risks](#)
Understand the motives and risks commonly associated with the Resource Consistency discipline.



[Maturity](#)
Align cloud management maturity with phases of cloud adoption.



[Indicators and metrics](#)
Indicators to understand if it is the right time to invest in the Resource Consistency discipline.



[Toolchain](#)
Azure services that can be implemented to support the Resource Consistency discipline.

Cost Management Tools in Azure

This is a list of Azure native tools that can help mature the policies and processes that support this governance discipline.

Tool	Azure portal	Azure Cost Management	Azure EA Content Pack	Azure Policy
Enterprise Agreement required?	No	No	Yes	No
Budget control	No	Yes	No	Yes
Monitor spending on single resource	Yes	Yes	Yes	No
Monitor spending across multiple resources	No	Yes	Yes	No
Control spending on single resource	Yes - manual sizing	Yes	No	Yes
Enforce spending across multiple resources	No	Yes	No	Yes
Enforce accounting metadata on resources	No	No	No	Yes
Monitor and detect trends	Yes	Yes	Yes	No
Detect spending anomalies	No	Yes	Yes	No
Socialize deviations	No	Yes	Yes	No

Determine Identity Integration Requirements

Question	Cloud baseline	Directory synchronization	Cloud-hosted domain services	Active Directory Federation Services
Do you currently lack an on-premises directory service?	Yes	No	No	No
Do your workloads need to use a common set of users and groups between the cloud and on-premises environment?	No	Yes	No	No
Do your workloads depend on legacy authentication mechanisms, such as Kerberos or NTLM?	No	No	Yes	Yes
Do you require single sign-on across multiple identity providers?	No	No	No	Yes

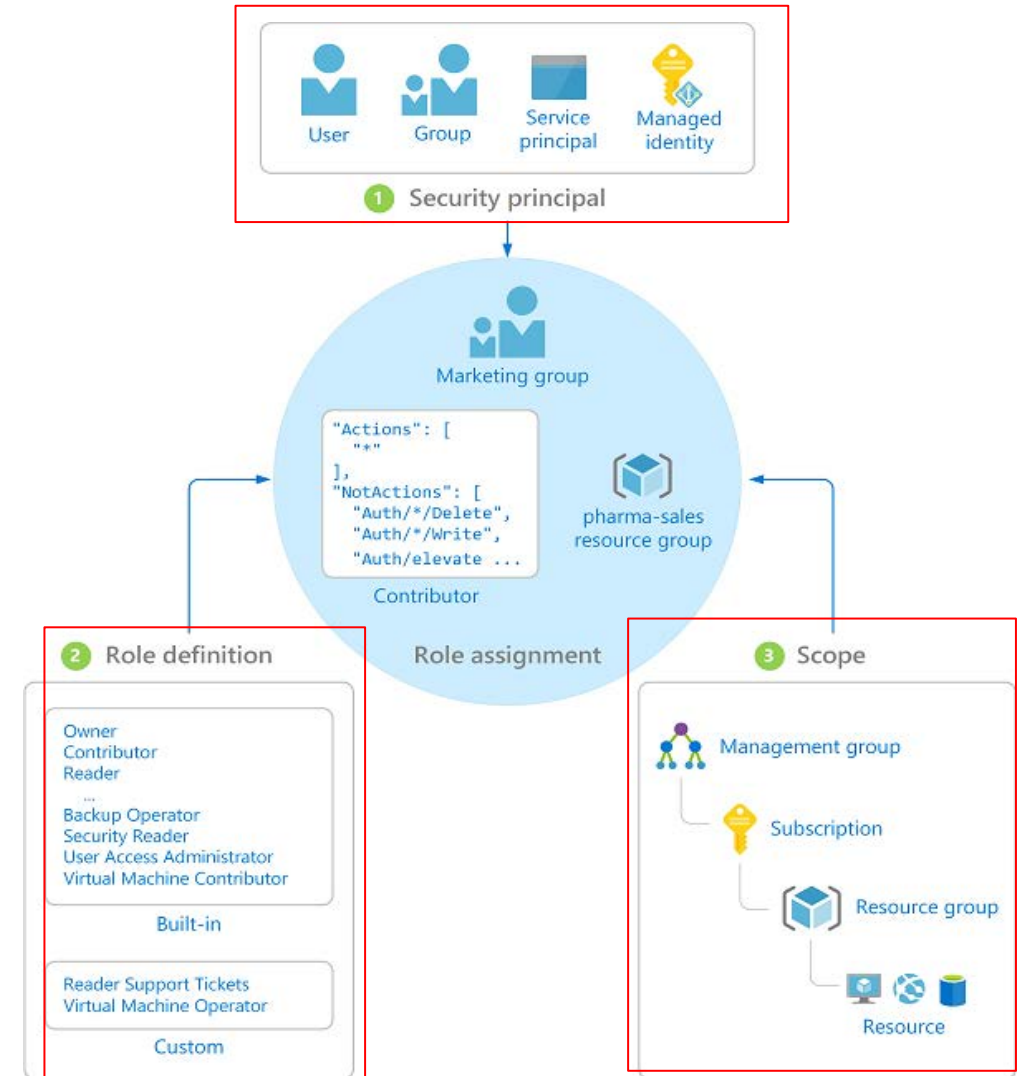
Azure Role-Based Access Control (RBAC)

Fine-grained access control to Azure "control plane"

Grant access by assigning Security Principal a Role at a Scope

- Security Principal: User, group, or service principal
- Role: Built-in or custom role
- Scope: Subscription, resource group, or resource

Assignments are inherited down the resource hierarchy



Learn more <https://aka.ms/azureiam>

Security baseline tools in Azure

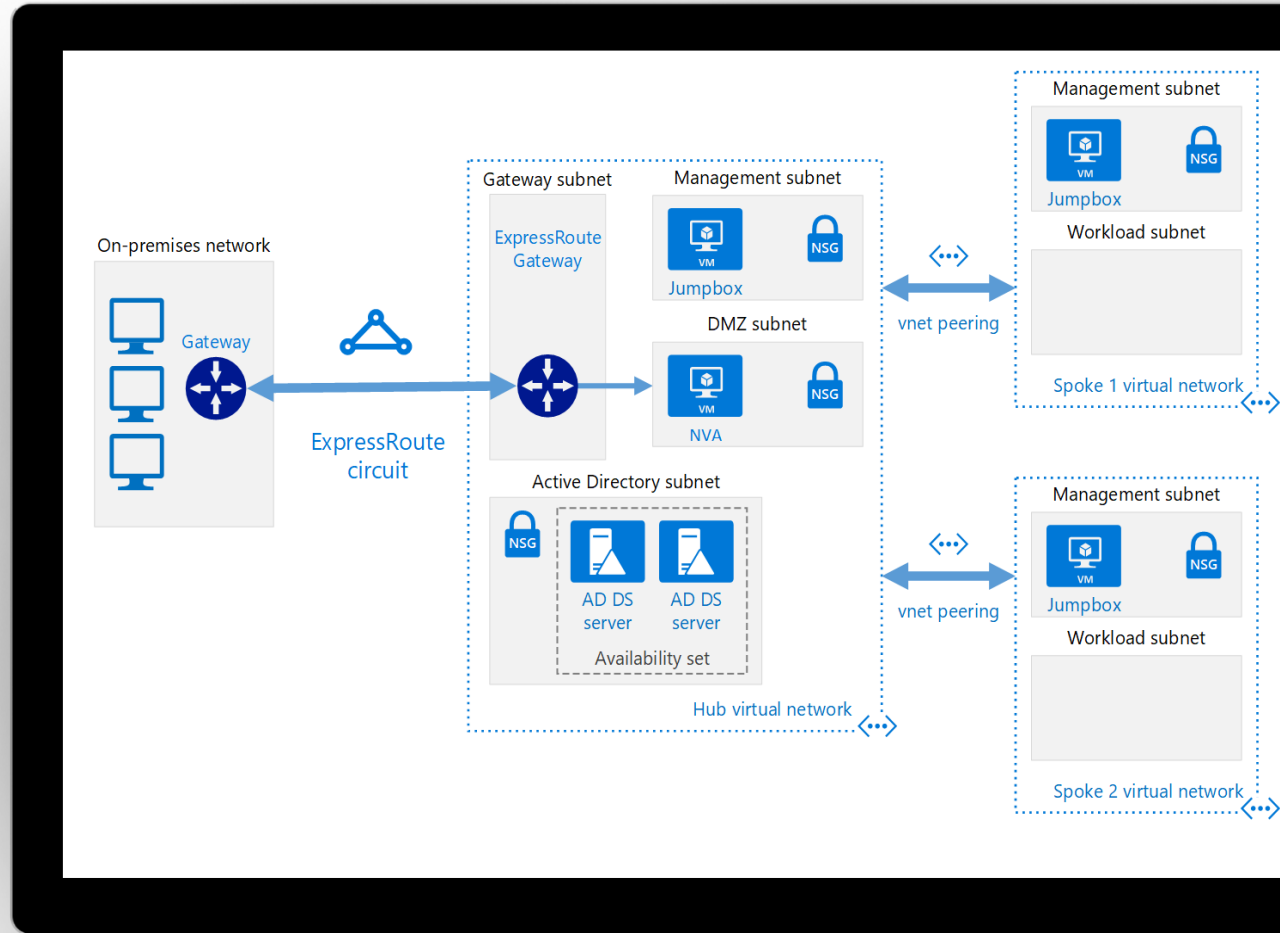
These Azure tools can help mature the policies and processes that support Security Baseline.

Tool	Azure portal and Azure Resource Manager	Azure Key Vault	Azure AD	Azure Policy	Azure Security Center	Azure Monitor
Apply access controls to resources and resource creation	Yes	No	Yes	No	No	No
Secure virtual networks	Yes	No	No	Yes	No	No
Encrypt virtual drives	No	Yes	No	No	No	No
Encrypt PaaS storage and databases	No	Yes	No	No	No	No
Manage hybrid identity services	No	No	Yes	No	No	No
Restrict allowed types of resource	No	No	No	Yes	No	No
Enforce geo-regional restrictions	No	No	No	Yes	No	No
Monitor security health of networks and resources	No	No	No	No	Yes	Yes
Detect malicious activity	No	No	No	No	Yes	Yes
Preemptively detect vulnerabilities	No	No	No	No	Yes	No
Configure backup and disaster recovery	Yes	No	No	No	No	No

For a complete list of Azure security tools and services, see [Security services and technologies available on Azure](#).

Azure Terraform Landing Zones

- ✓ Aligned on Cloud Adoption Framework
- ✓ Enterprise grade - Inspired by FSI requirements
- ✓ Best practices in a-box
- ✓ Lower entry cost to Infrastructure as Code
- ✓ Community based
- ✓ Easy to customize | deploy | reuse
- ✓ Comes with prescriptive deployment techniques



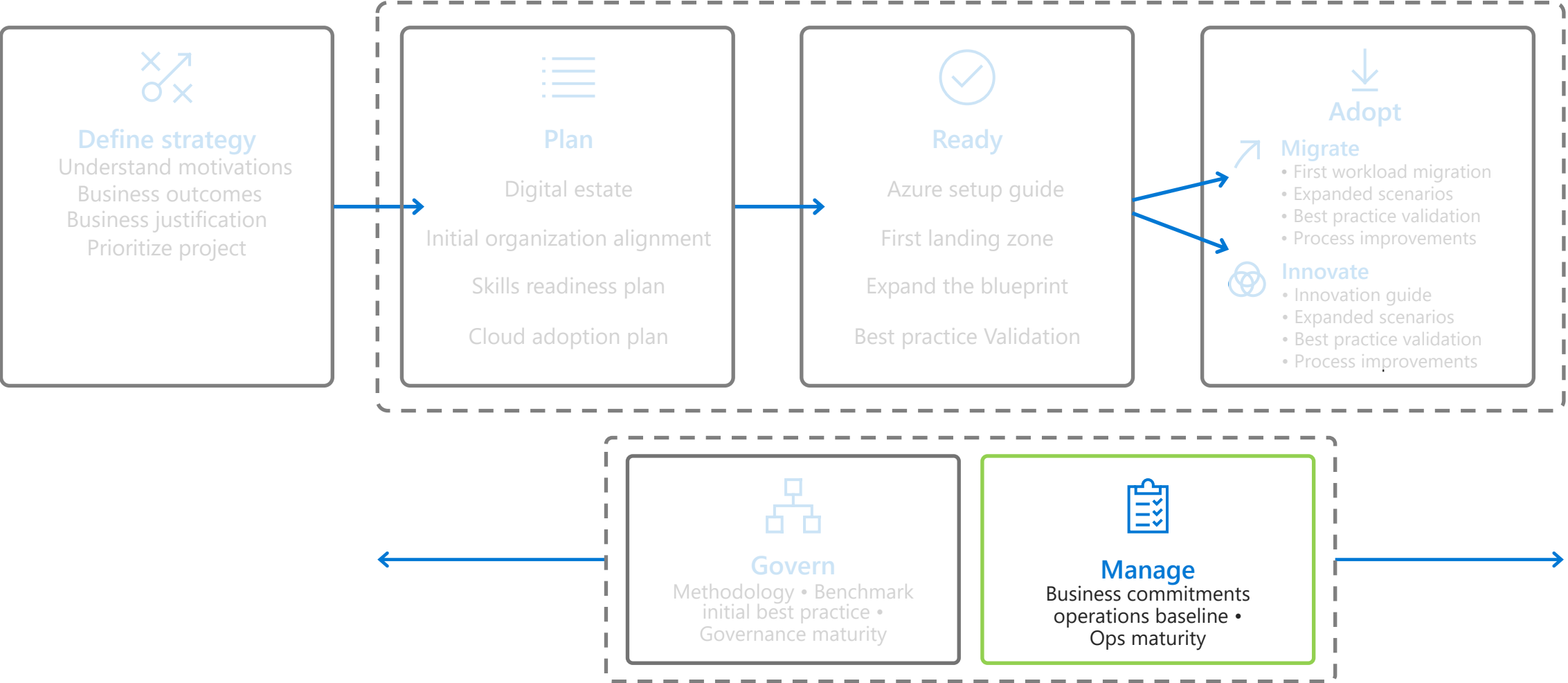
Deployment Acceleration Tools in Azure

These Azure tools that can help mature the policies and processes that support this governance discipline.

	Azure Policy	Azure Management Groups	Azure Resource Manager	Azure Blueprints	Azure Resource Graph	Azure Cost Management
Implement corporate policies	Yes	No	No	No	No	No
Apply policies across subscriptions	Required	Yes	No	No	No	No
Deploy defined resources	No	No	Yes	No	No	No
Create fully compliant environments	Required	Required	Required	Yes	No	No
Audit policies	Yes	No	No	No	No	No
Query Azure resources	No	No	No	No	Yes	No
Report on cost of resources	No	No	No	No	No	Yes

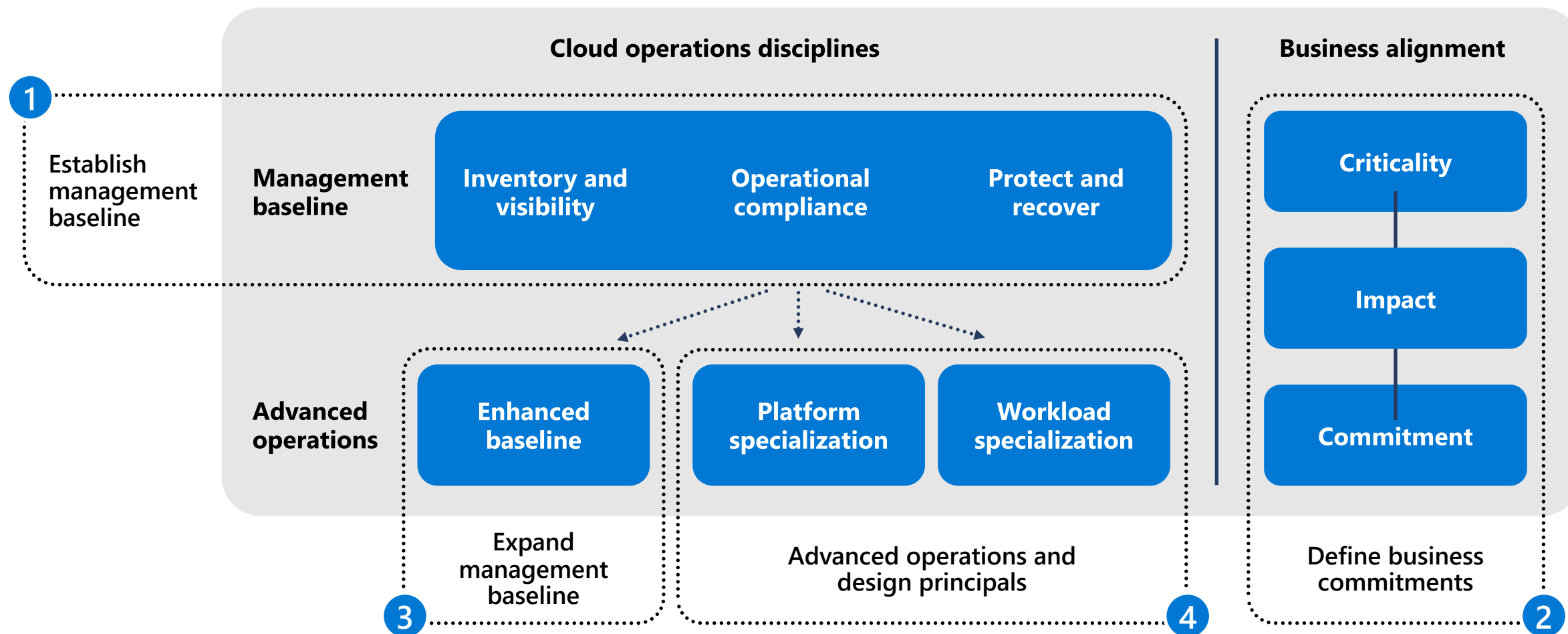
Demo: Azure Portal

Microsoft Cloud Adoption Framework for Azure



Establish Management Baseline

Methodology to Enable Cloud Management



Inventory and Visibility

Management baseline

Create an inventory of assets across multiple clouds, and develop deep visibility into the run state of each asset

- ✓ Each monitoring tool has been configured with **proper access and scope** for each operations team
- ✓ Each asset must be **inventoried and classified** towards stable operations
- ✓ **Centralization of logging** drives reports about change management, service health, and configuration for IT operations
- ✓ **Awareness and understanding of technical changes** across multiple workloads is essential for reliable operations
- ✓ Understand the **telemetry about the stability, performance, and operations** of the workload, and the assets which support the workload

Azure Tools and Services

- ✓ Service health
- ✓ Log analytics
- ✓ Azure change tracking and inventory service
- ✓ Azure activity log
- ✓ Azure monitor for VMs
- ✓ Azure network watcher
- ✓ DNS analytics

Management
baseline

Inventory
and visibility

Protect and Recover

Management baseline

Ensure all managed assets are protected and can be recovered using baseline management tooling

- ✓ **Protect and recover** business critical workloads in the cloud to anticipate and prepare for a potential workload outage
- ✓ **Define plans** to back up, protect, and recover your data and VMs in Azure
- ✓ Get **short- and long-term backup** without the need to deploy complex on-premises backup solutions
- ✓ **Replicate VMs and workloads** to the secondary location to ensure business continuity
- ✓ **Failover to secondary location**, and access apps and workloads even during outages

Azure tools and services

- ✓ Azure Backup
- ✓ Azure Site Recovery

Management
baseline

Protect and
recover

Understanding Business Impact

Business alignment

Understand the impact of potential outages to aid in evaluating return on investment for cloud management

- ✓ Business impact **serves as a prioritization variable** when recovering systems during an outage.
- ✓ **Calculate impact time** depending on the nature of workloads, from high to low frequency of workload usage
- ✓ **Calculate the total business impact** more accurately with three approaches, including adjusted losses, historical losses, and complete loss calculation
- ✓ **Calculate workload impact**, which must be attributed across each of the workloads

Azure tools and services

- ✓ Operations management workbook

Business alignment

Impact

Ops Management Planning Workbook

Help capture decisions that result from business alignment conversations

	A	B	C	D	E	F	G	H	I	J	K
1	Microsoft Cloud Adoption Framework for Azure										
2	Operations Management - Commitment alignment										
3											
4	Business inputs			Ops management responses							
5	Workload	Criticality	Time/Value impact	Commitment Level	Composite SLA	Monthly Cost	Est. Outage**	Standard In	Commitm	Comparison basis	Annual ROI
6	SAP	Mission Critical	\$ 1,000,000.00	High Availability Comm	99.9999%	\$ 100,000.00	0.00876	\$ 8,760,000	\$ 8,760.00	\$ 8,751,240.00	629%
7	Logistics	Mission Critical	\$ 1,000,000.00	High Availability Comm	99.9990%	\$ 30,000.00	0.08760	\$ 8,760,000	\$ 87,600.00	\$ 8,672,400.00	2309%
8	eCommerce	High	\$ 200,000.00	Platform Commitmen	99.9900%	\$ 1,000.00	0.87600	\$ 1,752,000	\$175,200.00	\$ 1,576,800.00	13040%
9	Payroll	Medium	\$ 10,000.00	Platform Commitmen	99.9500%	\$ 1,000.00	4.38000	\$ 87,600	\$ 43,800.00	\$ 43,800.00	265%
10	Marketing	Medium	\$ 10,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 87,600	\$ 87,600.00	\$ 87,600.00	7200%
11	workload 6	Medium	\$ 10,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 87,600	\$ 87,600.00	\$ 87,600.00	7200%
12	workload 7	Medium	\$ 10,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 87,600	\$ 87,600.00	\$ 87,600.00	7200%
13	workload 8	Medium	\$ 5,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 43,800	\$ 43,800.00	\$ 43,800.00	3550%
14	workload 9	Medium	\$ 5,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 43,800	\$ 43,800.00	\$ 43,800.00	3550%
15	workload 10	Medium	\$ 5,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 43,800	\$ 43,800.00	\$ 43,800.00	3550%
16	workload 11	Medium	\$ 5,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 43,800	\$ 43,800.00	\$ 43,800.00	3550%
17	workload 12	Medium	\$ 5,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 43,800	\$ 43,800.00	\$ 43,800.00	3550%
18	workload 13	Low	\$ 1,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 8,760	\$ 8,760.00	\$ 8,760.00	630%
19	workload 14	Low	\$ 1,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 8,760	\$ 8,760.00	\$ 8,760.00	630%
20	workload 15	Low	\$ 1,000.00	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ 8,760	\$ 8,760.00	\$ 8,760.00	630%
21	workload 16	Mission Critical	\$ 1,000.00	Standard Commitmen	99.9000%	\$ 20,000.00	8.76000	\$ 8,760	\$ 8,760.00	\$ 8,760.00	-96%
22	workload 17	Low	\$ -	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ -	\$ -	\$ -	-100%
23	workload 18	Low	\$ -	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ -	\$ -	\$ -	-100%
24	workload 19	Low	\$ -	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ -	\$ -	\$ -	-100%
25	workload 20	Low	\$ -	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ -	\$ -	\$ -	-100%
26	workload 21	Low	\$ -	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ -	\$ -	\$ -	-100%
27	workload 22	Low	\$ -	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ -	\$ -	\$ -	-100%
28	workload 23	Low	\$ -	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ -	\$ -	\$ -	-100%
29	workload 24	Low	\$ -	Standard Commitmen	99.9000%	\$ 100.00	8.76000	\$ -	\$ -	\$ -	-100%

Platform Specialization

Advanced operations

Invest in ongoing operations of a specific workload, generally reserved for mission-critical workloads

Platform specialization consists of a disciplined execution of the following **processes in an iterative approach**

- ✓ **Improve the design** of common systems (platforms) or specific workloads by considering best practices for architecture frameworks with Azure Architecture Frameworks
- ✓ **Minimize business interruptions** with Azure Architecture Framework by improving systems designs with scalability, availability, resiliency, security, and management
- ✓ **Automate remediation** and reduce the impact of interruptions
- ✓ **Scale changes** across the environment through the service catalog
- ✓ **Discover incremental improvements** to address in the next pass of system design, automation, and scale

Azure tools and services

- ✓ Azure Managed Applications
- ✓ Azure Monitor for containers
- ✓ Azure SQL analytics
- ✓ SQL Server health check
- ✓ Azure Automation
- ✓ Azure Architecture Framework

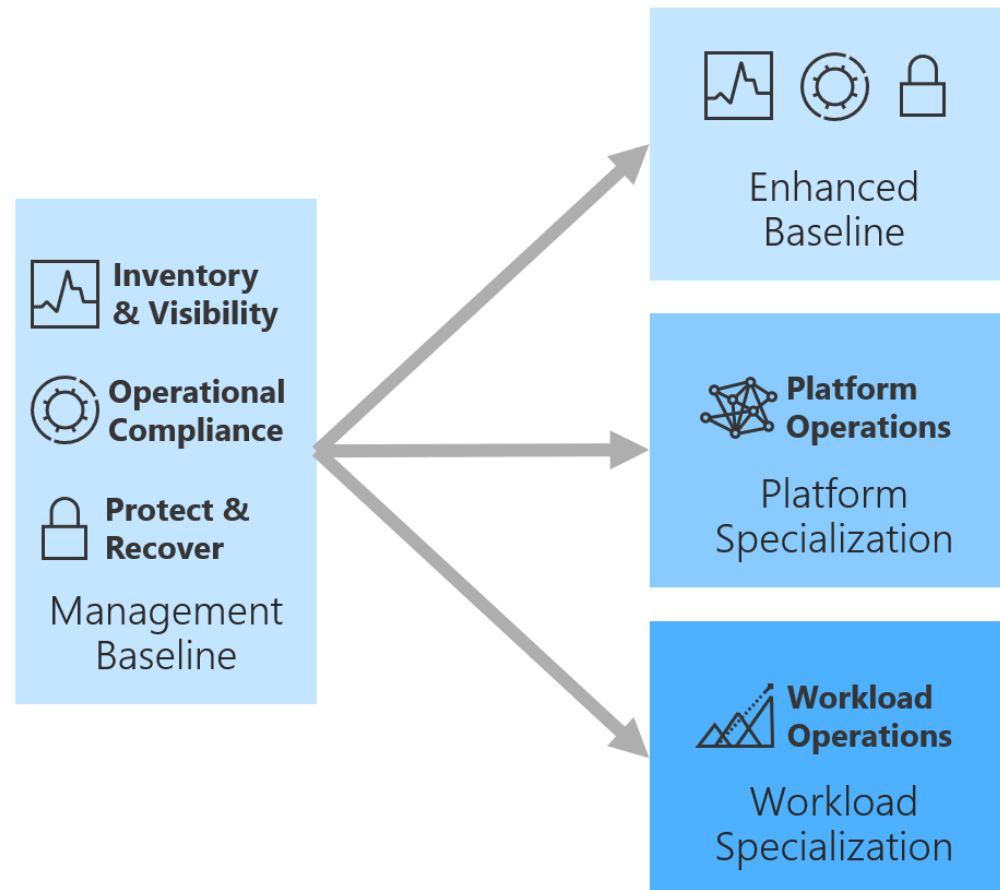
Platform operations

**Platform
specialization**

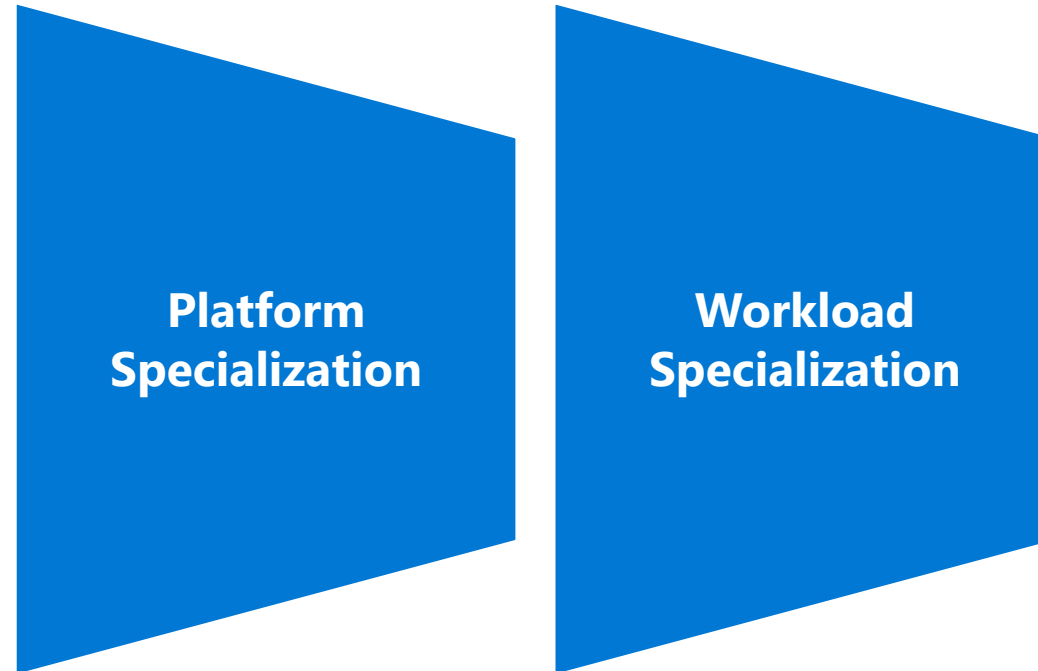
Demo: Azure Architecture Review

Advanced Operation and Design Principles

Advanced Operations Options








Areas of Management Specialization





homework

Homework

Topic		Link
Build a Cloud Governance strategy		https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/
Apply and monitor infrastructure standard with Azure Policy		https://docs.microsoft.com/en-us/learn/modules/intro-to-governance/
Predict Cost and optimize spending		https://docs.microsoft.com/en-us/learn/modules/predict-costs-and-optimize-spending
Azure policies repository		https://github.com/Azure/azure-policy
		https://github.com/Azure/Community-Policy
		https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/policy-as-code-github
Security baseline Hands on Lab		https://github.com/microsoft/MCW-Security-baseline-on-Azure

Q&A

Contact us - projectjourney@microsoft.com

Your feedback is important

Tell us what you think



Nick Westbrook



Jenzus Hsu



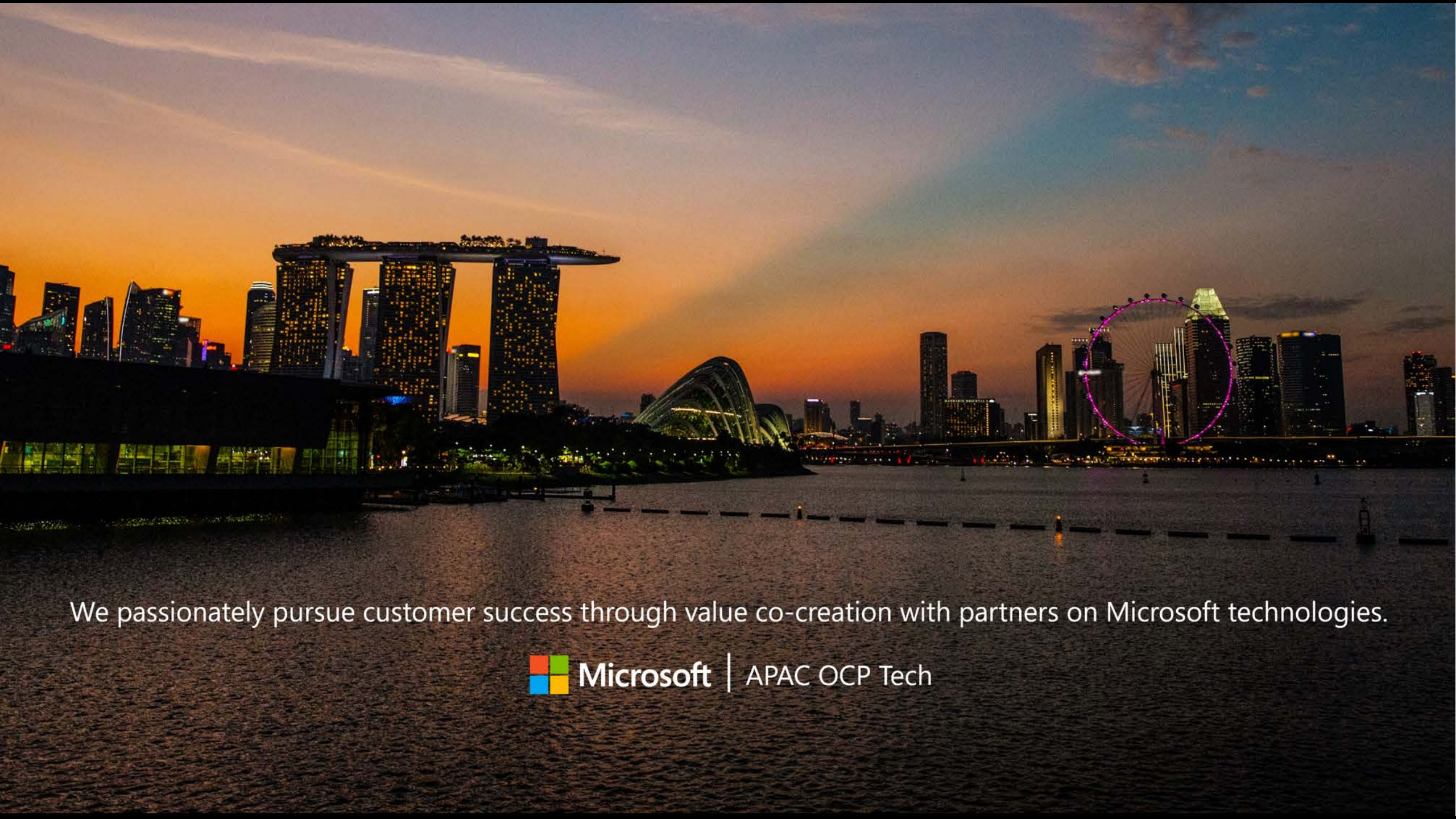
Nicolas Yuen



Inseob Kim



<https://aka.ms/JourneySurvey>



We passionately pursue customer success through value co-creation with partners on Microsoft technologies.

