Microsoft

SAP on Azure Enablement

Wednesday, Oct 14, 2020

Nicolas Yuen
APAC, Singapore

Module Two – Week Two

Day 2 – Tuesday, Oct 19th, 2020

IMPT 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**

SAP on Azure Partner Enablement

Module Two – Week Two

Day 2 – Azure Governance

Ravi Gangampalli
Cloud Solution Architect–
SAP on Azure

Nicolas Yuen
Cloud Solution Architect

Check-in

We are happy to host you ☺

https://aka.ms/apac-enablement-check-in

https://aka.ms/apac-sap-enablement

Agenda

What is Cloud Governance?

Cloud Governance tools in Azure

Resource Organization

Enforcing compliance

Cost Management

Identity

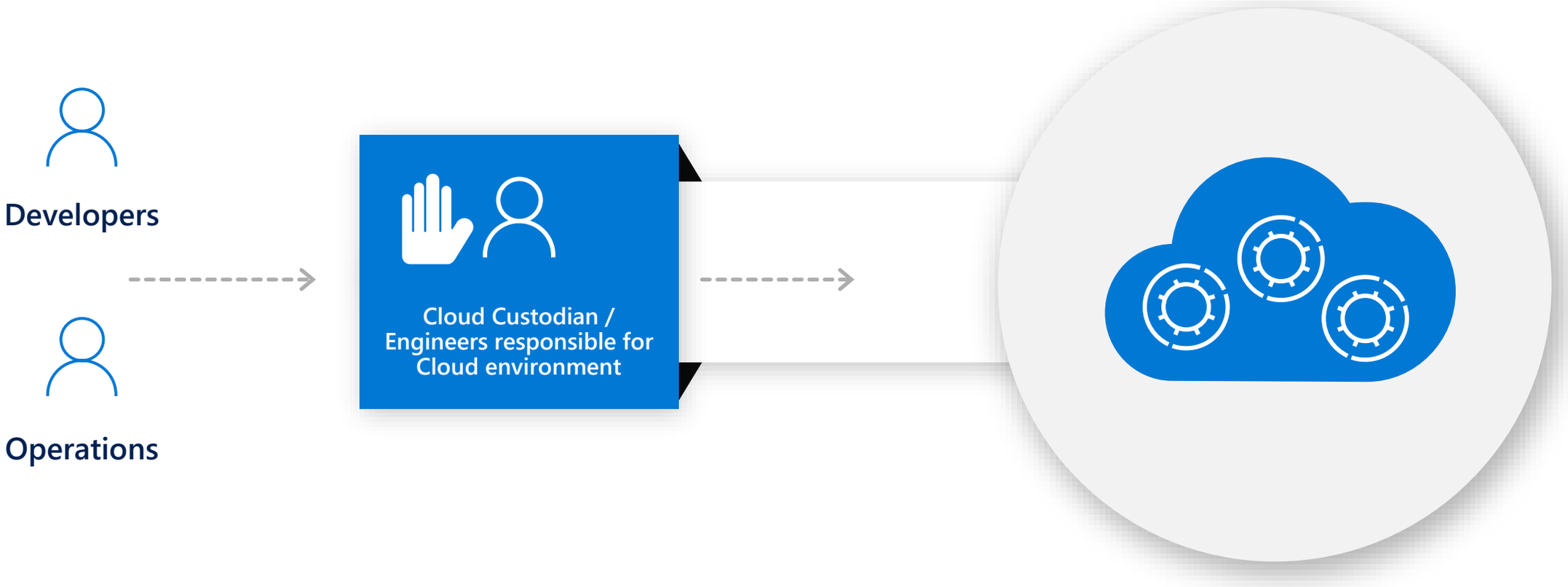
Govern

The major drivers for IT governance

- Keep risk at acceptable levels
- Maintain availability to systems and services
- Consistently apply policy and audit compliance
- Protect customer data

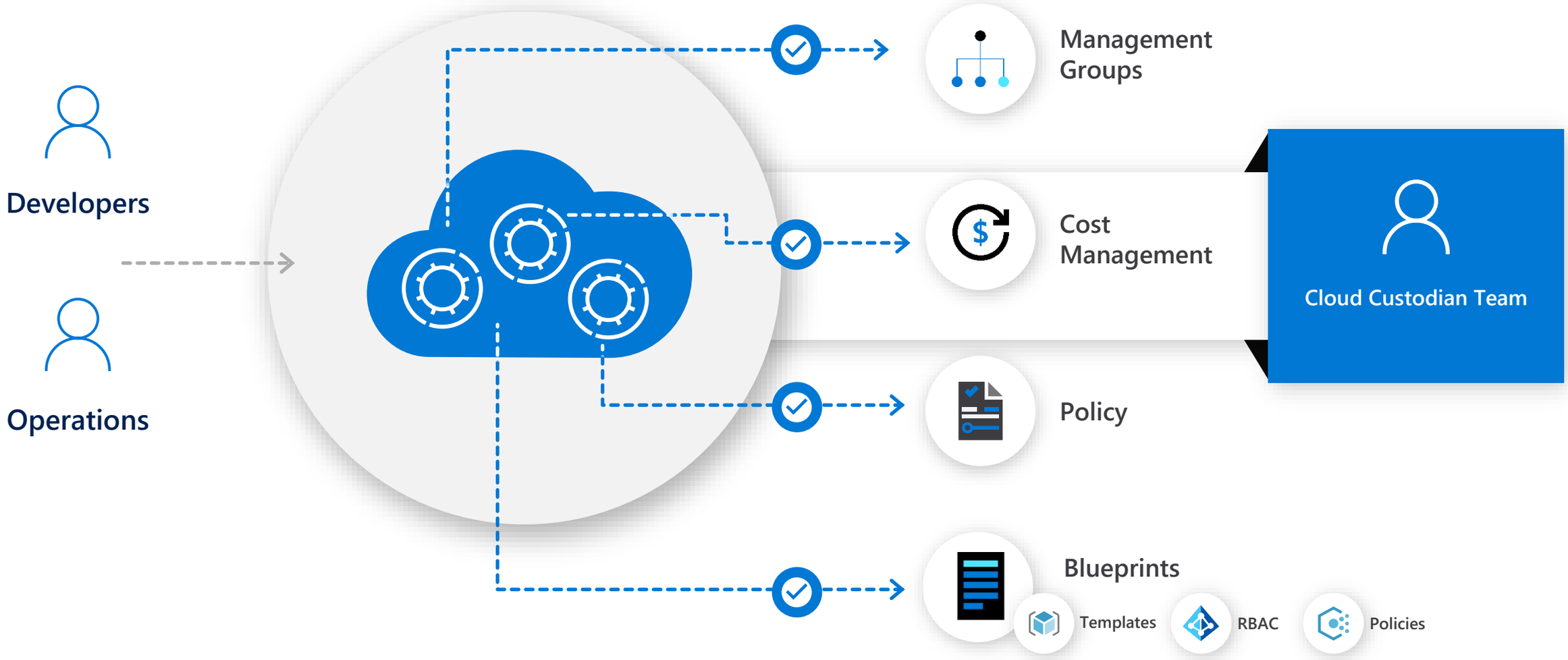
Traditional approach

Block Dev/Ops from directly accessing the cloud (portal/api/cli) to attain control



Speed + Control

Cloud-native governance -> removing barriers to compliance and enabling velocity



Govern

Policy definition ensures consistency across adoption efforts. Alignment to governance/compliance requirements is key to maintain a well-managed cross-cloud environment.

Business risk

- **Document** evolving business risk
- Document risk tolerance based on **data classification**, and **application criticality**

Policy & compliance

- Convert risk decisions into **policy statements**
- Establish cloud adoption boundaries

Processes

- Establish processes to **monitor violations**
- Adhere to corporate policies
- **Cloud Center of Excellence**

Cost management

- Evaluate and monitor cost
- Limit IT spend
- Scale based on business demand
- Create cost accountability

Security baseline

- Compliance with IT Security requirements
- Apply security baseline to all adoption efforts

Resource consistency

- Consistency in resource configuration
- Enforce on boarding, recovery and discoverability practices

Identity baseline

- Enforce identity and access baseline
- Apply role definitions and assignments

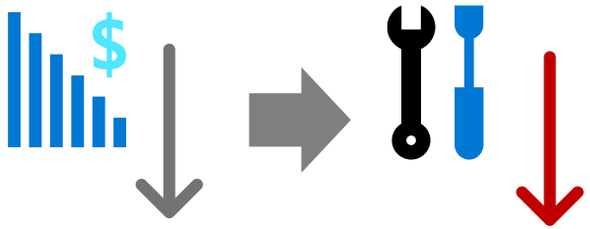
Deployment acceleration

- Centralize templates
- Drive consistency and standardization

Doing business means making trade-offs

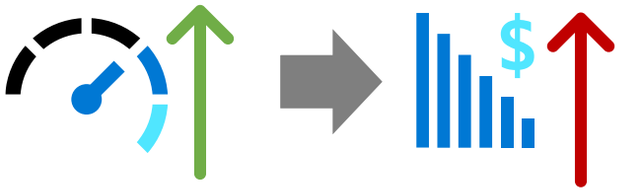
Business requirements influence workload architecture decisions

DEVELOPMENT WORKLOADS



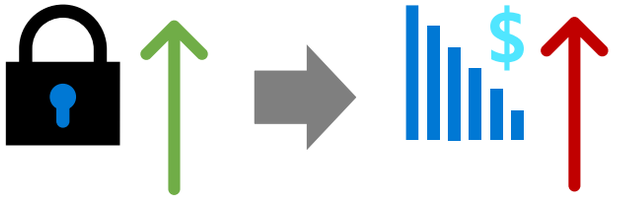
Optimizing costs in dev workloads may be the right approach, even when it may impact reliability, if it is in line with business expectations

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

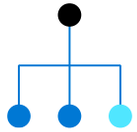
https://aka.ms/architecture/framework

Resource organization

Azure Management Groups

Efficiently apply governance controls and manage groups of Azure subscriptions

1. Ensure compliance
2. Empower DevOps
3. Manage costs

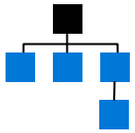


Simplify subscription management

Group subscriptions into logical groups

Inherit properties that apply to all subscriptions

View aggregated information above the subscription level

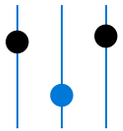


Fit your organization

Create a flexible hierarchy that can be updated quickly

Mirror the hierarchy to the organizational model that works for you

Scale up or down depending on the organizational needs



Apply controls at scale

Leverage Azure Resource Manager (ARM) objects that integrate with other Azure services

Azure services:

Azure Policy

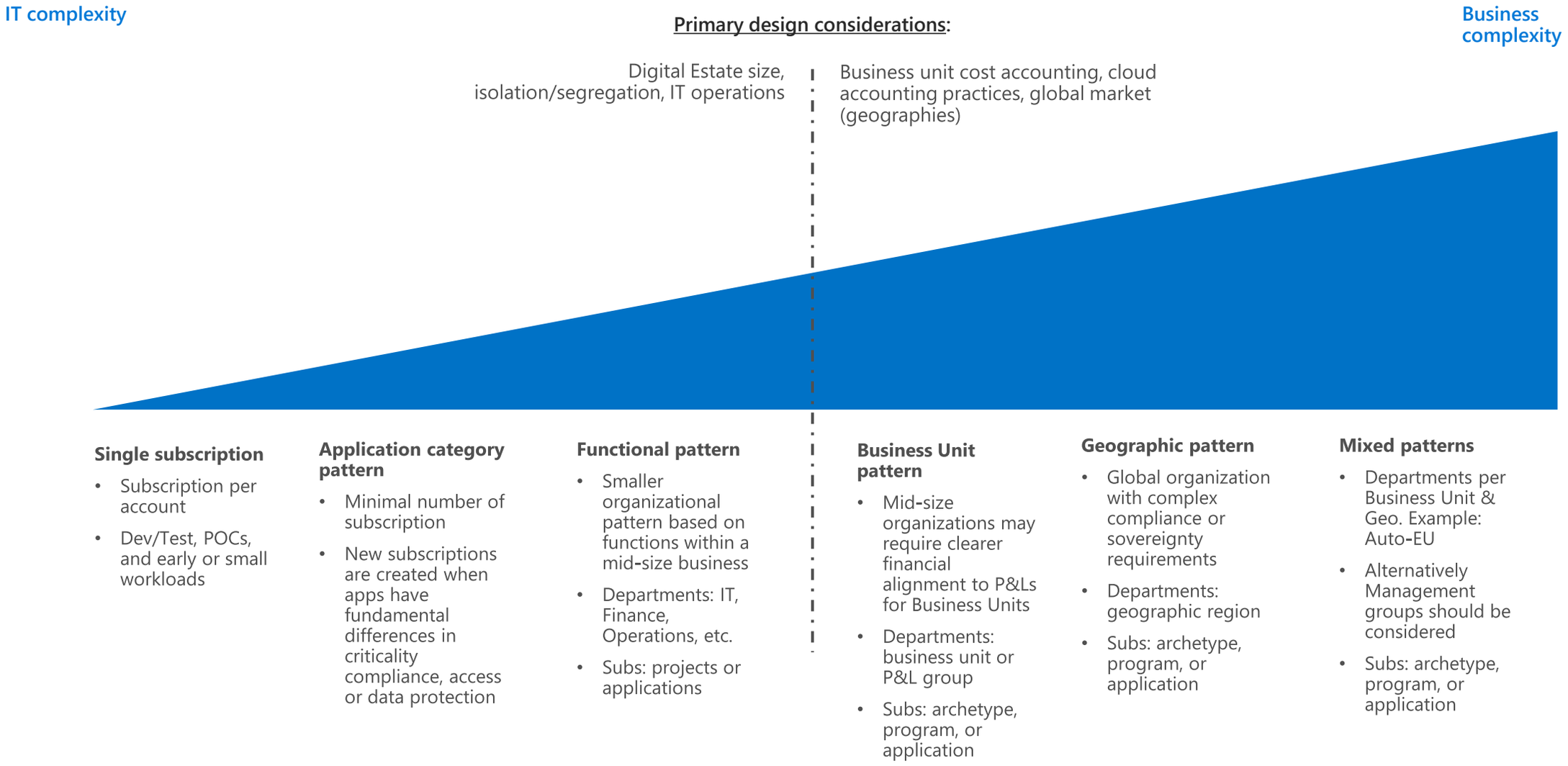
RBAC

Azure Cost Management

Azure Blueprints

Azure Security Center

Subscription design considerations

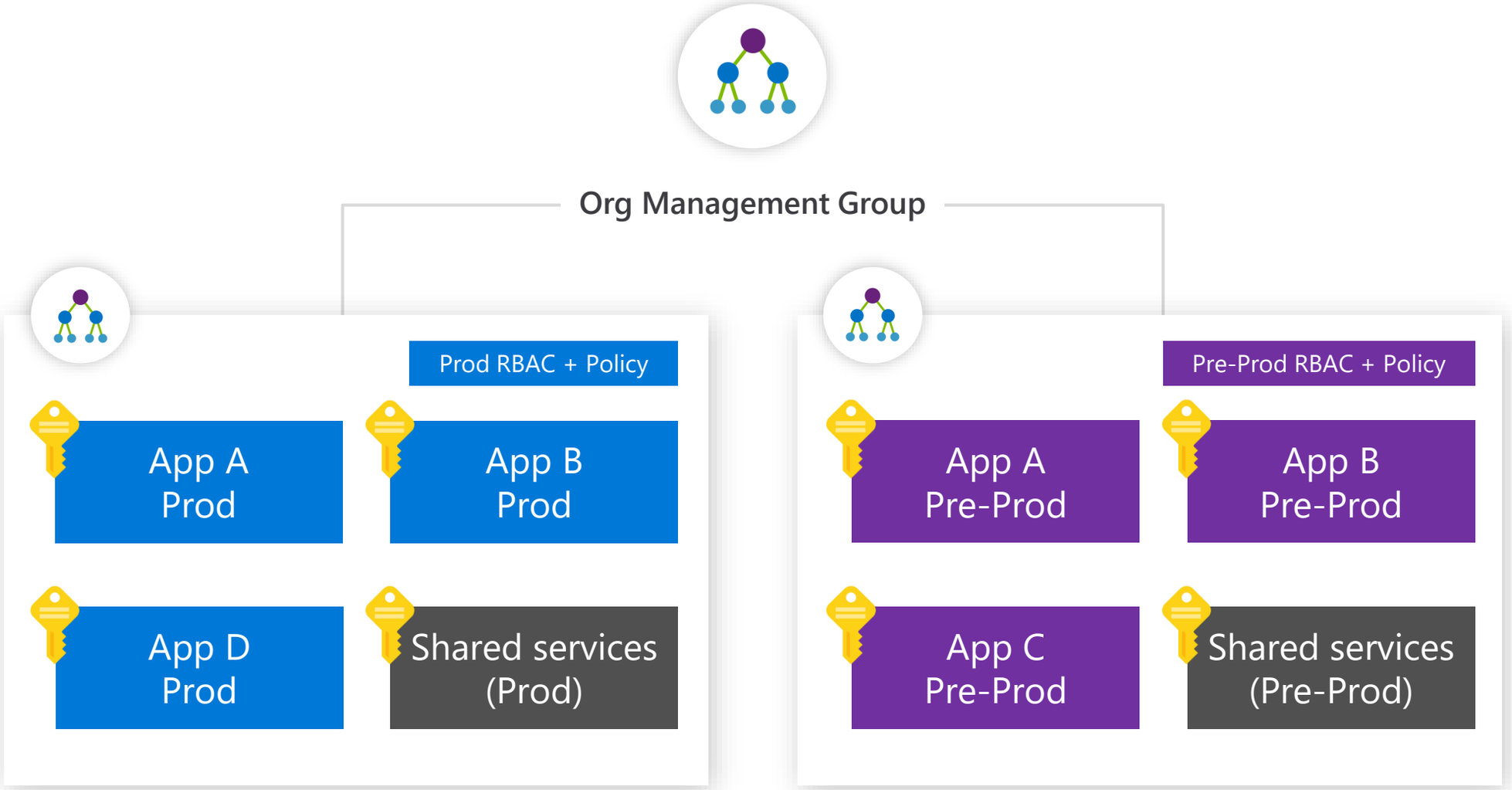


https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/decision-guides/subscriptions/

Management Group & subscription modeling strategy

1 Ensure compliance
2 Empower DevOps
3 Manage costs

Microsoft recommended



Managed tenants & subscriptions

Critical best practices

BEST PRACTICE CHOICE

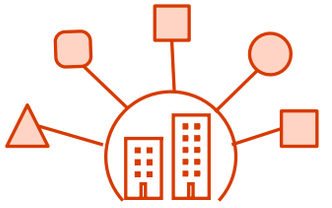
MANAGE CONNECTED TENANTS

- **What** – Ensure security organization has visibility into all subscriptions connected to your enterprise environment (via ExpressRoute or Site-Site VPN)
- **Why –** Visibility is required to assess risk and to identify whether the policies of the organization and any regulatory requirements are being followed
- **How** – Ensure all Azure environments that connect to your production environment/network apply IT governance

See http://aka.ms/magicbutton on how to discover existing connected tenants

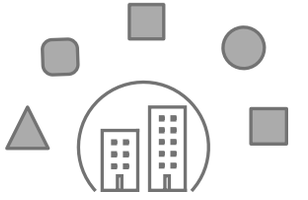
Managed & Connected

Ideal configuration is for subscriptions to be centrally controlled and managed



Unmanaged & Connected

This high-risk configuration has unmanaged azure environments connected to corporate network/resources



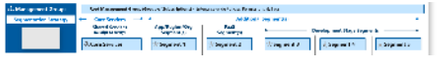
Independent Un/Managed

This model can be useful for learning and testing, but ensure to protect any production data or code appropriately

Source: Azure Security Compass v1.0

Management groups

Critical best practices



Azure Administration Model
Management Groups

ROOT MANAGEMENT GROUP

- **What** – Use the Root Management Group (MG) for enterprise consistency
- **Why –** This enables you to apply governance elements like policies, permissions, etc. consistently across multiple subscriptions
- **How –** Assign enterprise-wide elements that apply to all Azure assets such as:
  - Policy (Azure Policy)
  - Enterprise Permissions (RBAC)
  - Resource Tags
  - Sovereignty Policy for Data/Services

See next slide for "Root MG Usage" guidance and MG documentation

TOP LEVEL MANAGEMENT GROUPS

- **What** –Align top level of management groups (MGs) with segmentation strategy
- **Why –** This provides a point for control and policy consistency within each segment as this management group will affect all subscriptions in it
- **How –** Create a single MG for each segment under the root MG and do not create any other MGs under the root

MANAGEMENT GROUP DEPTH

- **What** – Limit management group depth
- **Why –** Too much complexity creates confusion that hampers both operations and security. This was illustrated by overly complex Organizational Unit (OU) and Group Policy Objects (GPO) designs for Active Directory
- **How** – Limit to 2 levels if possible and 3 only if needed. (e.g. finance department has a segment with both extremely sensitive applications and others that aren't)

Using all 4 levels of depth (including root) is not recommended unless absolutely required

Source: Azure Security Compass v1.0

Creation of resource groups

Critical best practices

USE OF RESOURCE GROUP (RG)

- **What** – All the resources in your group should share the same lifecycle and delegation need
- **Why** – It's easier to deploy, update, and delete resources together. If one resource, such as a database server, needs to exist on a different deployment cycle or be administrated by a different team, it should be in another resource group
- **How –** Create or move your resources sharing the same lifecycle/delegation in the same resource group

Naming standards

Well-designed naming conventions enable you to identify resources in the Administration portal, in logs, within scripts, and allow easier breakout of data in dashboards and billing

When adding Azure to your environment, you should extend those naming standards to your Azure resources

Consistent naming conventions make resources easier to locate

They can also indicate the role of a resource in a solution

Resource tags are tightly aligned with naming standards

As resources are added to subscriptions, it becomes increasingly important to logically categorize them for billing, management, and operational purposes

SHAKESPEARE SAID: "WHAT'S IN A NAME?"

Some points of views:

1. **Finance/Business –** While they don't necessarily care what something is NAMED, what they do care about is that they can group the data and understand the context whether it be for billing or just understanding what resources are where
2. **Security** - Like Finance/Business they don't necessarily care what something is named, but they do care about grouping of like resources for the purposes of identifying and applying security controls that are appropriate
3. **Technology Pros –** They are more concerned about identifying what a resource is quickly, filtering and grouping within the portal and in reports and ensuring that scripting and other repetitive tasks are simplified. Naming standards have long been a way to accomplish that

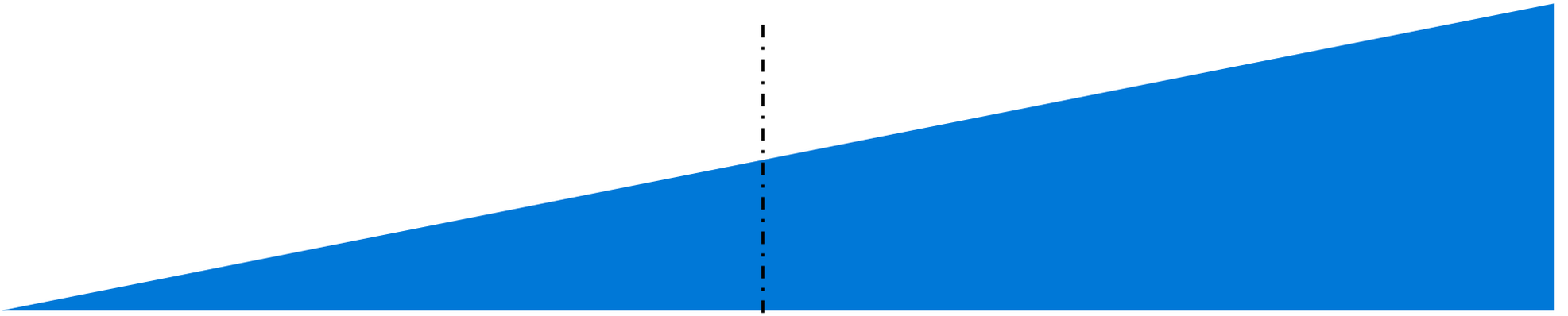
Naming and tagging design considerations

IT aligned naming and tagging

Primary design considerations:

Baseline operations requirements supplemented by additive business requirements

Business aligned naming and tagging



Baseline naming standards

- Resource naming is required for any deployment
- A standardized naming schema is the minimum "Tag"

Functional

- Add tags that describe the function of the resource/asset (VM, container, etc.) for easy identification
- Example: Workload, Function in the workload (app, data, etc.), Environment (Dev, Staging, Prod, etc.)

Classification

- Tags that classify the value of an asset can aid in decision making
- Example: Data classification (Public, General, Confidential, Highly Confidential, etc.)

Accounting

- Track costs associated with asset operations
- Example: Department, Project, Region, etc.

Partnership

- Align partner ship that count on this asset of IT
- Example: owner, Owner Alias, Stakeholder, Power User, Executive

Purpose

- Aligning an asset to a business function can be valuable in making investments decisions
- Example: Business Process, Business criticality, Revenue Impact

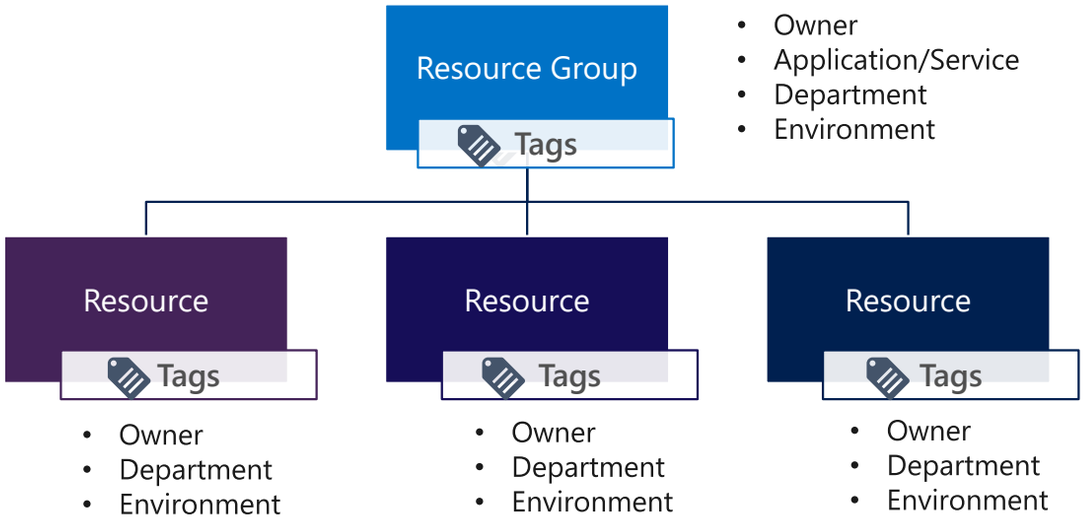
https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/decision-guides/resource-tagging/

Tags
Critical guidances

BEST PRACTICE CHOICE

ENFORCE TAGGING RULES

- **What –** Attach metadata to resources and resource groups through tags
- **Why –** To assure compliance, for charge-back purpose and for administrative purpose identification
- **How –** Use built-in Azure Policy like:
  - Apply tag and its default value
  - Billing Tags Policy Initiative
  - Enforce tag and its value



Use tags to organize your Azure resources

Resource organization tips

Setup a naming convention and enforce it

Use tag generously but ensure consistency

Don’t create too many Management group nested levels unless required

Group resources with the same lifecycle and boundary

Enforcing compliance with

Azure Policy and initiatives

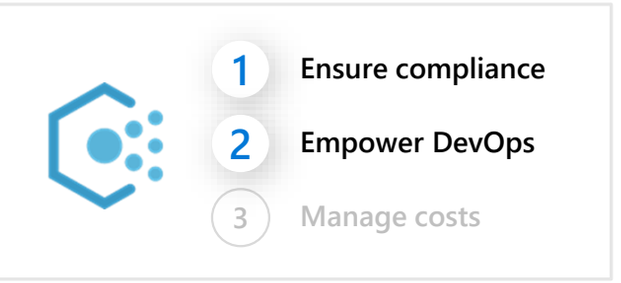
Azure Policy and initiatives are intended to manage risks by enforcing rules (with effects) over the resources and services in your subscriptions

They allow **real-time enforcement,** compliance assessment, and remediation at scale. And it's free!

Translate Risk into Policies

Azure Policy

Active control and governance at scale for your Azure resources



Enforcement & compliance

Turn on built-in policies or build custom ones for all resource types

Real-time policy evaluation and enforcement

Periodic & on-demand compliance evaluation

VM In-Guest Policy (NEW)

Apply policies at scale

Apply policies to a Management Group with control across your entire organization

Apply multiple policies and & aggregate policy states with policy initiatives

Exclusion Scope

Remediate & automate

Remediate existing resources at scale (NEW)

Automatic remediation resources at deployment time

Trigger alerts when a resource is out of compliance

Azure Policy language

Logical operators

"not": {condition or operator}
"allOf": [{condition or operator},
{condition or operator}]
"anyOf": [{condition or operator},
{condition or operator}]

Conditions

"equals": "value"
"like": "value"
"match": "value"
"contains": "value"
"in": ["value1","value2"]
"containsKey": "keyName"
"exists": "bool"

Fields

name
kind
type
location
tags
tags.*
property aliases

Effects

Deny,
Audit,
Append,
AuditIfNotExists,
DeployIfNotExists

Policy lifecycle

What drives your need for Policy?

- Regulatory Compliance
- Controlling cost
- Maintain security and performance consistency
- Enforce enterprise wide design principles

Who owns policy definitions & implementation?

- “Initiative" owners like Security Architect or Cloud Architect or Cloud Engineers

What is involved in defining a new Policy or refining an existing one?

- Research or gather evidence on the impact of a particular configuration on a particular fundamental (like cost or security)
- What-if analysis of enforcing configuration in a particular manner
- Assess the current state of compliance to understand the impact of new policy and what exceptions are needed
- Roll out new policy in phases
- Understand the applications & teams who are non-compliant

What are the capabilities needed for this workflow?

- Checking on existing configurations for new policies
- Compliance Reporting
- Intuitive authoring experience
- Ability to control more resource configurations in policy
- Ability to test policy on-demand to understand impact
- Ability to remediate non-compliant configurations
- Exception Handling

Azure Policy

Critical best practice and general guidance

ADOPT AZURE POLICY

- **What –** Use Azure policy to monitor and enforce your organization's security policy
- **Why –** Ensure compliance with your security strategy and/or regulatory security requirements across your Azure workloads
- **How –** Follow the instructions in the Azure Policy documentation to plan and create policies

  https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

USE AUDIT MODE

- **What –** Start policy deployments in Audit mode and then later progress to Deny or Remediate
- **Why –** Business operations can be negatively impacted by Deny effect or Remediate effect so start with Audit effect to limit risk of negative impact from policy
- **How –** Test and review the results of the Audit effect

MONITOR POLICY ASSIGNEMENT

- **What –** Ensure that an alert exists for the scope of the entire subscription when a new policy is assigned
- **Why –** Monitoring for create policy assignment events gives insight into changes done in "azure policy - assignments" and may reduce the time it takes to detect unsolicited changes
- **How –** Create a new alert rule in Azure monitor that will apply to the subscription

Tip *Start considering the Azure Policy samples repo on GitHub:* https://github.com/Azure/azure-policy

Common guardrails

Leverage built-in initiatives & policies

Security

Azure Security Center

Guest Config baselines

Key Vault certificate

NSG rules

AKS & AKS Engine

RBAC role assignment

Regulatory Compliance

NIST SP 800-53 R4

ISO 27001:2013

CIS

PCI v3.2.1:2018

FedRAMP Moderate

Canada Federal PBMM

SWIFT CSP-CSCF v2020

UK Official and UK NHS

IRS 1075

Tags

Require specified tag

Add or replace a tag

Inherit a tag from the RG

Append a tag

Resource standardization

Allowed/ not allowed RP

Allowed locations

Naming convention

Back up VMs

Allowed images for AKS

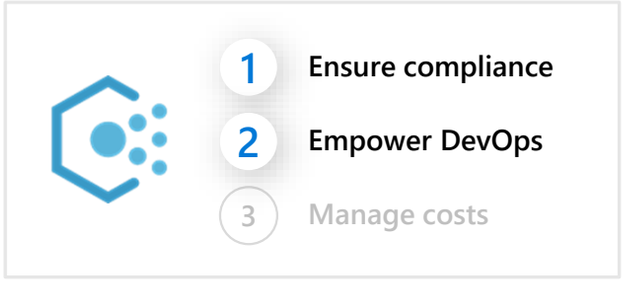
Cost

Allowed VM SKUs

Allowed Storage SKUs

Enforce policies as part of the development process

Shift left to deliver compliant code faster



Code | Build/Test | Deploy | Operate

Policy as Code

Pre-flight

Validation

Authoring

Policy

Security

Monitoring

Azure DevOps

Enforce policies as part of the development process

Shift left to deliver compliant code faster

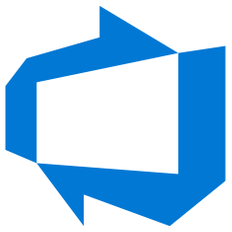
1. Ensure compliance
2. Empower DevOps
3. Manage costs

Code | Build/Test | Policy as Code: Pre-flight / Validation / Authoring | Deploy | Operate

Policy

Security

Monitoring



Azure DevOps

Azure Policy

Azure Blueprints

Enabling quick, repeatable creation of fully governed environments

1. Ensure compliance
2. Empower DevOps
3. Manage costs

Streamline environment creation

Centralize environment creation through templates

Add resources, policies and role access controls

Track blueprint updates through versioning

Enable compliant development

Empower developers to create fully governed environments through self-service

Create multiple dev-ready environments and subscriptions from a centralize location

Leverage the integration with Azure Policy on the DevOps lifecycle

Lock foundational resources

Ensure foundational resources cannot be changed by subscription owners

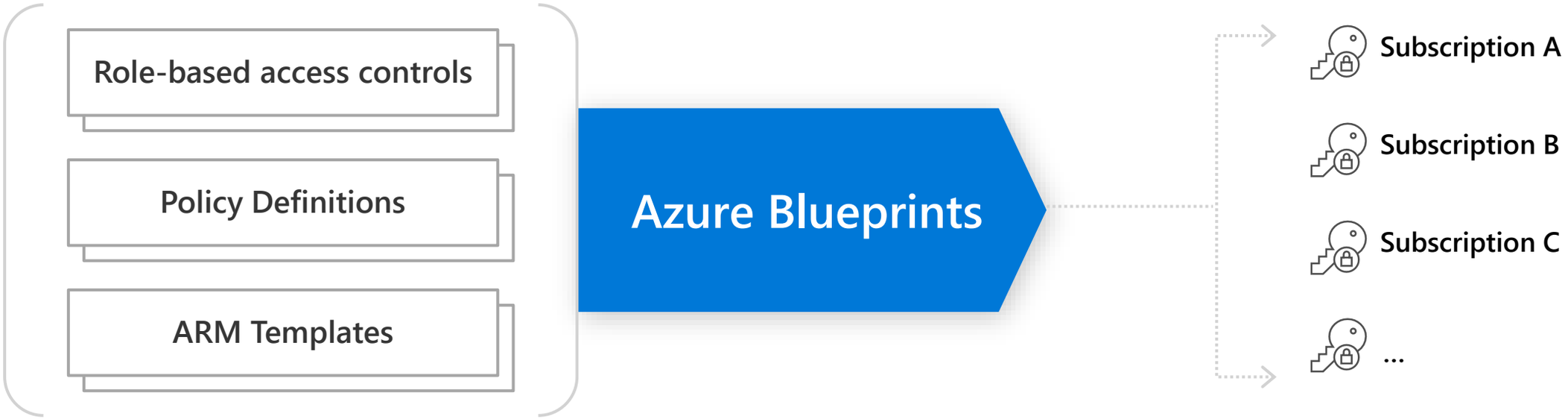
Manage locks through a centralize location

Update locked resource through blueprint definition updates

Azure Blueprints

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

1. Ensure compliance
2. Empower DevOps
3. Manage costs



Compose | Manage | Scale

Cost Management

1 Ensure compliance

2 Empower DevOps

3 Manage costs

Azure Resource Graph

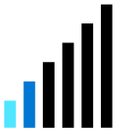
Resource Graph allows asset exploration and visibility powered by advanced Kusto Query Language KQL across all subscriptions and management groups

Explore your resources

Get visibility into your Azure resources across subscriptions and management groups.

Access the information you need in the portal, CLI or PowerShell

Find assets based on resource properties or their relationships



Query & analyze

Get the exact information you need through queries in seconds

Perform analysis at scale across all your environments

Leverage Keyword Query Language for easy query creation

Assess impact

Understand the impact of applying policies before their implementation

Get a view of the operational impact of common actions like deprecations

Cost management

One of the major changes that you will face when you move from on-premises cloud to the public cloud is the switch from capital expenditure (buying hardware) to operating expenditure (paying for service as you use it)

This switch from CAPEX to OPEX also brings the need to more carefully manage your costs

The benefit of the cloud is that you can fundamentally and positively impact the cost of a service you use by merely turning it off (or resizing) when it's not needed

Deliberately managing your costs in the cloud is a recommended practice and one that mature customers do daily

This discipline focuses on ways of establishing cloud spending plans, allocating cloud budgets, monitoring and enforcement of cloud budgets, detecting costly anomalies, and adjusting the cloud governance plan when actual spending is misaligned

The consistent use of patterns discussed throughout the decision guides can help establish a baseline level of policy compliance

Governance discipline template

https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/cost-management/

Continuous cost optimization process

Extend visibility to stakeholders

Management groups, RBAC, and tagging

Management teams

Set clear goals

Budgets and alerts

Finance teams

Hold teams accountable for improvement

App teams

Billing

You can use tags to group your billing data

For example, if you are running multiple VMs for different organizations, use the tags to group usage by cost center and categorize costs by runtime environment (production, staging, etc.)

Tips

Tags should be enforced by configuration policies. Use Azure Policy to set and track ARM tagging policies

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags#templates

You can retrieve information about tags through

- The Azure Resource Usage and RateCard APIs

-or-

- The usage comma-separated values (CSV) file. (You download the usage file from the Azure Enterprise portal)

Azure Cost Management

1 Ensure compliance

2 Empower DevOps

3 Manage costs

Monitor cloud spend

Track usage and cost trends

Detect spending anomalies and usage inefficiencies

Forecast future spend using your historical data

Visualize data in consolidated or custom dashboards

Drive organizational accountability

Allocate usage and costs to business units and projects

Produce chargeback and show back reports

Let teams access data and insights with Role-Based Access Control

Automatically alert stakeholders of spending anomalies and overspending risks

Optimize cloud efficiency

Increase resource utilization with virtual machine right-sizing

Eliminate idle resources

Improve virtual machine reserved instances management

Pay less for Windows Server and SQL Server resources through Azure Hybrid Benefit

Identity

Identity baseline

One of the first, and most crucial, questions you ask yourself when starting with the public cloud is "who should have access to resources?" and "how do I control this access?"

Allowing or disallowing access to the Azure portal and controlling access to resources in the portal, by scripts or through code is critical to the long-term success and safety of your assets in the cloud

This discipline focuses on ways of establishing policies that ensure consistency and continuity of user identities (guest vs. employee) and ensure appropriate (dynamic) entitlements & access, and reviews

The consistent use of patterns discussed throughout the decision guides can help establish a baseline level of policy compliance

See also administration and identity sections of the Azure Security Compass for best practices and guidance

Governance discipline template

https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/identity-baseline

Toolchain for identity baseline

Azure Administration portal

AD (on-premises, IaaS)

Azure AD

- Azure AD Connect for hybrid identities, Azure AD B2B capabilities, Azure AD Domain Services

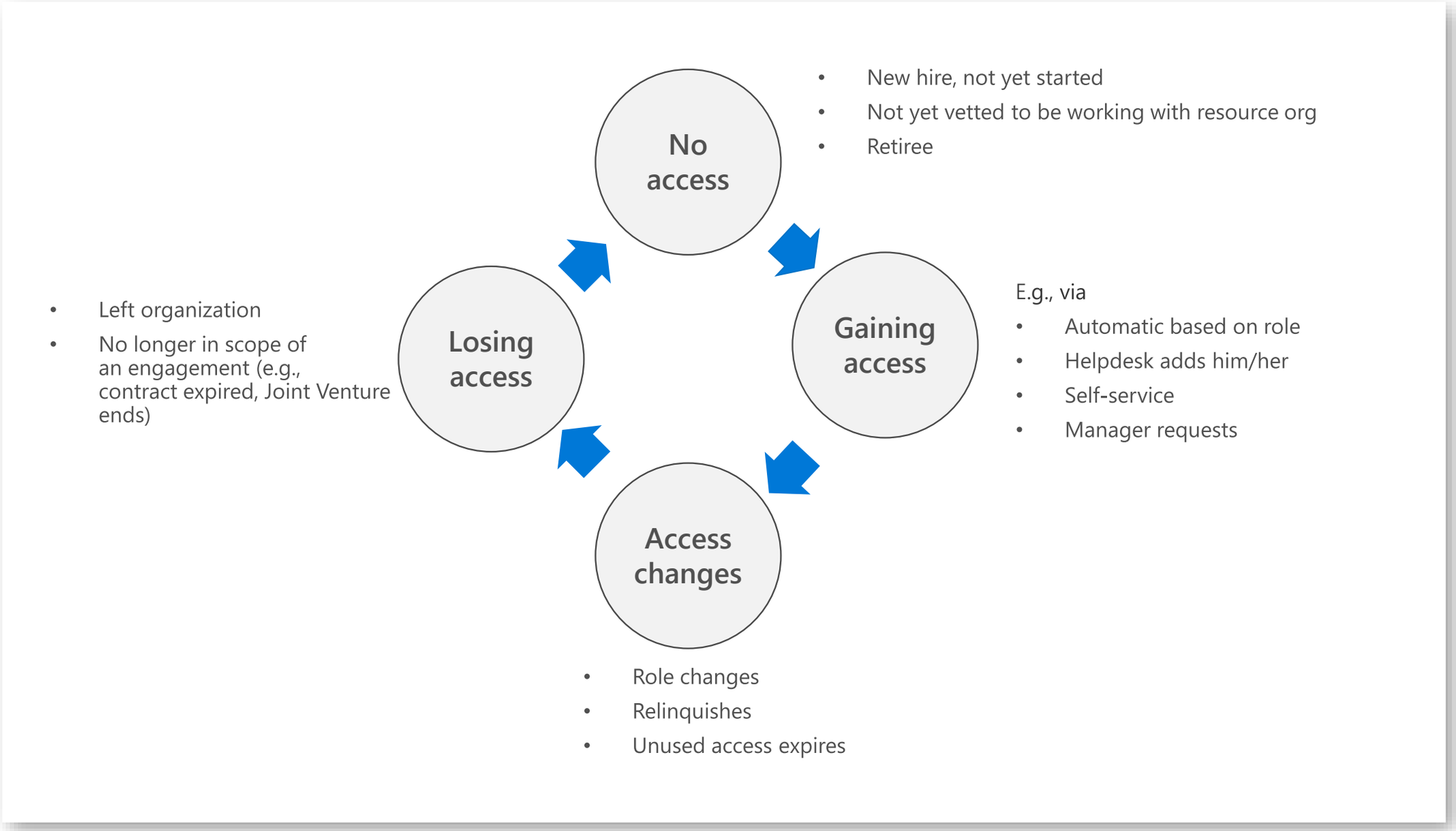
Azure AD (newly introduced) governance capabilities

IMPROVE THE IDENTITY BASELINE

Some related activities:

- Evaluate the toolchain options and implement your toolchain by first rolling out in a pre-deployment phase, and then migrate from
- Develop a (draft) Architecture Guideline document. First review for that purpose the use of patterns discussed throughout the architectural decision guides.
- Customize the toolchain based on changes in your organization's requirements and needs. Update the Architecture Guideline document accordingly

Identity and access lifecycle



Here's the story of how a guy making $66,000 a year lost $7.2 billion for one of Europe's biggest banks

Kim Iskyan, Stansberry Churchouse Research May 8, 2016, 7:02 PM

It's not a normal – or lo
trading practice to amas
securities position that'
five times the total econ
output of Cambodia... o
times the market capita
of the major global bank
working for. It's even les
normal if the bank you'
working for has no clue about
what you're doing.

By manipulating the bank's software, he was making risky one-sided bets when his firm thought he was making lower-risk arbitrage trades. Kerviel reportedly made nearly US$2 billion in profits in 2007 by making these kinds of unauthorized trades.

exclusive photo session. Reuters/Philippe Wojazer

Jerome Kerviel was a junior level derivatives trader earning US$66,000 per year at Societe Generale, one of Europe's largest banks. By January 9, 2008, he had amassed a stock index futures position of US$73 billion. The way he did so ended up costing

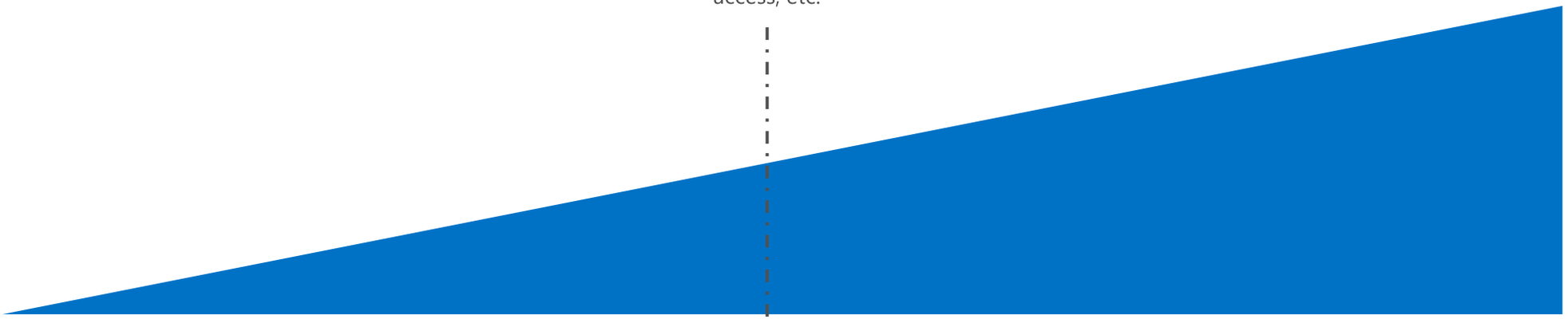
Identity design considerations

Limited identity complexity

Primary design considerations:

Legacy authentication support, complex directory environment/organizational unit structures, employees vs. external users' access, etc.

Highly complex identity



Cloud baseline

- Standalone authentication not integrated with (on-premises) directory

Directory synchronization

- Authentication against a cloud identity service that is synchronized with other (on-premises) identity services
- Commonly performed as part of an Office 365 adoption

Cloud hosted domain services

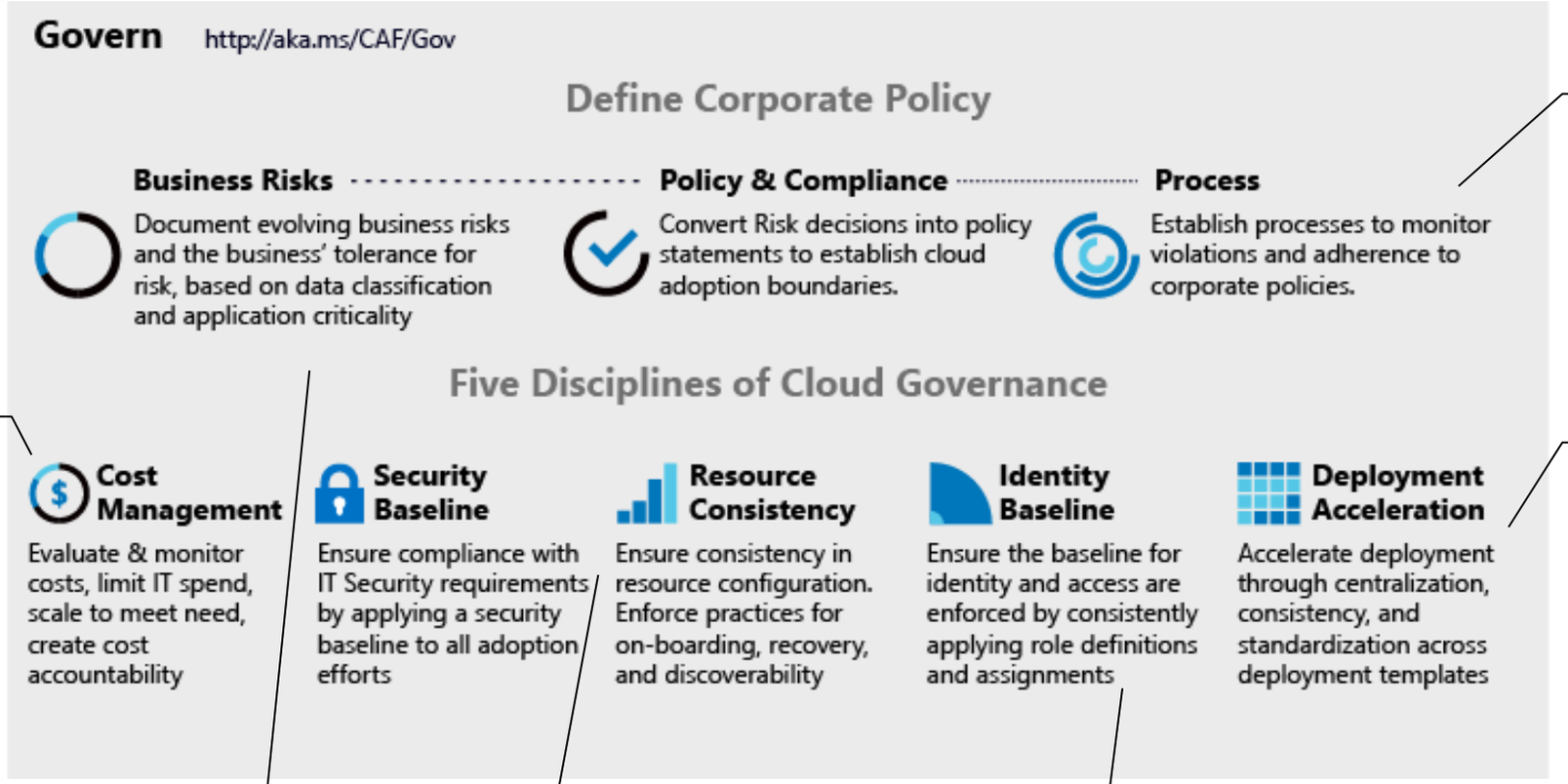
- Identity services running on VMs/appliances to supports Kerberos or other claims-based authentication methods
- Likely also using directory synchronization for shared identity with on-premises

Identity federation with other (social) identity services

- Single sign-on capabilities
- Federation across multiple identity providers

https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/decision-guides/identity/

Making Governance Actionable with Native Tools



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

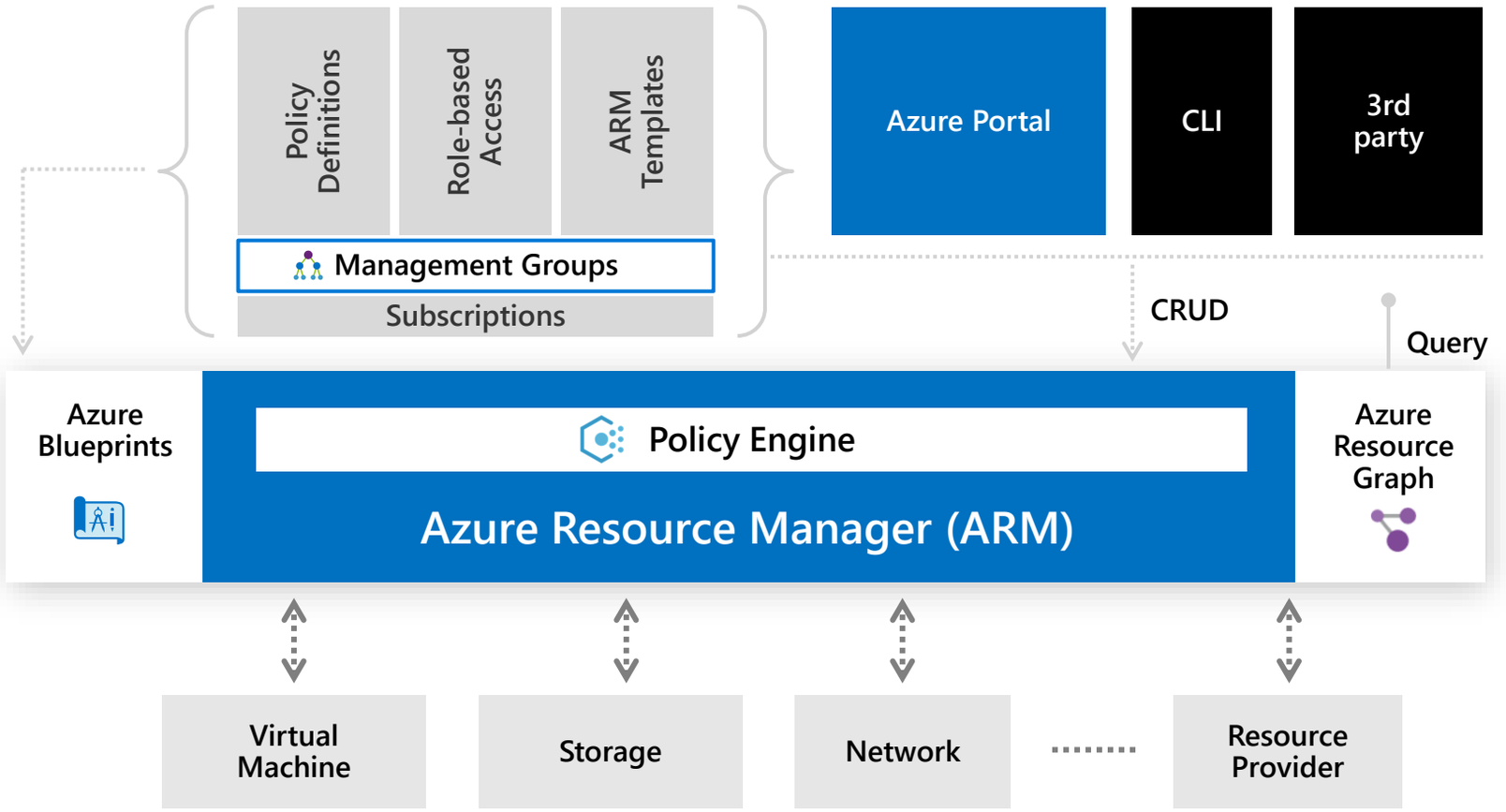
Azure Governance Architecture

Providing control over the cloud environment, without sacrificing developer agility

1. **Environment factory**
   Deploy and update cloud environments in a repeatable manner using composable artifacts

2. **Policy-based control**
   Real-time enforcement, compliance assessment and remediation at scale

3. **Resource visibility**
   Query, explore & analyze cloud resources at scale



Q&A

Reach out to the team

sap-on-azure-pe-apac@microsoft.com

Feedback

Your feedback is very important for us.

Your responses are Anonymous

https://aka.ms/SAPAPAC-POE-FEEDBACK

Microsoft

SAP on Azure Enablement

Next Session – SAP and DevOps

Wednesday, Oct 21th, 2020, 10am SGT

Reach out to the team
sap-on-azure-pe-apac@microsoft.com