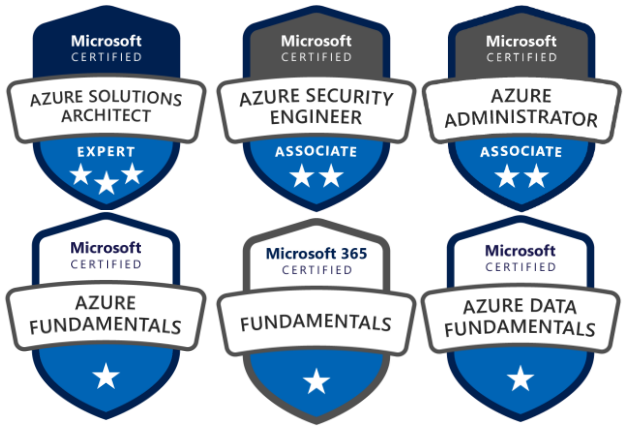
TechDay پاکستان

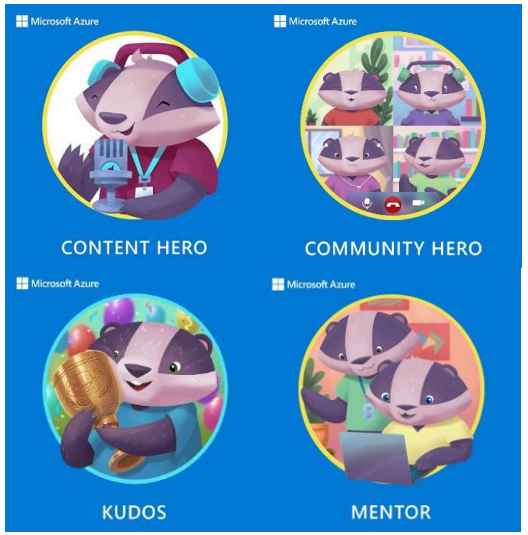
Cloud Adoption Framework Governance Overview

Abdul Kazi

March 2023

TechDay پاکستان





Abdul Kazi

Blogger | Mentor | Speaker

www.abdulwkazi.com

abdulkazi

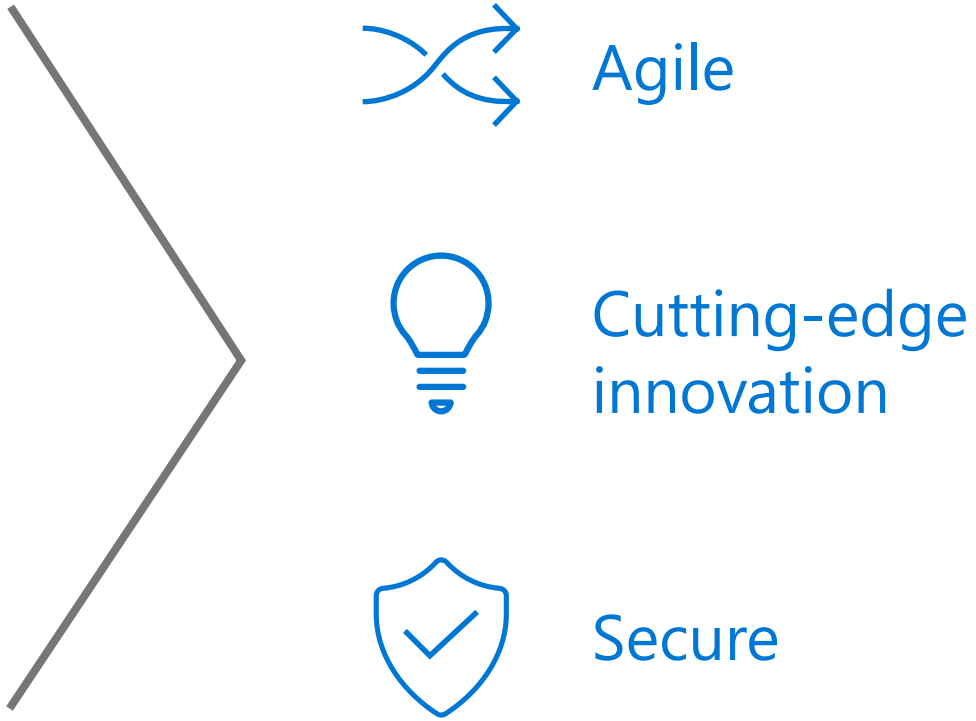
abdulwkazi

ComeCloudWithUs

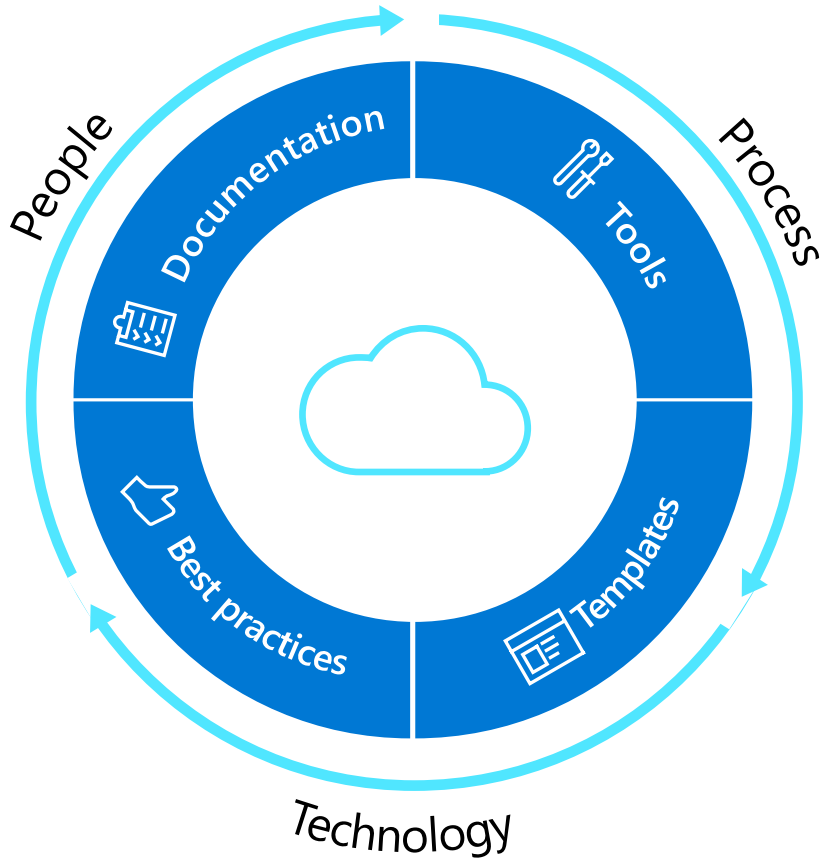
TechDay
پاکستان

The value of creating cloud-ready environments

- Aligned to business priorities
- Cloud-design considerations
- Adapted for cloud operating model
- Ready for cloud applications
- Adaptable to grow and expand
- Compliant

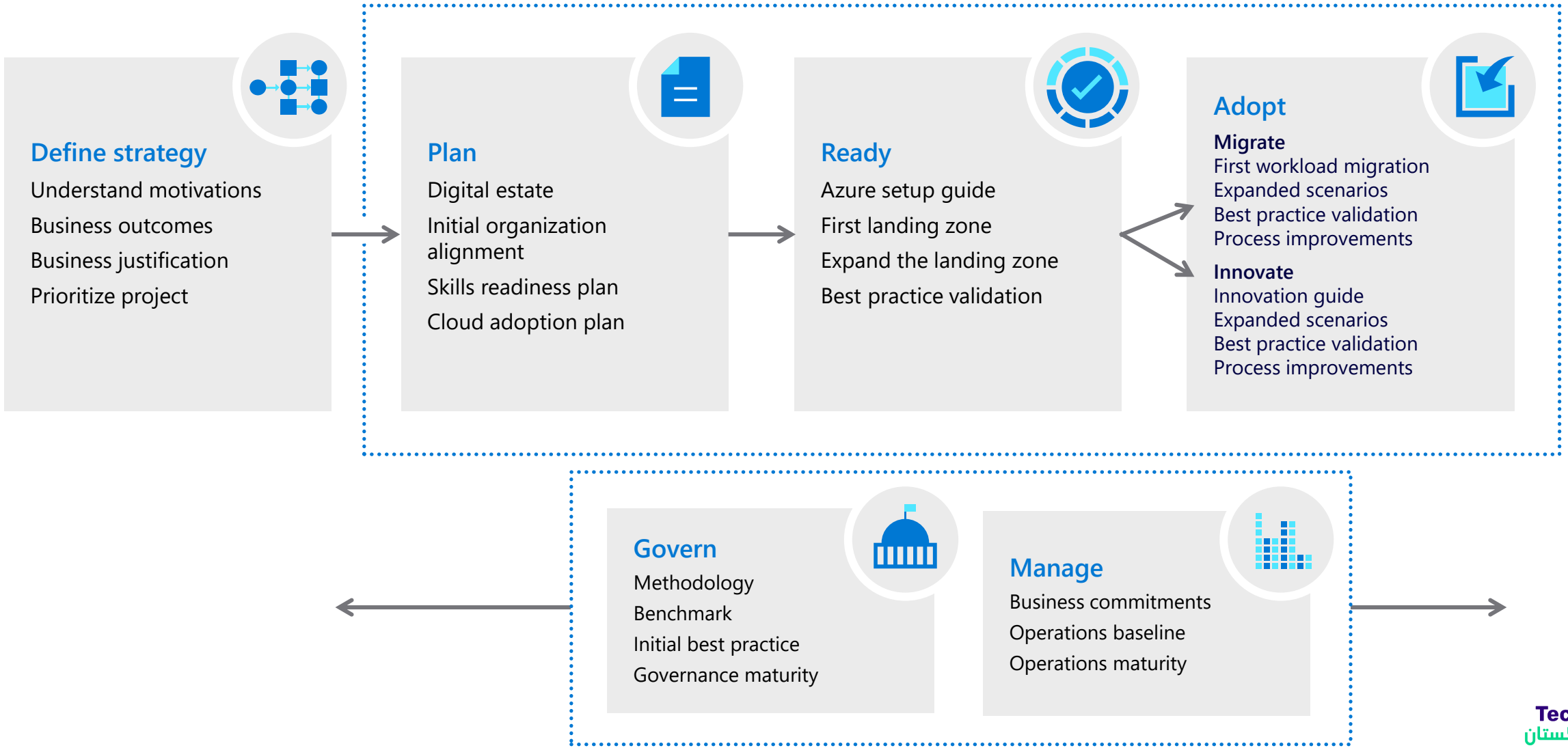


Microsoft Cloud Adoption Framework for Azure



Align **business, people and technology strategy** to achieve business goals with **actionable, efficient, and comprehensive** guidance to deliver fast results with control and stability.

Microsoft Cloud Adoption Framework for Azure



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

Modernization

Improving customer and employee experiences

Transformation

Evolving how businesses operate and interact with the market

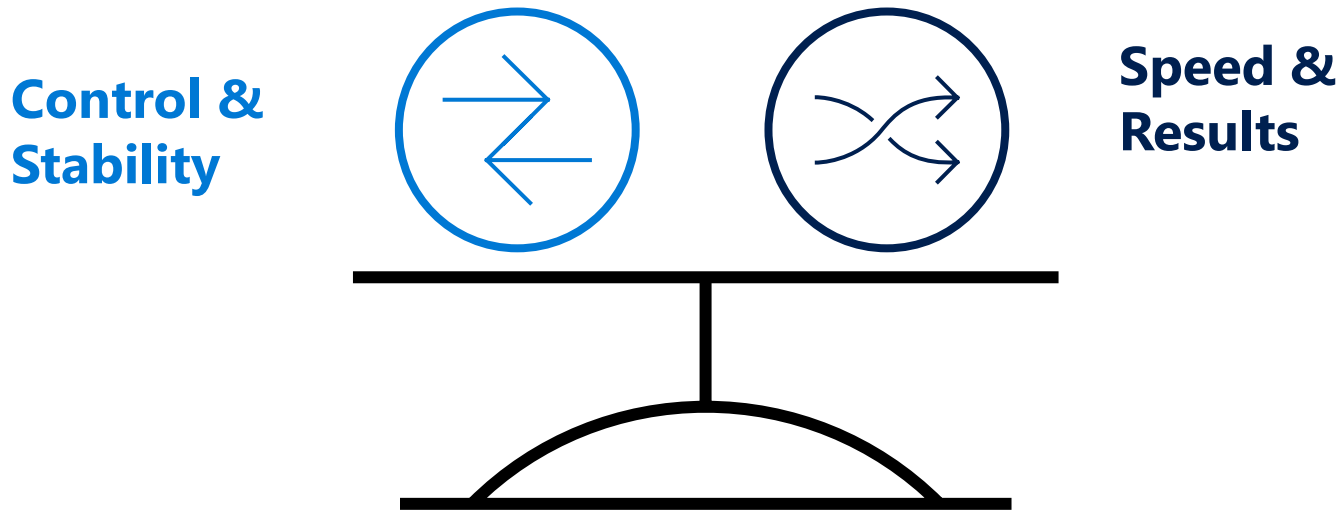
Growth

Scaling products and services to meet ever growing business needs

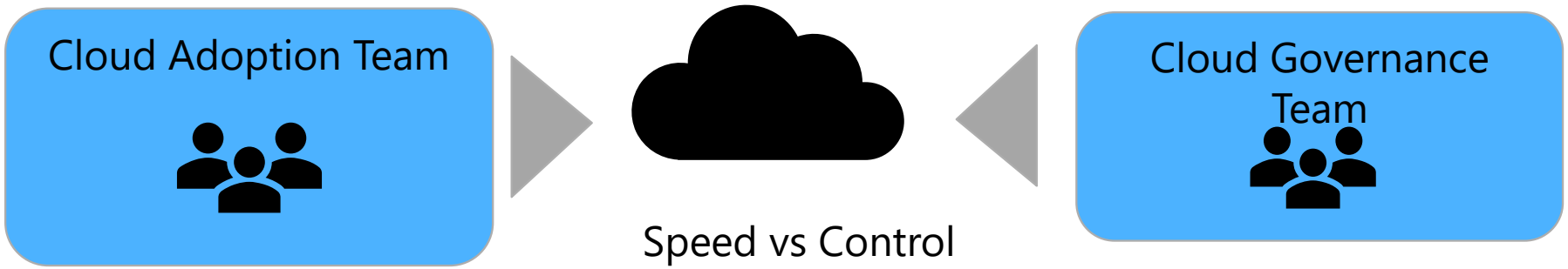
Business Returns

IT must rapidly produce measurable business returns to stay relevant

Objective of this model: Create balance



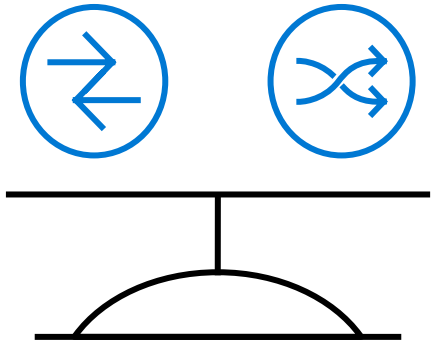
Organization Alignment



- Create a balance between speed or *moving quickly* and control or *reducing risks* by have teams accountable for adoption and governance.
- While cloud adoption team is required to execute cloud adoption tasks, governance team ensures processes and controls are implemented

Why is Governance Important?

Transformation



Risk mitigation

- Maintaining full compliance
- Creating better cost visibility and control
- Improving security posture
- Being agile—to support scale

Who is responsible for monitoring and supporting cloud operations?

Which services should be migrated to Azure?

What roles & responsibilities must be defined?

What security measures should be considered?

What are the core processes needed for service management?

How do we ensure balance between innovation, cost and agility?

What organizational changes are needed?

What key capabilities must we develop?

Assessment - **Cloud Adoption Framework Governance Benchmark Tool**

https://cafbaseline.com/

CAF Governance Model

Envision an end state – and incrementally build trust and confidence.

Govern

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.

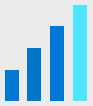
Five disciplines of cloud governance

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

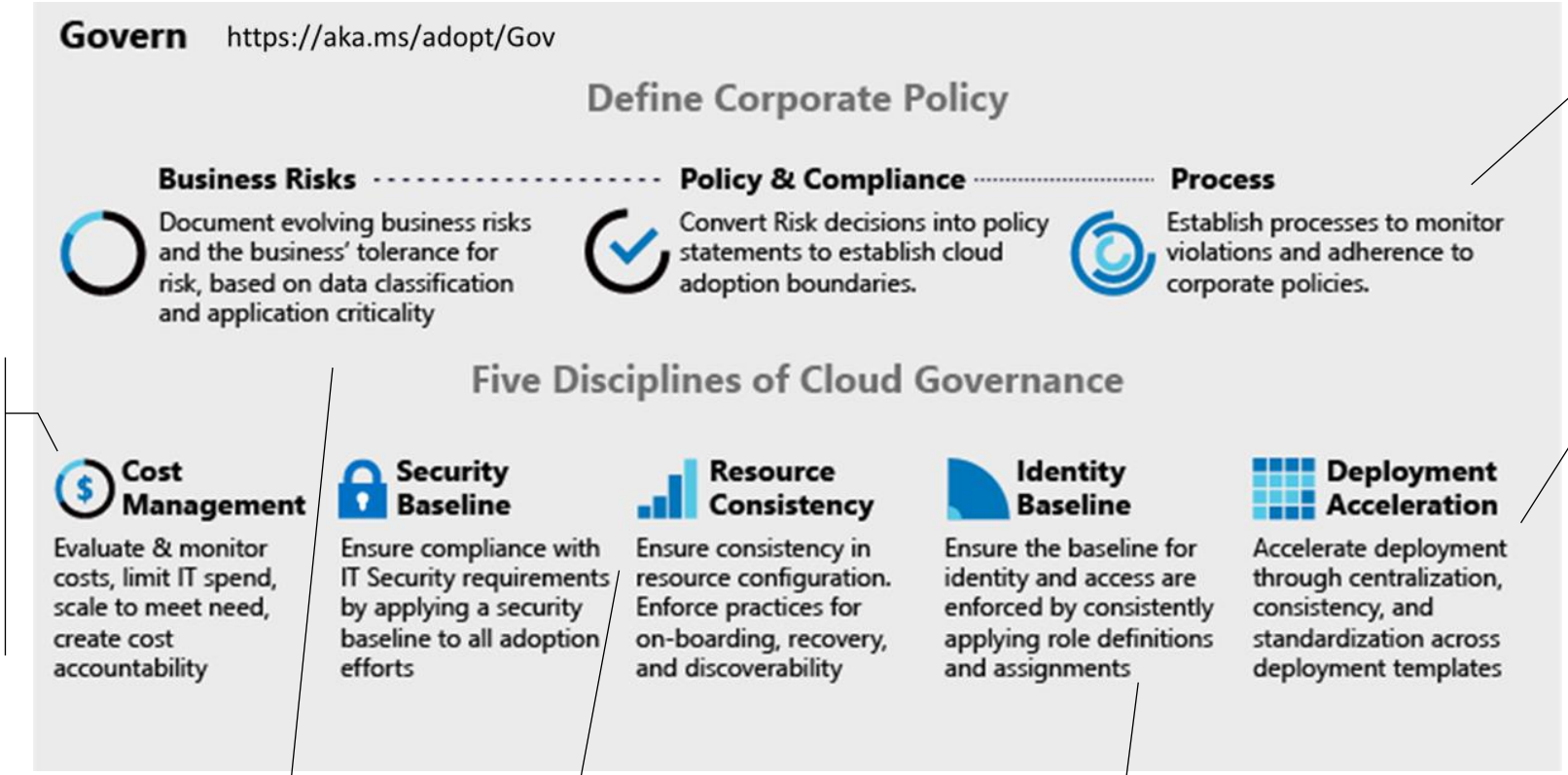
Deployment acceleration

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

Governance funnels corporate policy changes into five actionable disciplines – **enabling your organization to modernize and reach business goals.**

https://aka.ms/adopt/Gov

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

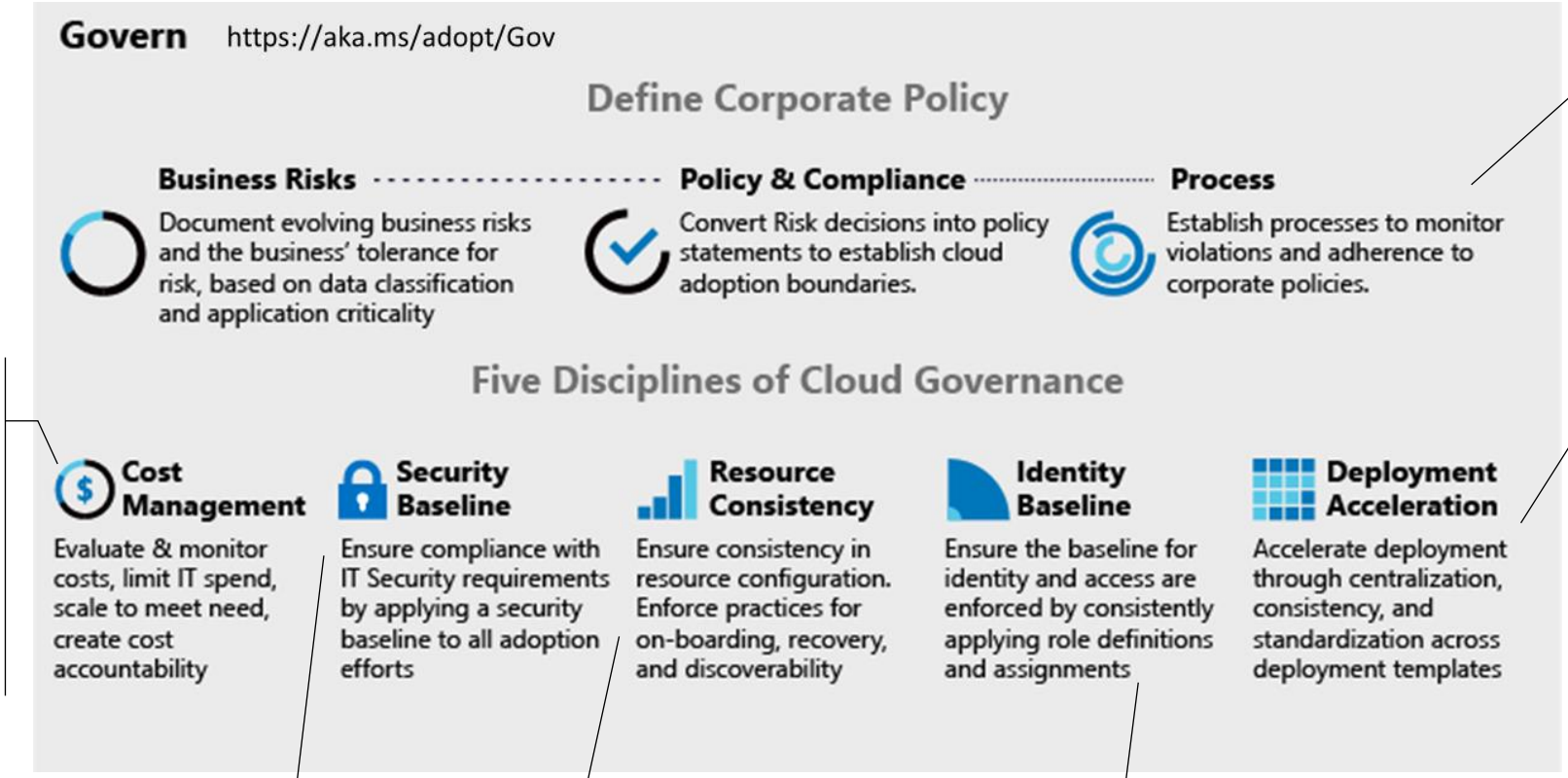
- **Azure Blueprints**
- **Azure Policy**
- ***Azure Security Center***
- ***Azure Sentinel***
- Subscription Design
- Encryption
- Hybrid Identity
- Azure Networking
- Azure Automation

- **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

TechDay پاکستان

Integrating 3rd Party Tools



Monitoring 3rd parties
- OpsCompass
- Splunk
- AppDynamics
- Solarwinds
- New Relic
- Data Dog

Cost Management 3rd parties
- HashiCorp Terraform (ROI tools)
- Cloudcheckr

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

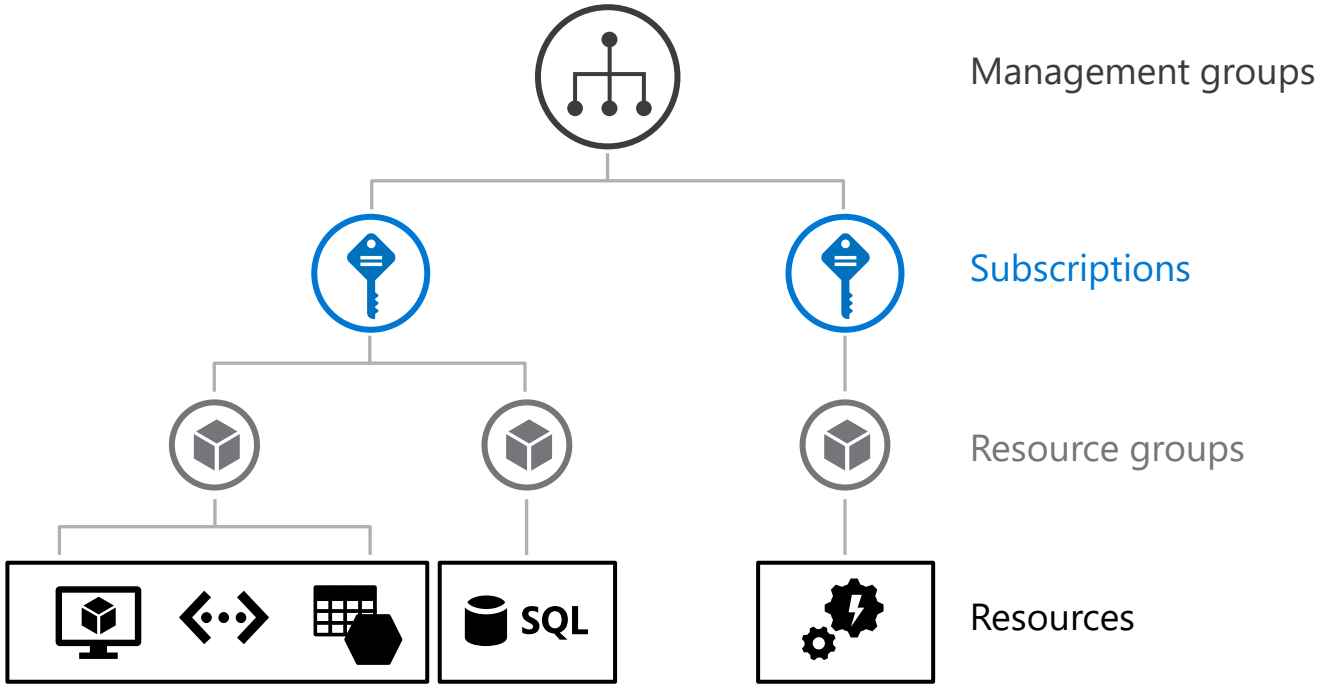
3rd party identity providers
- HashiCorp Vault
- RSA
- Omada
- Ping Identity
- SailPoint

Understand Business Risks

1) What are your compliance requirements?
2) Have you identified your business risks as it relates to cloud?
3) What are your business priorities and reasons for moving to cloud?
4) How do you think about data risks and data governance?
5) Is there a list of applications which are prioritized by business impact?
6) Do you have specific application governance requirements?
7) How do you audit for compliance?

How to organize your Azure Resources

- Use the management hierarchies within the Azure platform
- Implement well-thought-out naming conventions
- Apply resource tagging



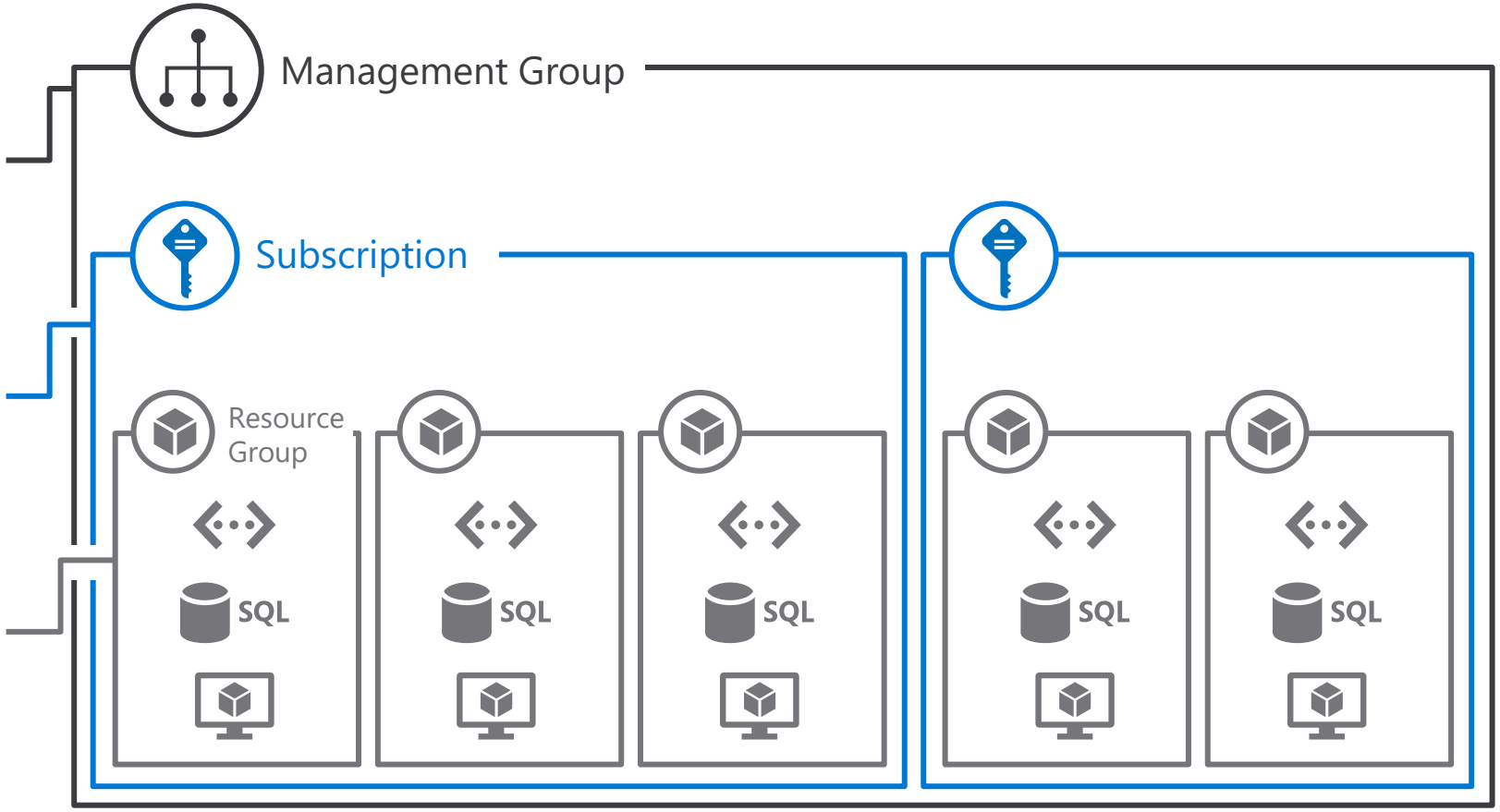
What is Resource Consistency?

The basic foundation of all governance practices.
Achieving the right Governance starts with the correct resource organization.

Management Groups
To reflect security, operations and business/accounting hierarchies.

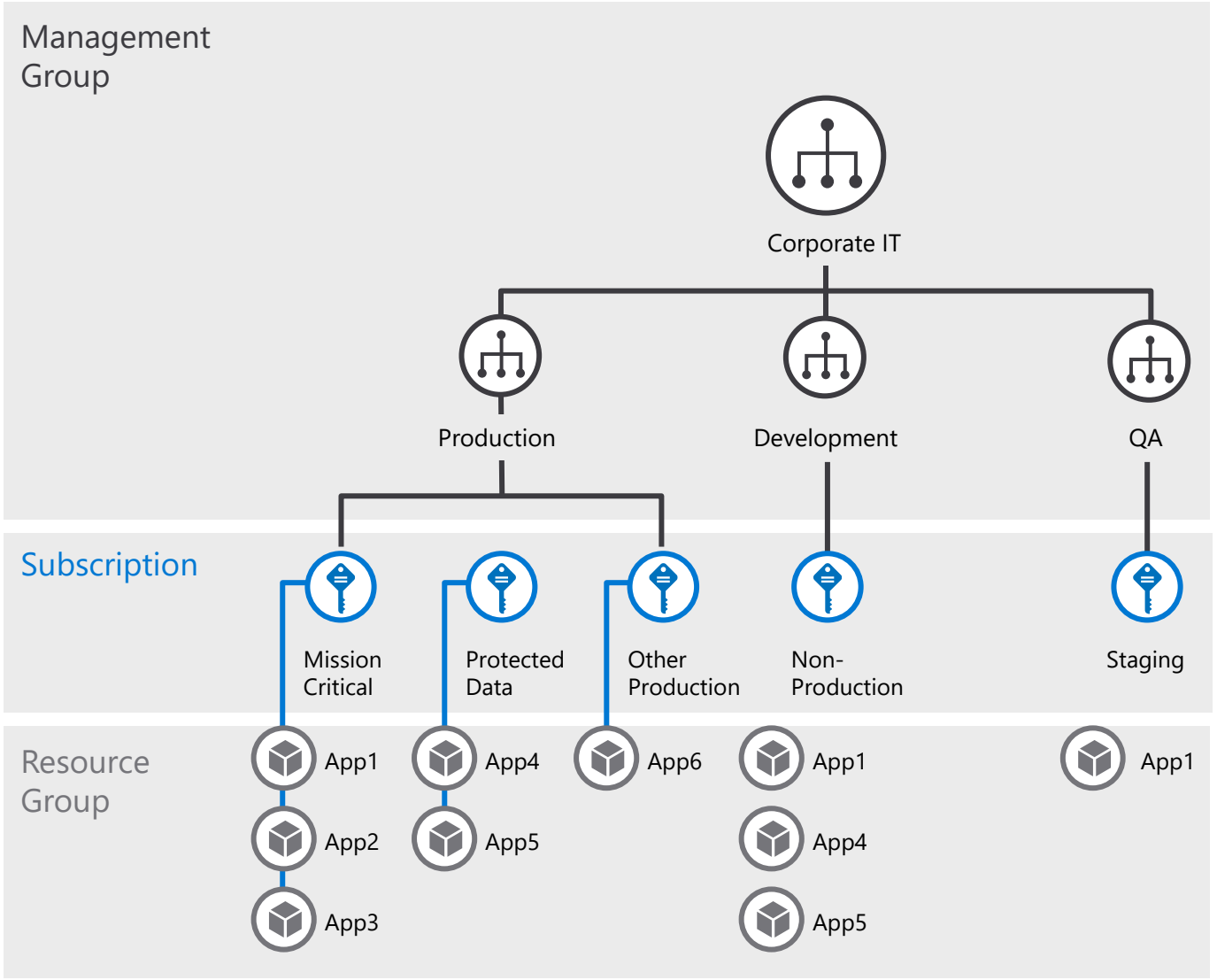
Subscriptions
To group similar resources into logical collections.

Resource Groups
To further group applications or workloads into deployment and operations units.



Management Group best practices

- Define your hierarchy based on organization and environment type (prod, pre-prod, etc.)
- The root MG is for global configuration
  - Be careful with MG level assignments as they will cascade through large chunks of your hierarchy
- Try not to repeat yourself. Assign common policies and RBAC higher up in your hierarchy
- Built-in RBAC roles for MGs (MG contributor, MG reader)
  - Need subscription owner access to move to another MG



Governance MVP Considerations

Resource Organization

Build only what you need, add as the requirements are needed.

Management Group Hierarchy

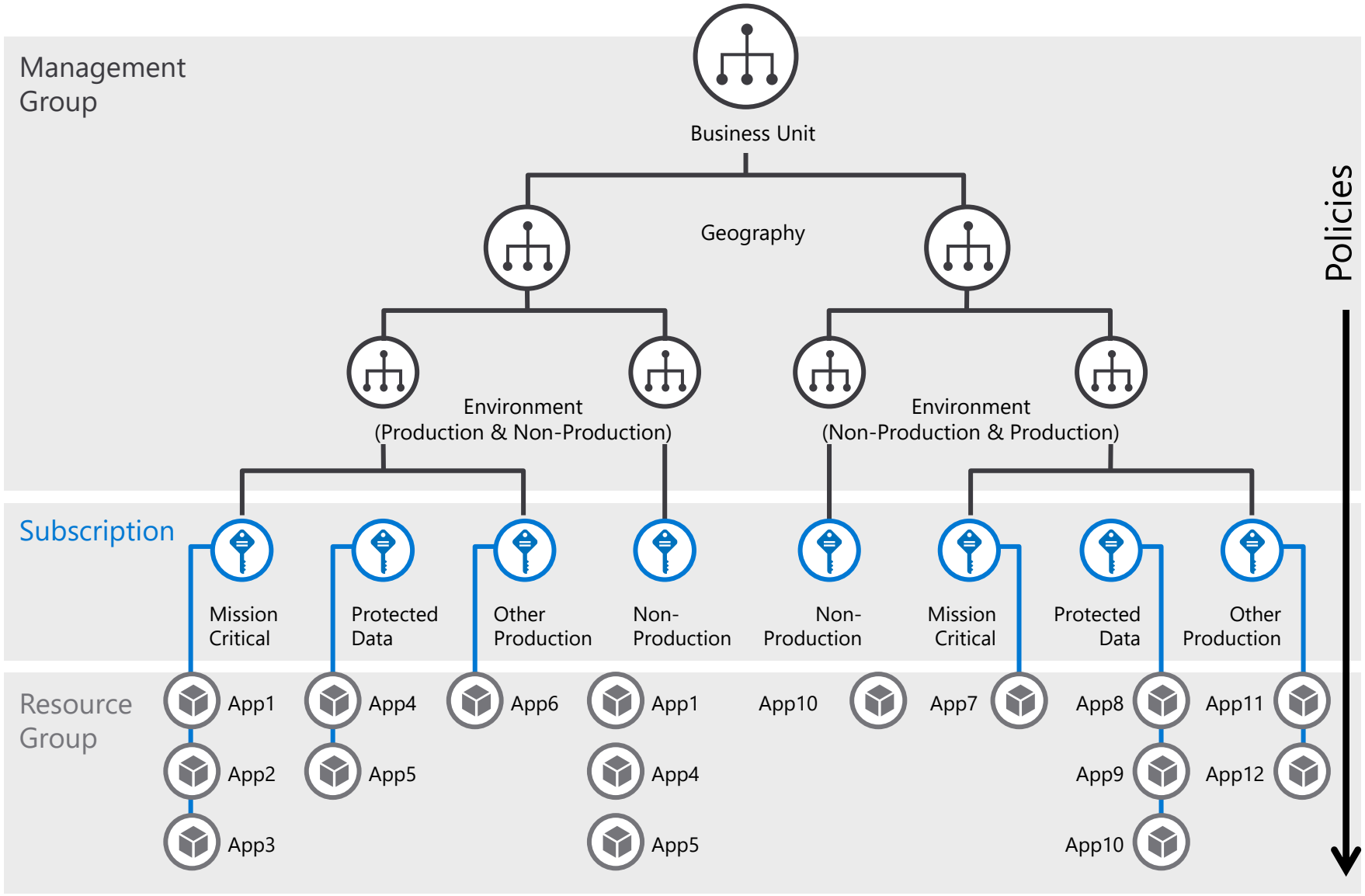
- Business Unit
- Geography
- Environment

Subscription

- Per Application Category
- Pre-production
- Dev environments
- Production

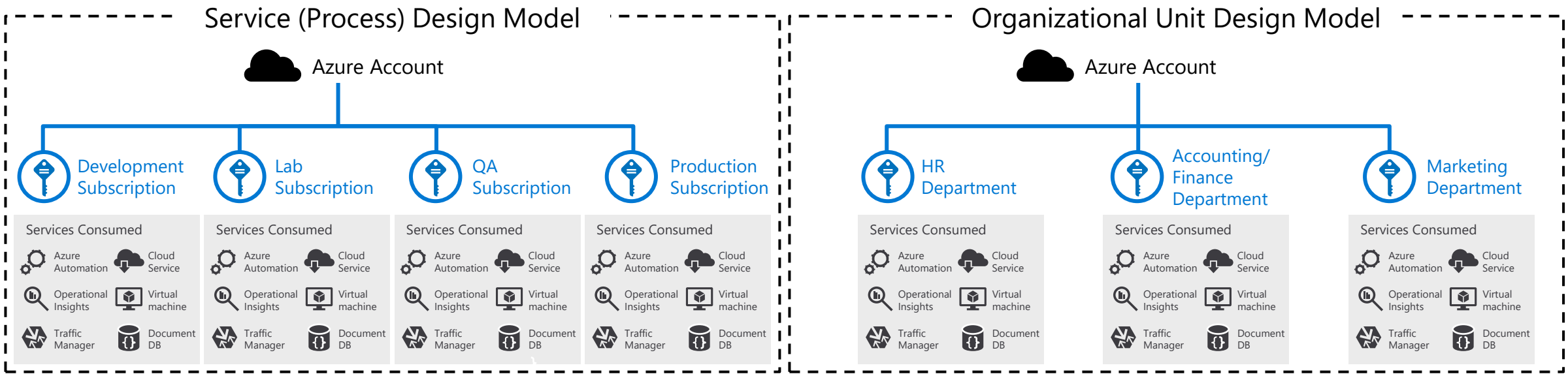
Resource Groups

- Per Application



Subscription | Design considerations

Develop the Subscription, Network, Storage, Availability and Administrative models together in order to have a cohesive approach.



Items to look at when designing the subscription model:

Business Requirements

- Accountability
- Audit/Compliance
- Performance
- Availability & Recoverability

Technical Requirements

- Network Connectivity (shared or dedicated)
- Active directory requirements, clustering, identity, management tools

Security Requirements

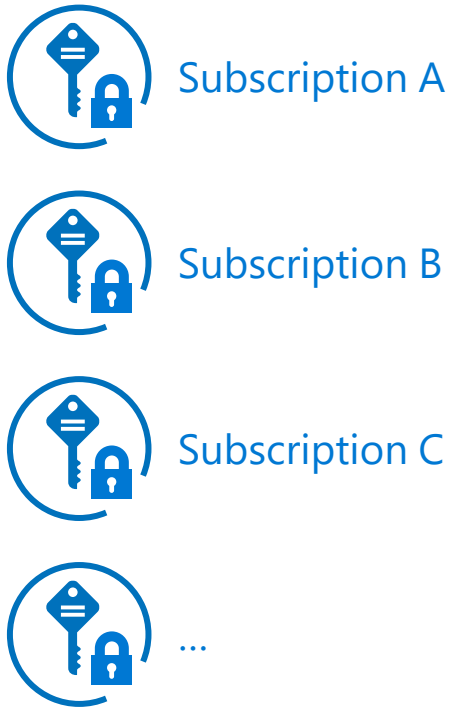
- Who are the subscription administrators
- Least privilege model

Scalability Requirements

- Growth plans
- Allocation of limited resources
- Evolution over time (users, shared access, resource limits)

Single subscriptions vs. multiple | Considerations

- Subscriptions have different quota limits for different resource types
- At a certain level of usage you will need to create new subscriptions to scale out, so you need to have a strategy for doing so
  - A very crucial workflow that can slow down a lot of organizations
- Some questions you'll need to answer:
  - Who will be responsible for creating subscriptions?
  - What resources will be in a subscription by default?



Organize subscriptions

Ask yourself the following questions:

- Are there any capacity / technical limitations?
- Do we want to ensure separation of concerns? In example:
  - Separation of duties
  - Dev/Test Vs. Production
  - Different end customers
  - Different departments or business units
  - Different projects
- What is the right naming convention to be used?
  i.e.: `<Company> <Department (optional)> <Product Line (optional)> <Environment>`
- Use a dedicated subscription for shared infrastructure (i.e. Azure Active Directory, monitoring and patching tools…). You will be able to spread the cost of this mutualized infrastructure to app owners.

Azure Role-Based Access Control (RBAC)

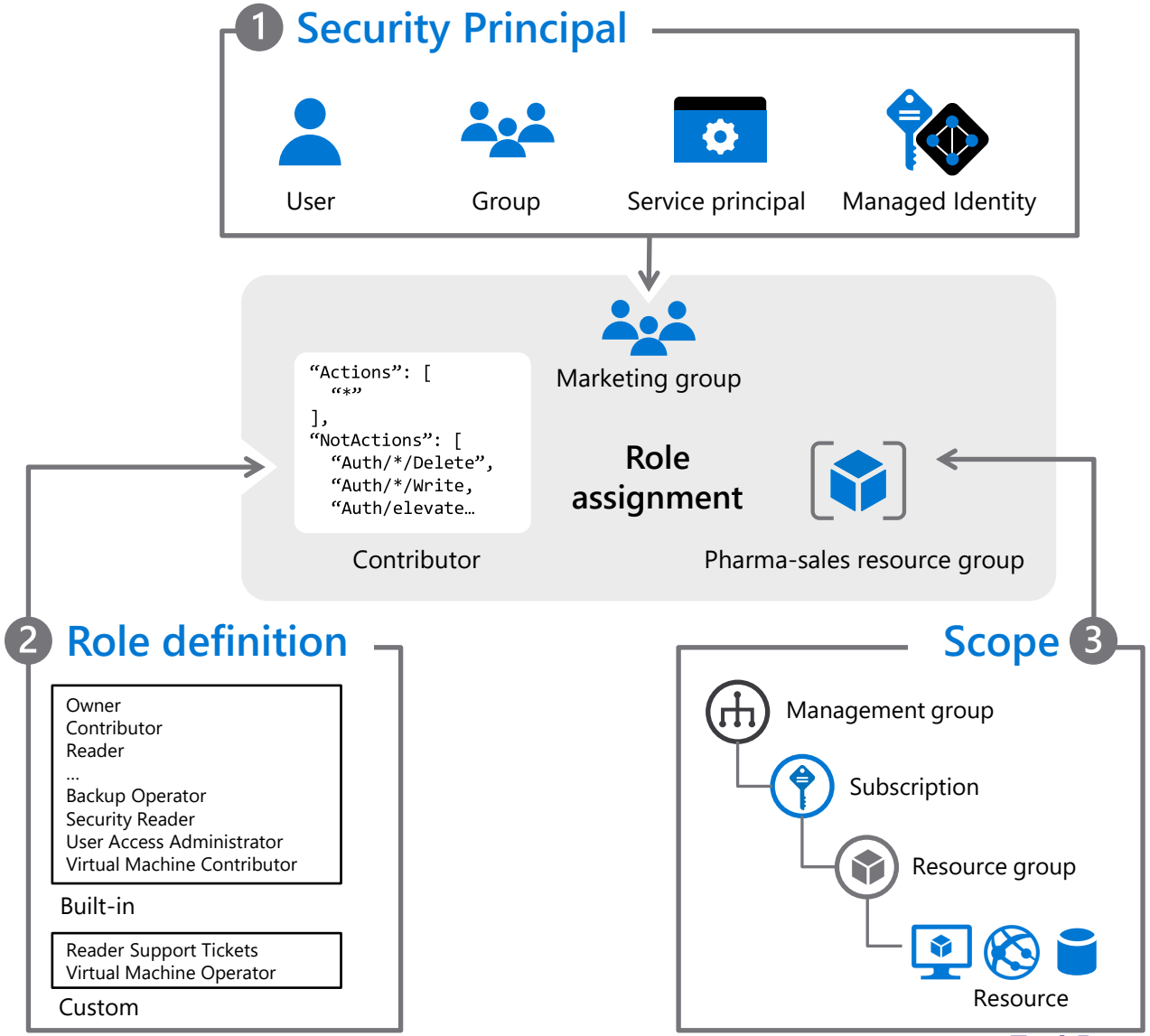
Fine-grained access control to Azure "control plane"

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

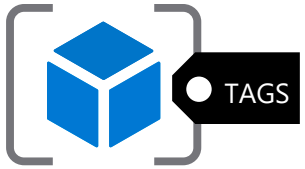


Resource Groups, Tags and RBAC

Finance/Business

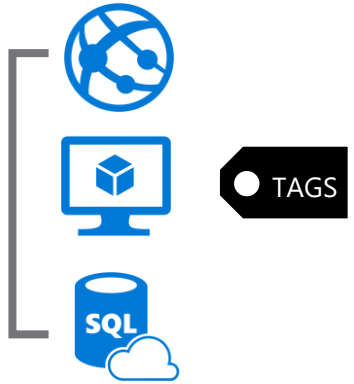
Need to be able to break out costs by various dimensions such as Customer, Cost Center, Environment.

Create roles with appropriate permissions.



Always Tag!

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



Resources in an RG should be tagged as needed.

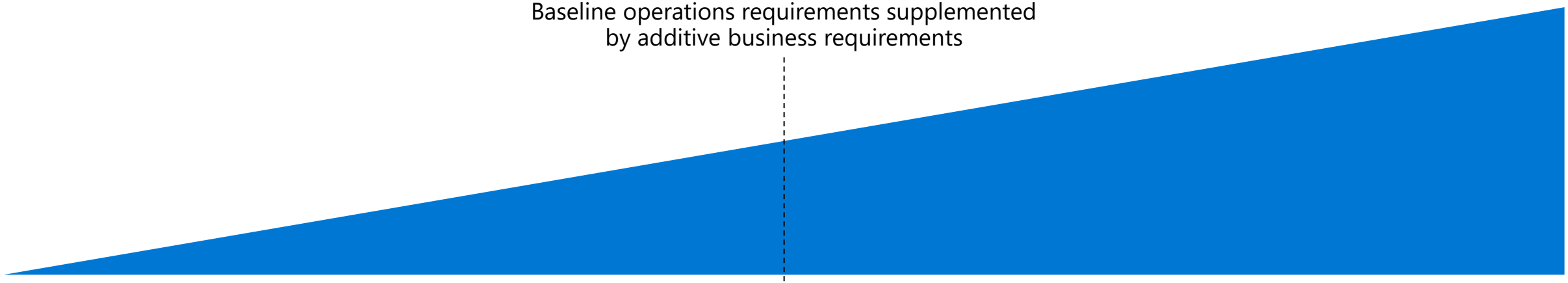
Tagging Decision Guide

IT Aligned Tagging

Business Aligned Tagging

Primary design considerations:

Baseline operations requirements supplemented by additive business requirements



Baseline Naming Conventions

- Resource naming is required for any deployment
- A standardized Naming Scheme is the minimum “Tag”

Functional

- Add tags that describe the function of the VM 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, Private, Confidential, etc.), Criticality, SLA

Accounting

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

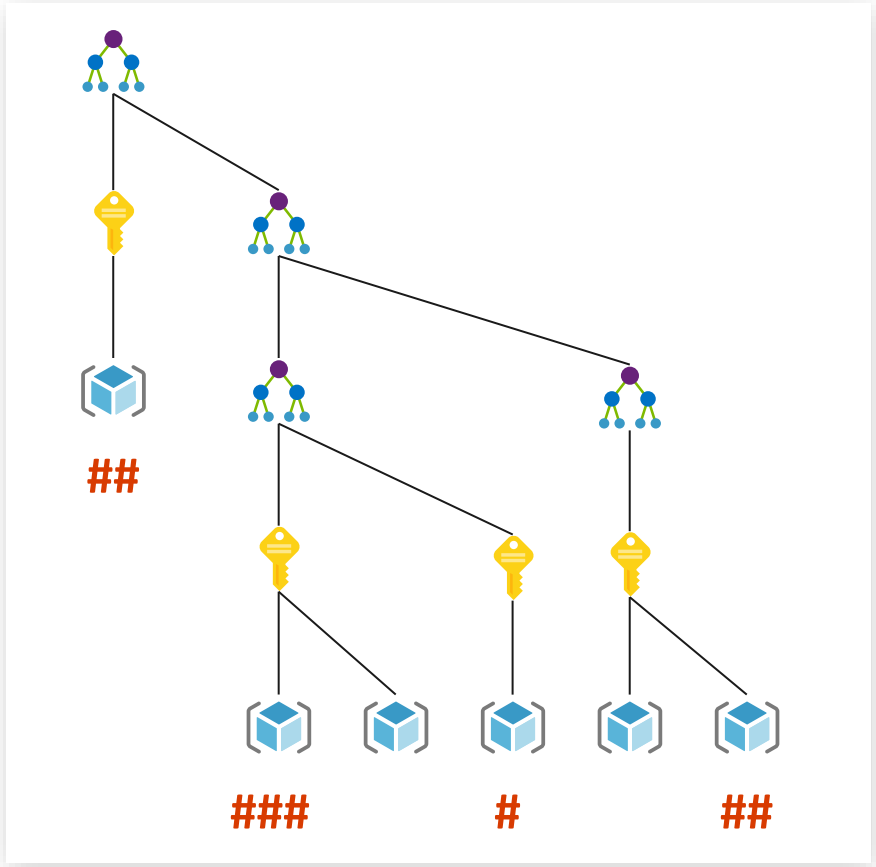
Partnership

- Align partners that count on this asset, outside of IT
- Example: Owner, Owner Alias, Stakeholder, Power User, Executive

Purpose

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

Tags add context for cost analysis



TAG = #

Finance codes - CostCenter tag, etc.

Application context - AppService tag, etc.

Deployment context - Environment tag, etc.

Who is accountable - BusinessOwner tag, etc.

Tags should be enforced by configuration policies

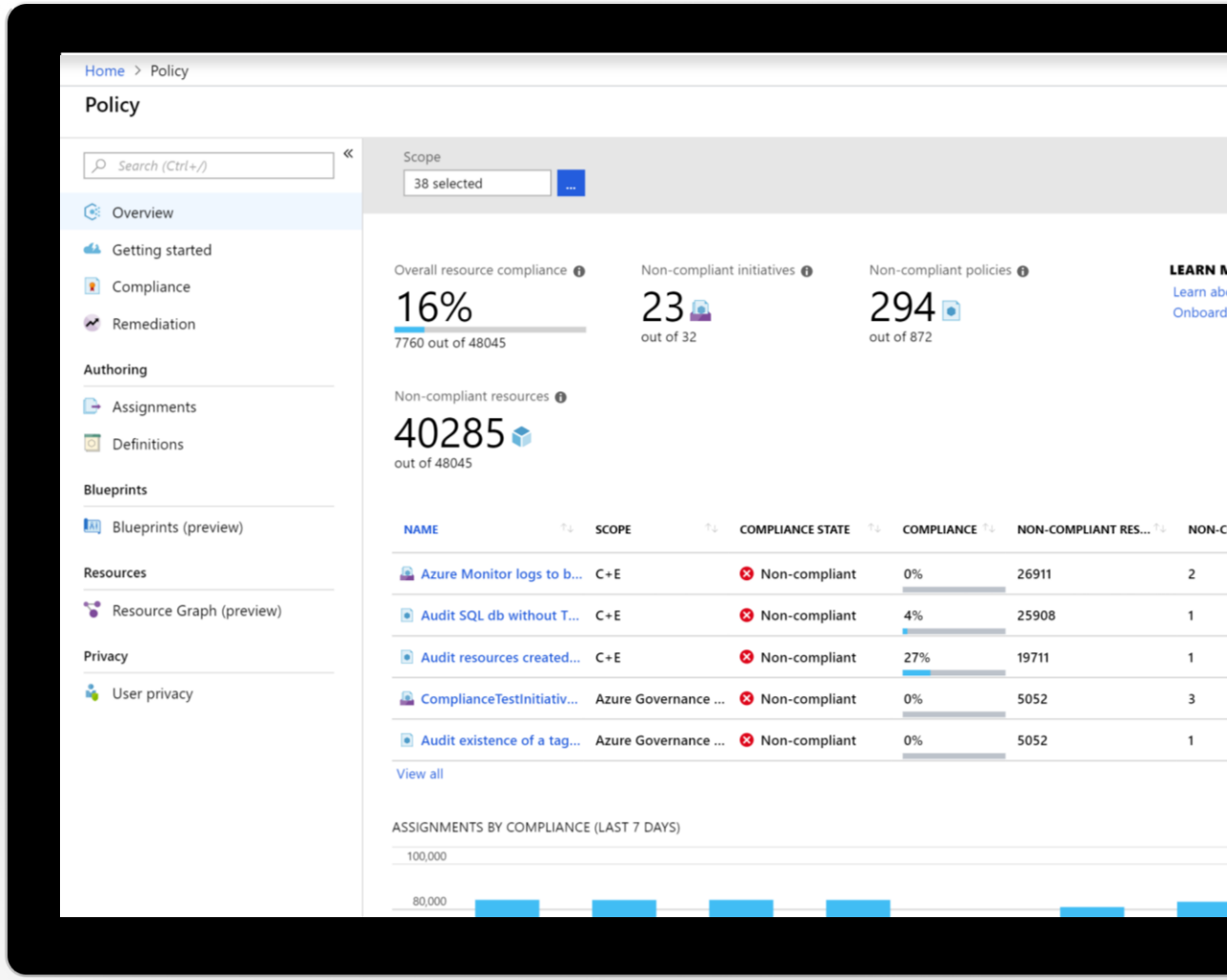
Use Azure Policy to set and track tagging policies

MG, Subscription, RG scopes

- Enforce that tags exist
- Set default values for tags
- Audit if tags are missing

Azure Policy | Key info

- Real time policy enforcement and at-scale compliance assessment
- Policy evaluates all Azure resources & in-guest VM
- Policy generate compliance events that can be used for alerting
- Aggregated and raw compliance data are available through API, PowerShell & CLI
- Can be used to automatically remediate problems in your environment



TechDay پاکستان

Azure Policy | Scenarios

- Restrict location or resource type (built-in)
- Inherit tags from Resource Group (see right →)
- Block 'open to any' NSG rule creation (Github)
- Enable diagnostic logs at-scale (MVP blog)
- Security (built-in from Azure Security Center & In-Guest)

```
{
  "mode": "indexed",
  "policyRule": {
    "if": {
      "field": "tags.costCode",
      "exists": "false"
    },
    "then": {
      "effect": "append",
      "details": [
        {
          "field": "tags.costCode",
          "value": "[resourcegroup().tags.costCode]"
        }
      ]
    }
  }
}
```

Azure Policy | Best practices

- Start with Audit Policies, which is a safe way of understanding what a policy will do without affecting user activity
- Used staged rollouts for Deny policies to understand impact
- Rollout remediation in stages

Details | Definition (JSON)

Duplicate this policy definition

```
{
  "if": {
    "anyOf": [
      {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Compute/virtualMachines"
          },
          {
            "field": "Microsoft.Compute/virtualMachines/osDisk.
            "exists": "True"
          }
        ]
      },
      {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Compute/VirtualMachineScaleSet
          },
          {
            "anyOf": [
              {
                "field": "Microsoft.Compute/VirtualMachineScale
                "exists": "True"
              },
              {
                "field": "Microsoft.Compute/VirtualMachineScale
                "exists": "True"
              }
            ]
          }
        ]
      }
    ]
  },
  "then": {
    "effect": "audit"
  }
}
```

Cloud Governance Team and Functions

A cloud governance team evaluates and manages risk tolerance, identifies high-risk areas for business, and converts risks into governing corporate policies.

- Ensures cloud-adoption risks and risk tolerance are properly evaluated and managed.

- Identifies risks that can't be tolerated by the business, and it converts risks into governing corporate policies.

Cloud Governance Team

- Review Govern module of Cloud Adoption Framework
- Complete the governance benchmark
- Implement the governance MVP approach
- Continuously improve governance maturity

Cloud Governance Team

Align with other teams to

- Review your company's strategy and plan
- Review your company's cloud adoption plan
- Review the operation team's operations management workbook

Establish cadence with teams that aligns with

- Release and planning cycles.
- The cloud strategy team to review risks of the next wave of adoption and gauge the team's level of tolerance for risks.
- Review and iterate.

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

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:
- Network:

Implement these best practices for corporate policy:

- Network requirements:
- Hybrid identity strategies:
- Encryption:
- Security Baseline policies:

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

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.

Operationalize Azure Privileged Identity Management

- Cloud-based identity management is an iterative process.

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 repeatable 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

TechDay پاکستان

Thank you

#TechdayPakistan | @TechDayP | TechDayPakistan.com

TechDay پاکستان