AZUREISH Live!

Mert to the Future

Azure Landing Zones

with
Abdul Kazi

10/03/2022

6pm GMT

/azureishlive

Abdul Kazi

Blogger | Mentor | Speaker

abdulkazi

www.abdulwkazi.com

abdulwkazi

Agenda

- Cloud Adoption Motivations
- The value of creating cloud-ready environments
- Microsoft Cloud Adoption Framework for Azure
- Azure Landing Zones in Cloud Adoption Framework
- Azure Landing Zones Design Areas
- Azure Blueprints
- Azure Policy

Cloud Adoption Motivations

Why is the company adopting the cloud?
More than one motivation is common in most cloud adoption efforts

Critical Business Events

- Data center exit
- Mergers, acquisition or divestiture
- Reductions in capital expenses
- End of support for mission critical technologies
- Regulatory compliance, data sovereignty requirements
- Reduce disruptions and improve IT stability

Migrate Motivations

- Cost Savings
- Reduction in vendor or technical complexity
- Optimization of internal operations
- Increase business agility
- Prepare for new technical capabilities
- Scale to meet market demands
- Scale to meet geographic demands

Innovation Motivations

- Prepare for new technical capabilities
- Build new technical capabilities
- Scale to meet market demands
- Scale to meet geographic demands
- Improve customer experiences / engagements
- Transform products or services
- Disrupt the market with new products or services

The value of creating cloud-ready environments

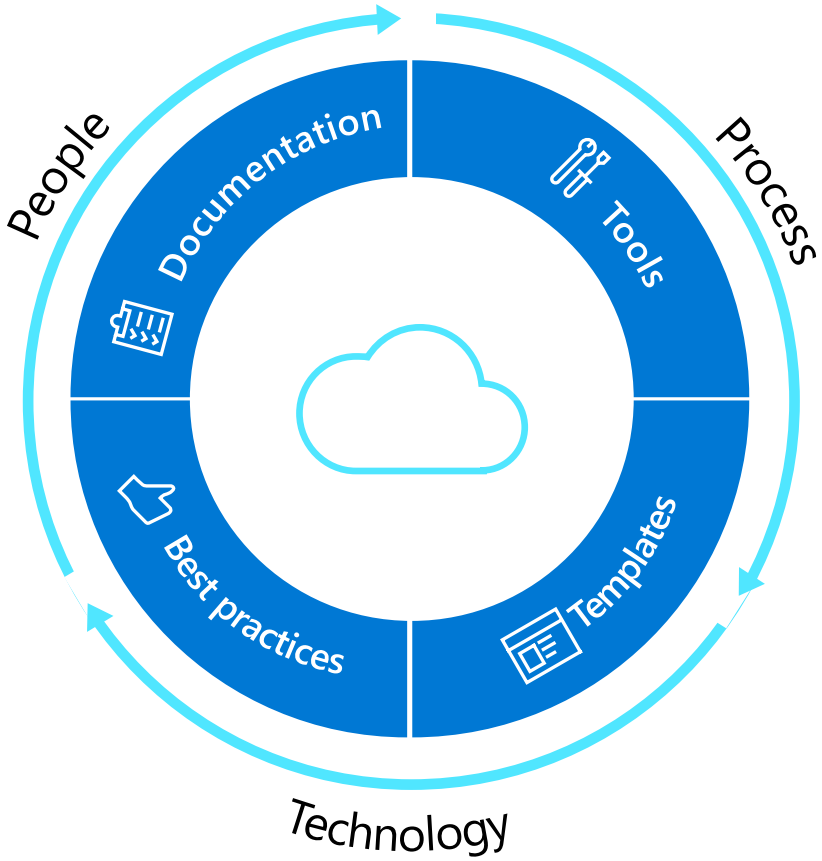
- Aligned to business priorities
- Cloud-design considerations
- Adapted for cloud operating model
- Ready for cloud applications
- Adaptable to grow and expand
- Compliant

Agile

Cutting-edge innovation

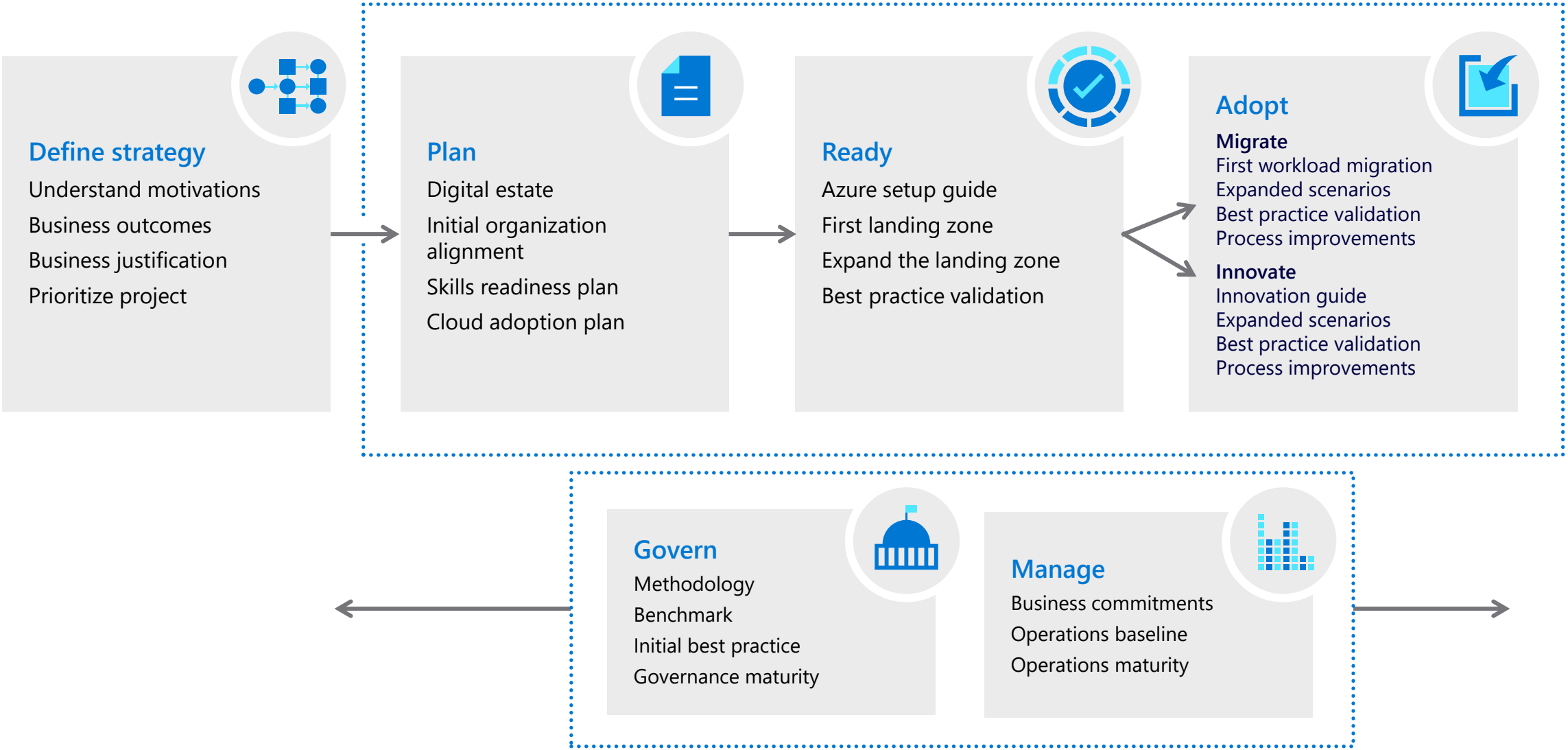
Secure

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



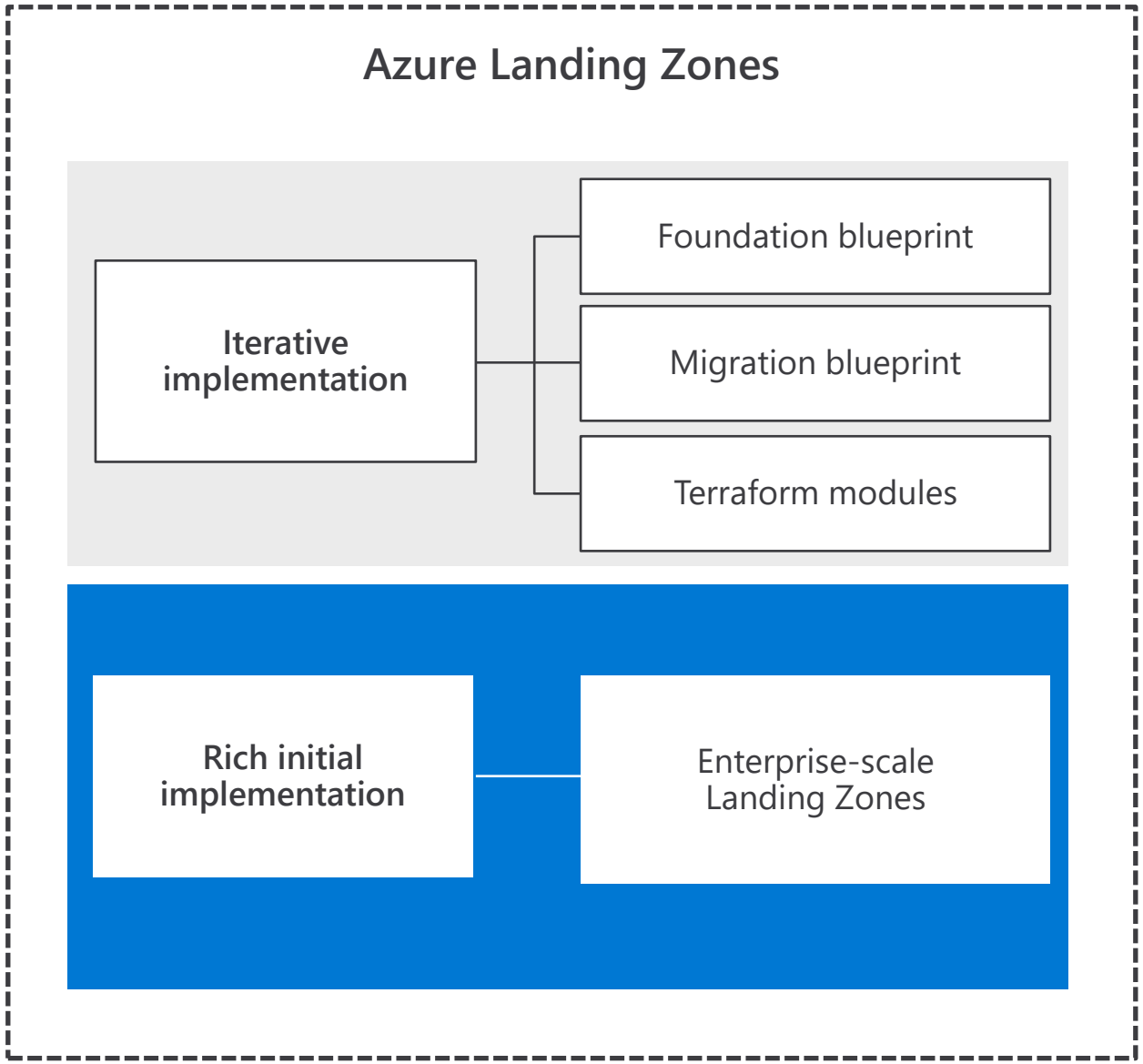
Azure landing zones help customers set up their Azure environment for scale, security, governance, networking, and identity.

Azure landing zones:

- Enable migrations and net new apps
- Consider all platform resources
- Don't differentiate between IaaS or PaaS

How do you get started?

Platform Development Velocity: how fast your cloud platform team can develop the required skills.



Azure landing zones

Design areas

- Enterprise Enrollment
- Identity
- Resource Organization
- Network Topology & Connectivity
- Business Continuity & Disaster Recovery
- Governance Disciplines
- Deployment Options
- Operations Baseline

Do you need more?

To migrate you absolutely need:

- RBAC
- Network
- Naming & Tagging

But you may need a mature landing zone configuration to address:

- Governance
- Security
- Operations
- Shared foundational utilities

Enterprise Enrollment

Business Continuity & Disaster Recovery

Identity

Governance Disciplines

Resource Organization

Deployment Options

Network Topology & Connectivity

Operations Baseline

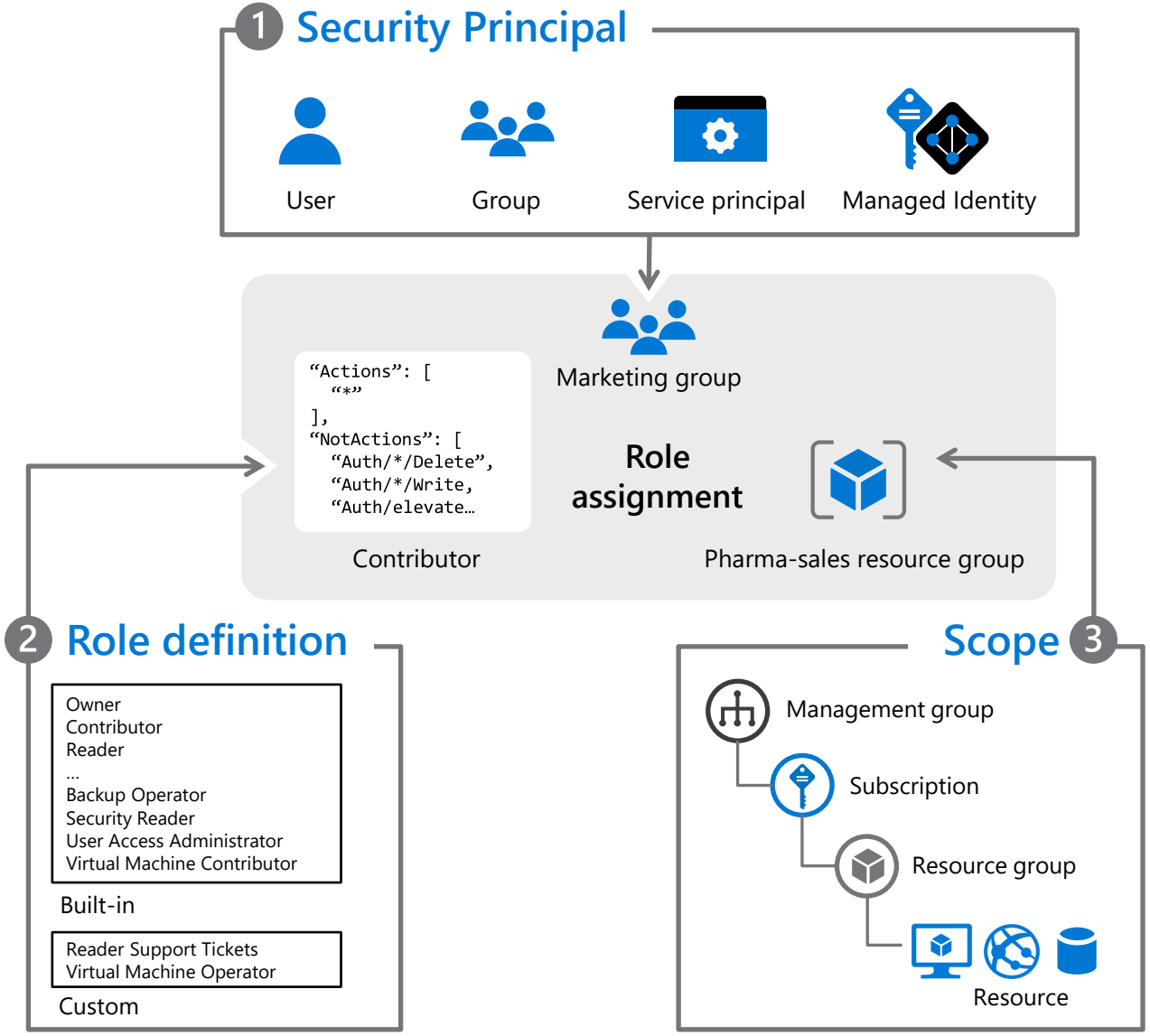
Azure Role-Based Access Control (RBAC)

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

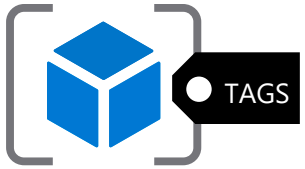
©Microsoft Corporation
Azure

Resource Groups, Tags and RBAC

Finance/Business

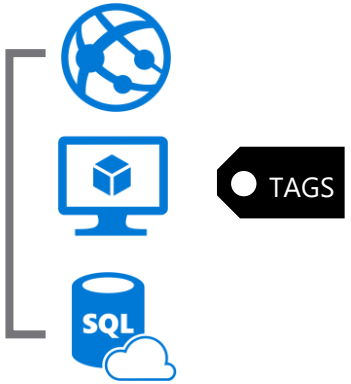
Need to be able to break out costs by various dimensions such as Customer, Cost Center, Environment.

Create roles with appropriate permissions.



Always Tag!

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



Resources in an RG should be tagged as needed.

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

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

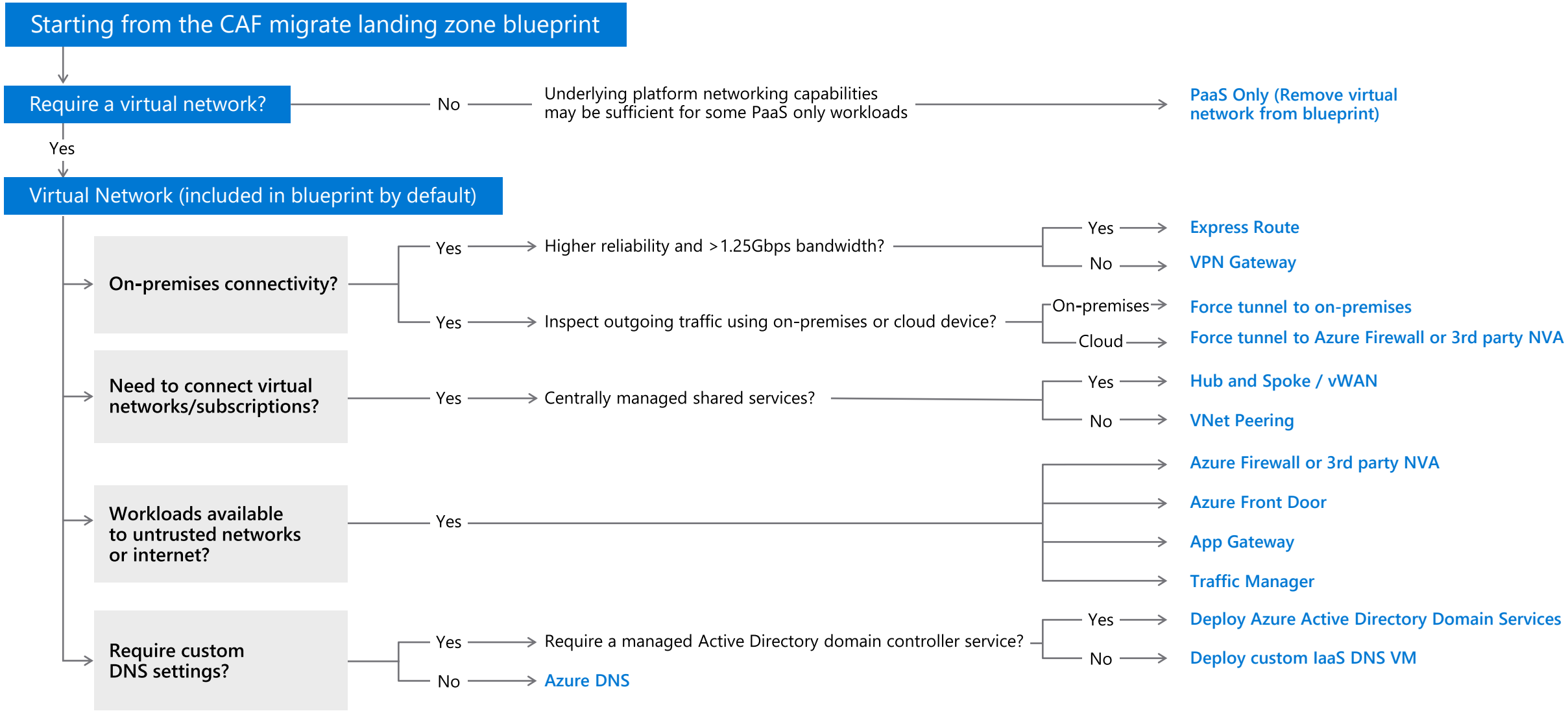
- Align partners that count on this asset, outside of IT
- Example: Owner, Owner Alias, Stakeholder, Power User, Executive

Purpose

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

Network decision guide

Evaluate each of the following concerns to identify potential services and features when modifying your blueprint



Factors that influence the right setup

Organize Azure to reflect your organization, not the other way!

Cost transparency:

- Set up a cost structure that reflects the actual usage for departments and projects
- Tagging and ownership
- Allowed resource types (policy)

Roles and responsibility:

- Who has access to what. Account owners and delegations (RBAC)
- Minimal access level to carry out the task
- Design for Partners and 3rd parties

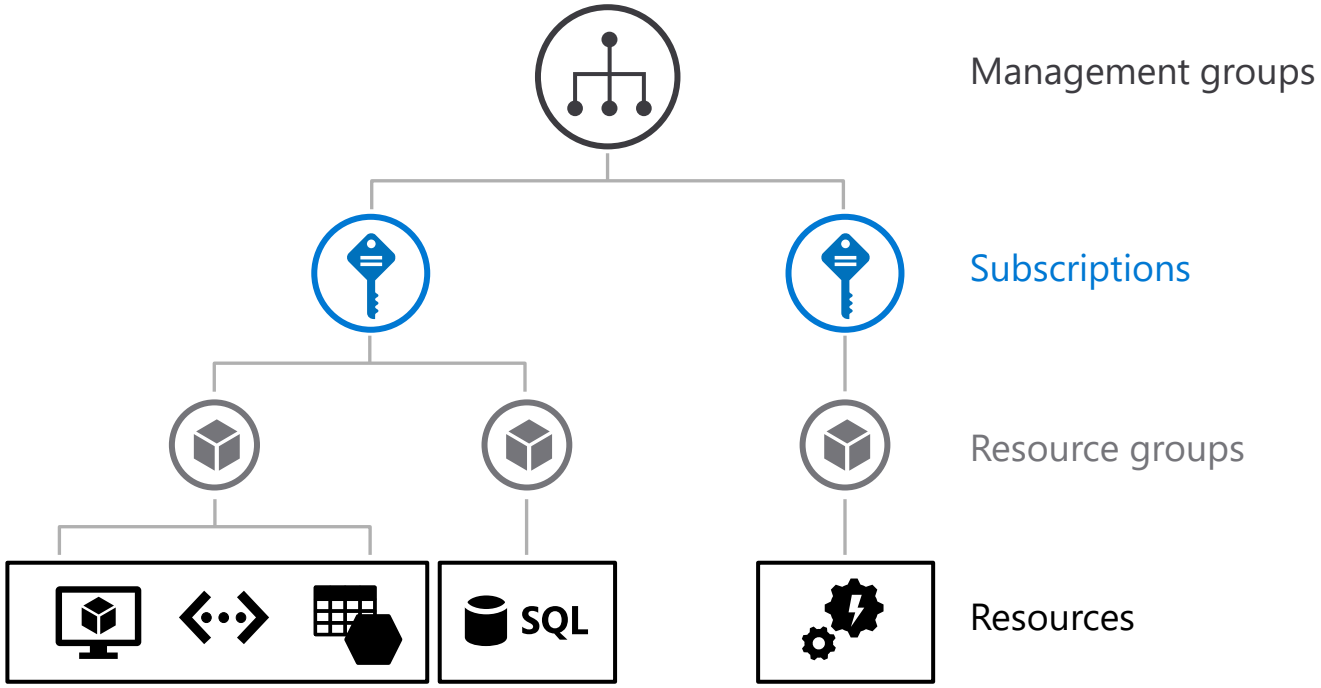
Compliance and Security:

- Allowed locations e.g. EU (policy)
- Network and connectivity (Internet facing, or using the approved VNETS? Policy and NSG)
- Continuous Monitoring and integration to existing ITSM (Azure Monitor)

©Microsoft Corporation
Azure

How to organize your Azure Resources

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



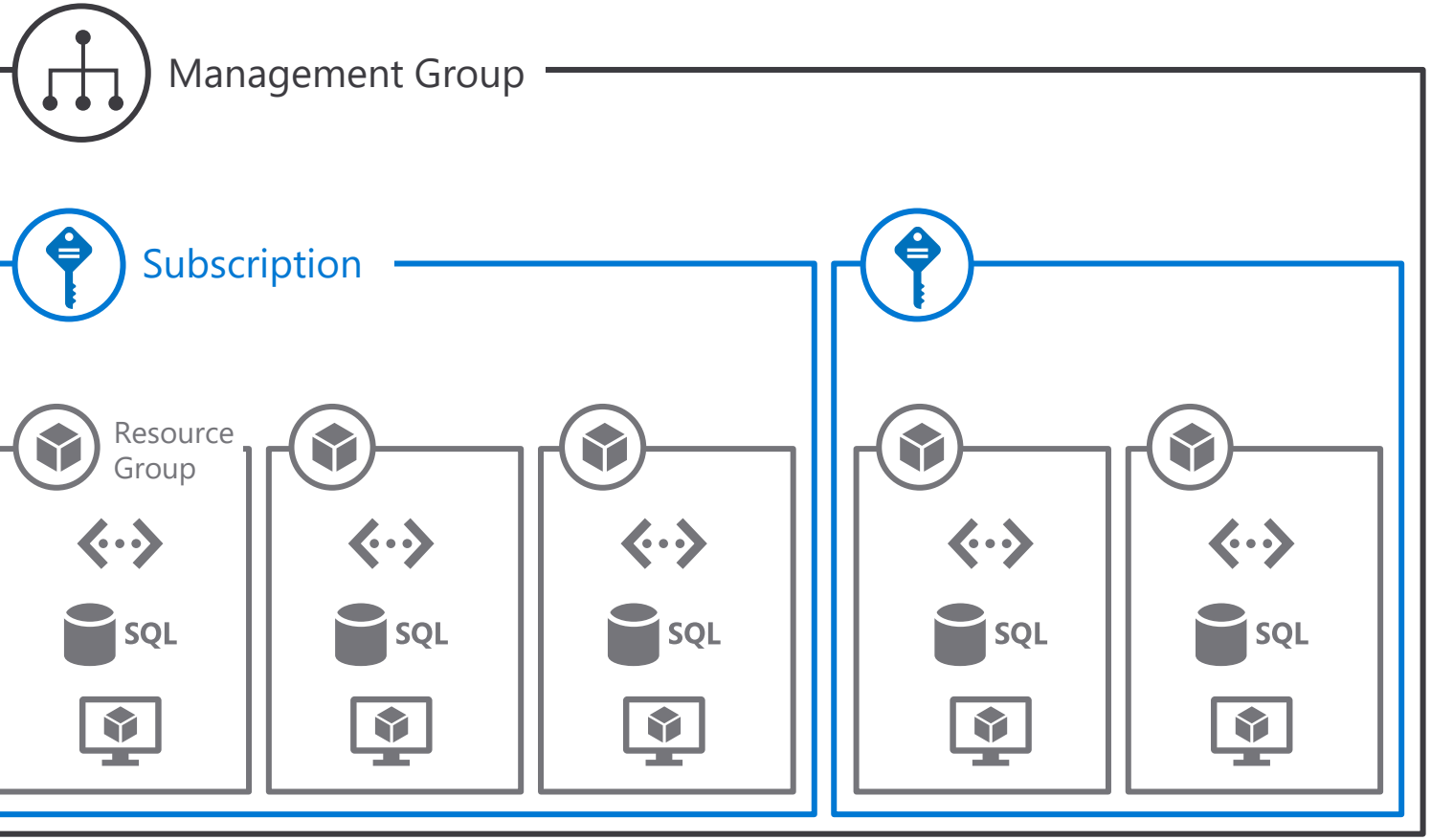
What is Resource Consistency?

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.

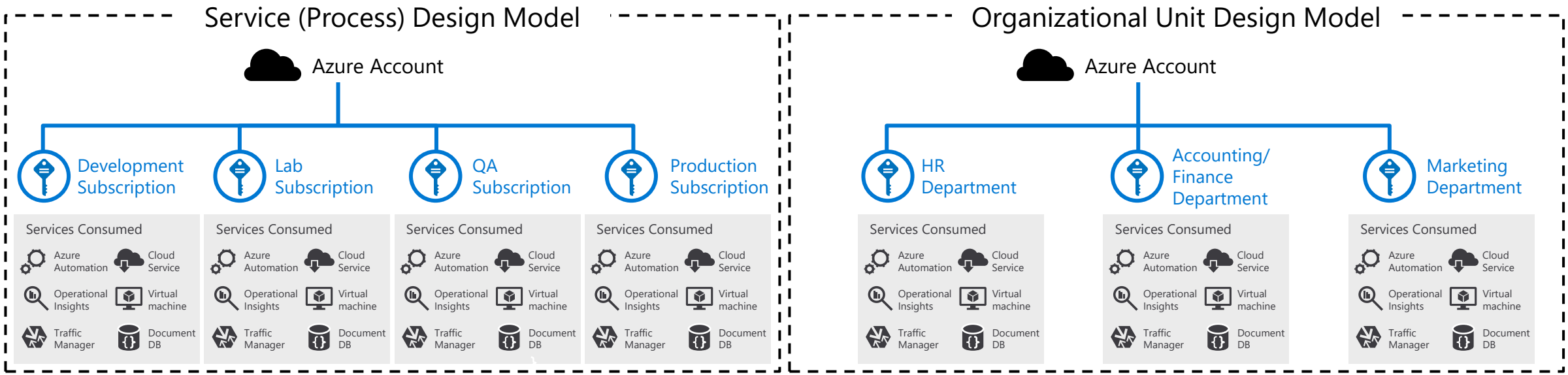
Resource Groups
To further group applications or workloads into deployment and operations units.



©Microsoft Corporation
Azure

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

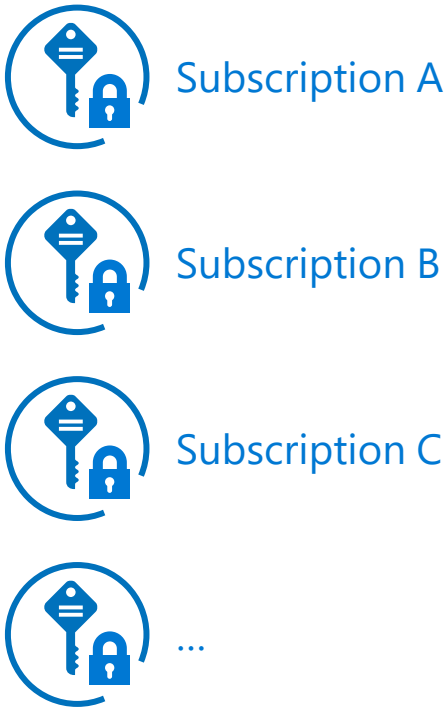
Scalability Requirements

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

©Microsoft Corporation
Azure

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?



©Microsoft Corporation
Azure

Organize subscriptions

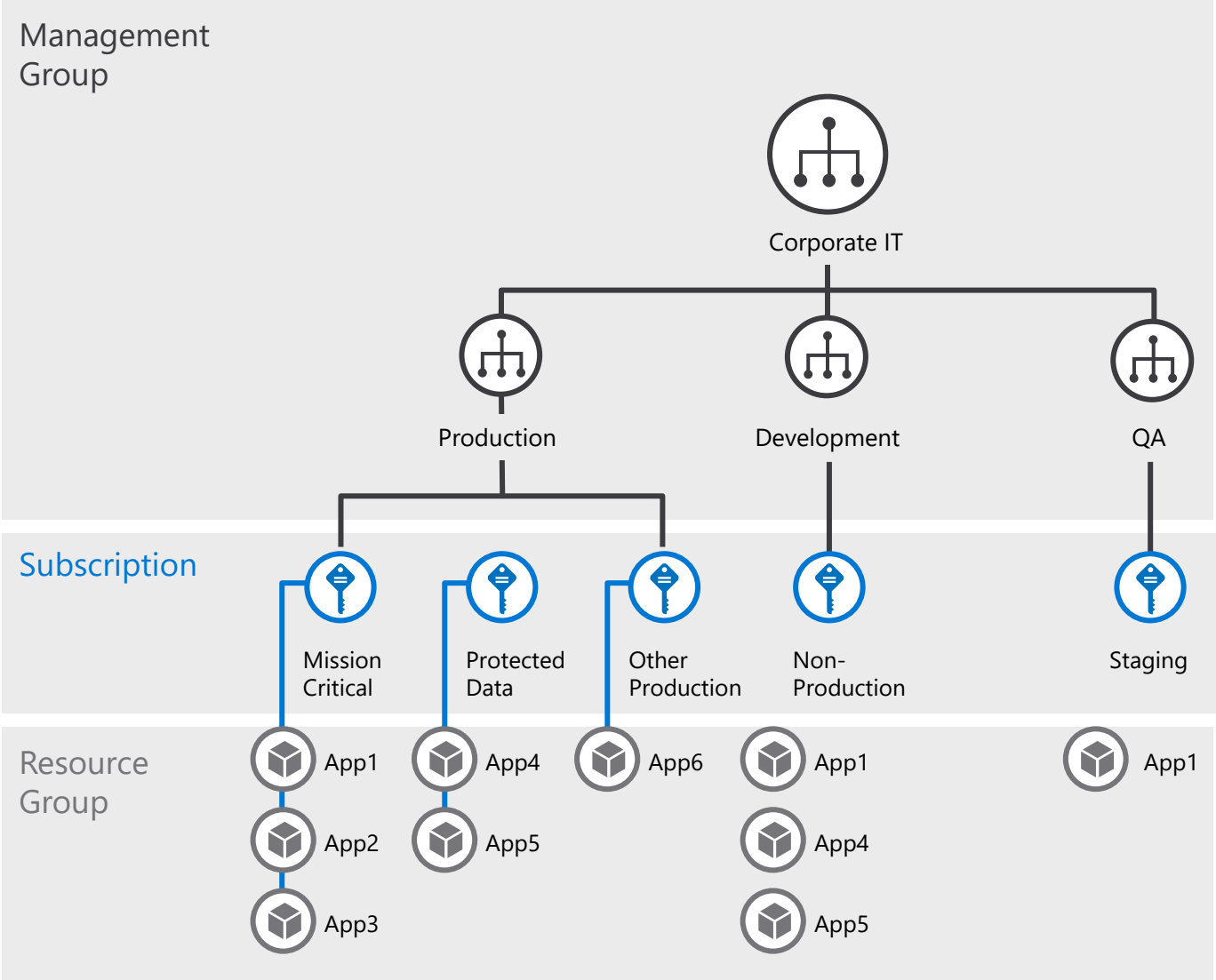
Ask yourself the following questions:

- 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.

©Microsoft Corporation
Azure

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



©Microsoft Corporation
Azure

Governance MVP Considerations

Resource Organization

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

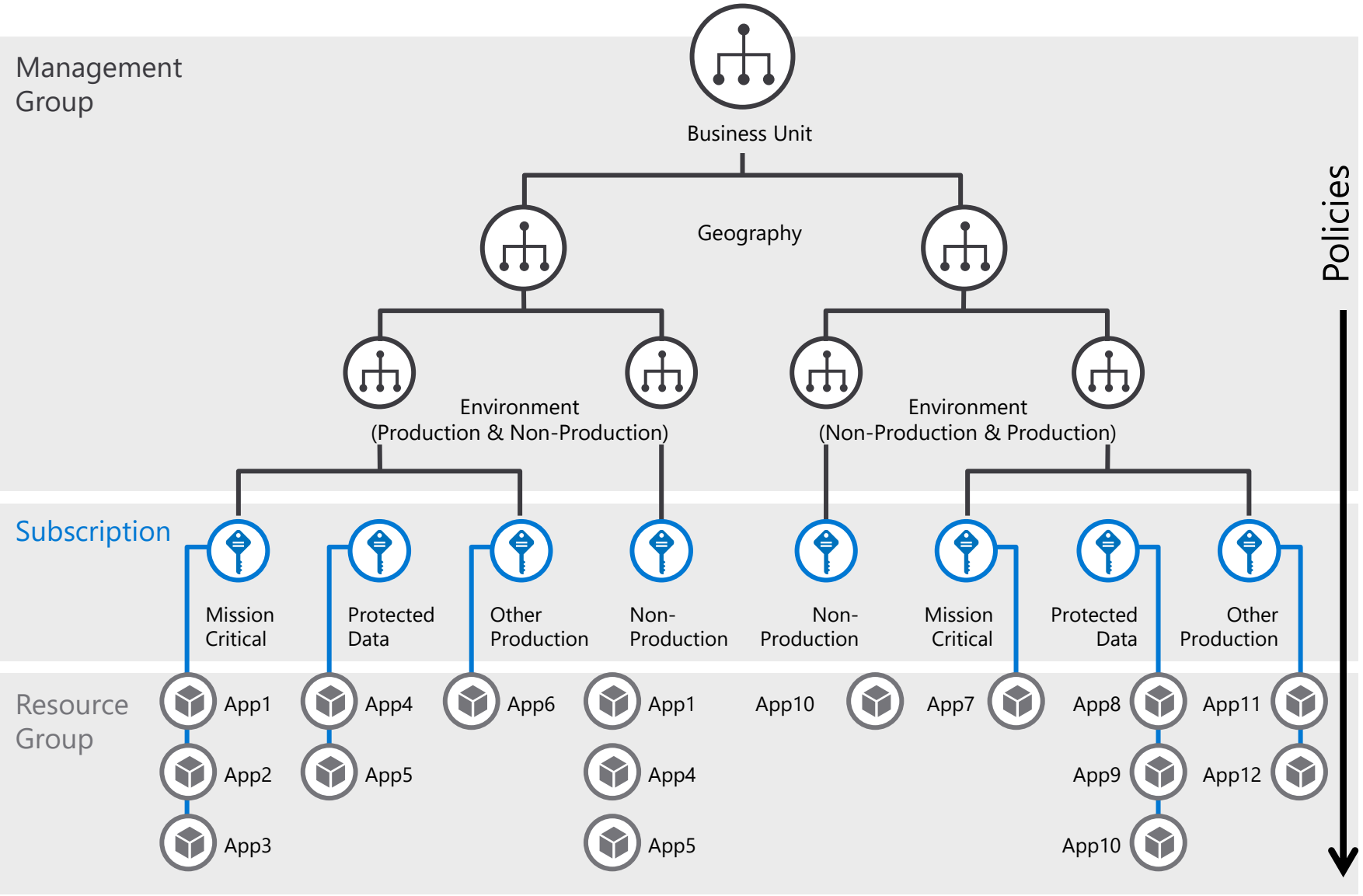
Management Group Hierarchy

- Business Unit
- Geography
- Environment

Subscription

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

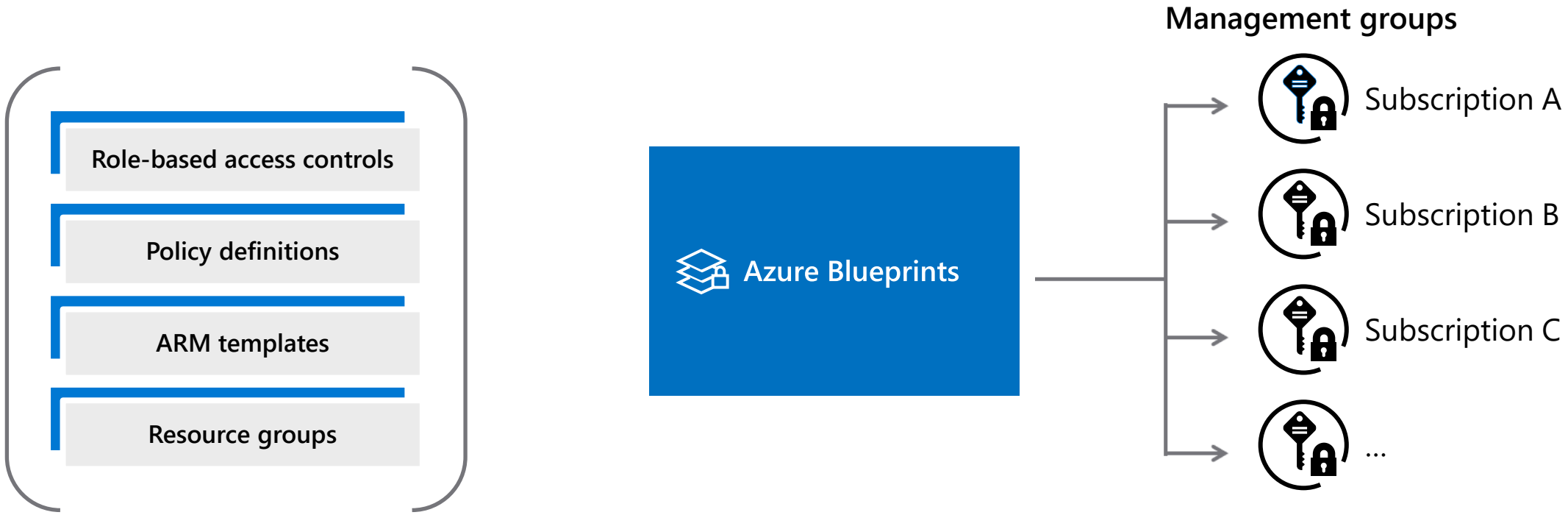
Resource Groups



Microsoft Confidential

Azure Blueprints

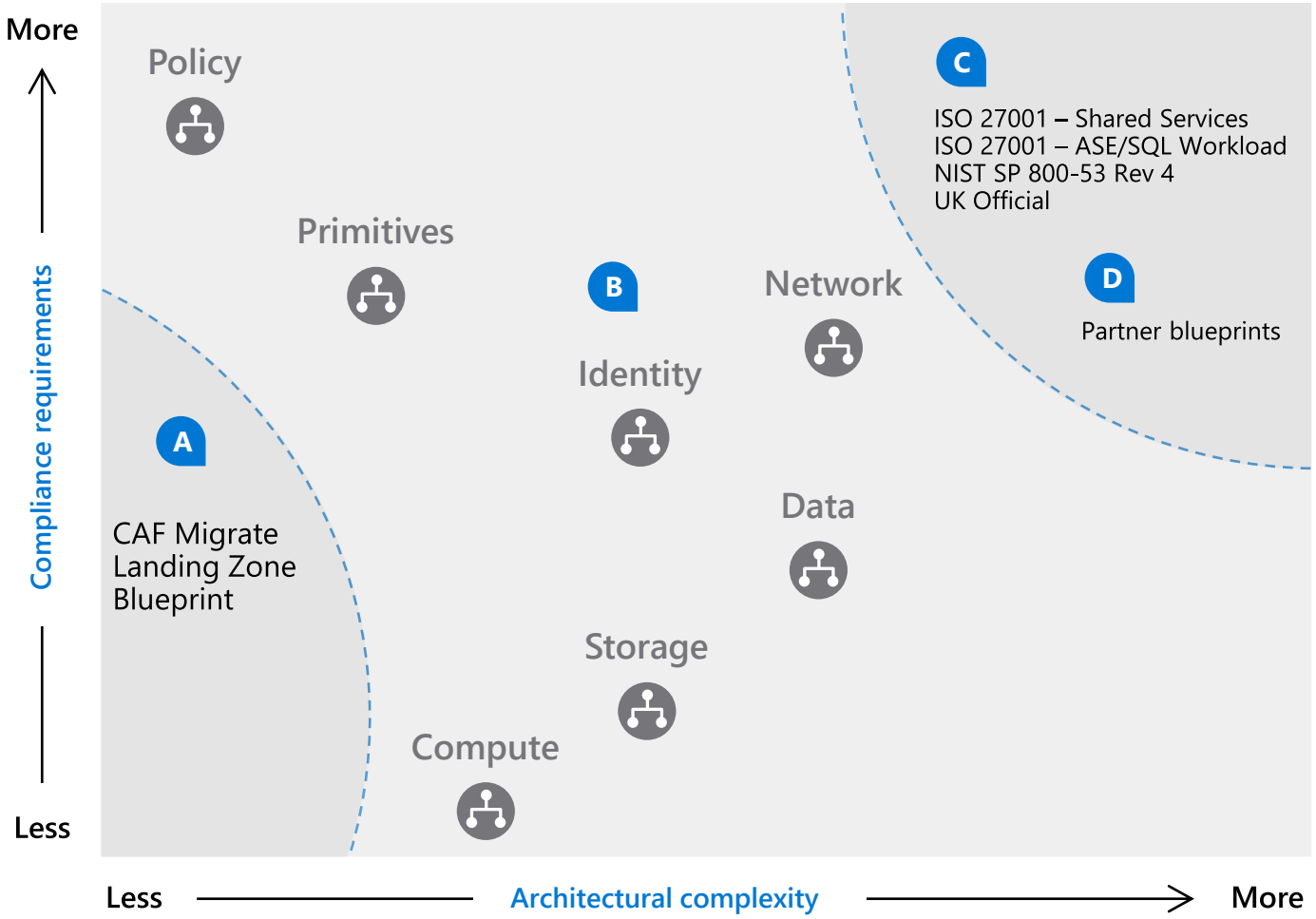
Deploy and update cloud environments in a repeatable manner using composable artifacts.



compose | manage | scale

Ready | First Landing Zone

- Landing zone is the environment that is provisioned to host workloads being migrated from an on-premises environment into Azure.
- The Cloud Adoption Framework migrate landing zone blueprint creates a landing zone which can be updated to meet your specific needs.

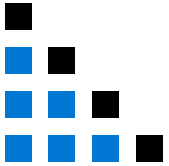


Ready | Expand the landing zone

The considerations for implementing a landing zone fall into three categories.

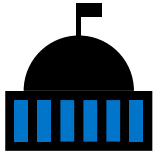
Hosting

Decisions need to be made around compute, storage, networking, databases to help create hosting options in the landing zone blueprint.



Azure fundamentals

These are the foundational building blocks for organizing resources in the cloud environment.



Governance considerations

Applying governance principles on each landing zone.

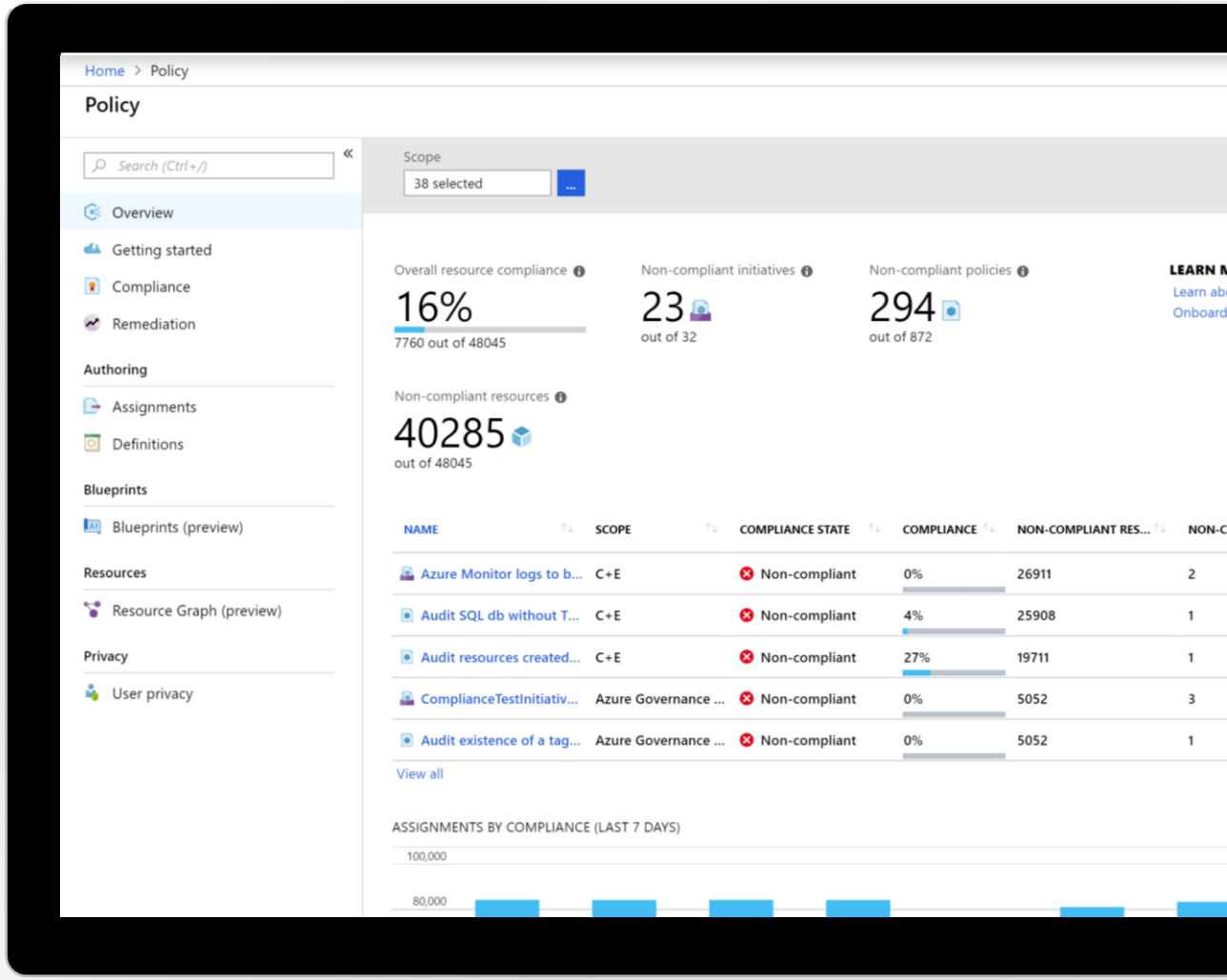
Ready | Recommended Practices

Leverage best practices in Cloud Adoption Framework to help your teams establish and prepare the Azure environment. These include guidance in the areas of:

- Azure fundamentals
- Networking
- Identity and Access Control
- Storage
- Databases
- Cost Management

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



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

```
1  {
2    "if": {
3      "anyOf": [
4        {
5          "allOf": [
6            {
7              "field": "type",
8              "equals": "Microsoft.Compute/virtualMachines"
9            },
10           {
11             "field": "Microsoft.Compute/virtualMachines/osDisk.
12             "exists": "True"
13           }
14         ]
15       },
16       {
17         "allOf": [
18           {
19             "field": "type",
20             "equals": "Microsoft.Compute/VirtualMachineScaleSet
21           },
22           {
23             "anyOf": [
24               {
25                 "field": "Microsoft.Compute/VirtualMachineScale
26                 "exists": "True"
27               },
28               {
29                 "field": "Microsoft.Compute/VirtualMachineScale
30                 "exists": "True"
31               }
32             ]
33           }
34         ]
35       }
36     ]
37   },
38   "then": {
39     "effect": "audit"
40   }
41 }
```

AZUREISH Live!

Mert to the Future

Azure Landing Zones

with
Abdul Kazi

10/03/2022

6pm GMT

/azureishlive