Microsoft Azure

AZ-305

Designing Microsoft Azure Infrastructure Solutions
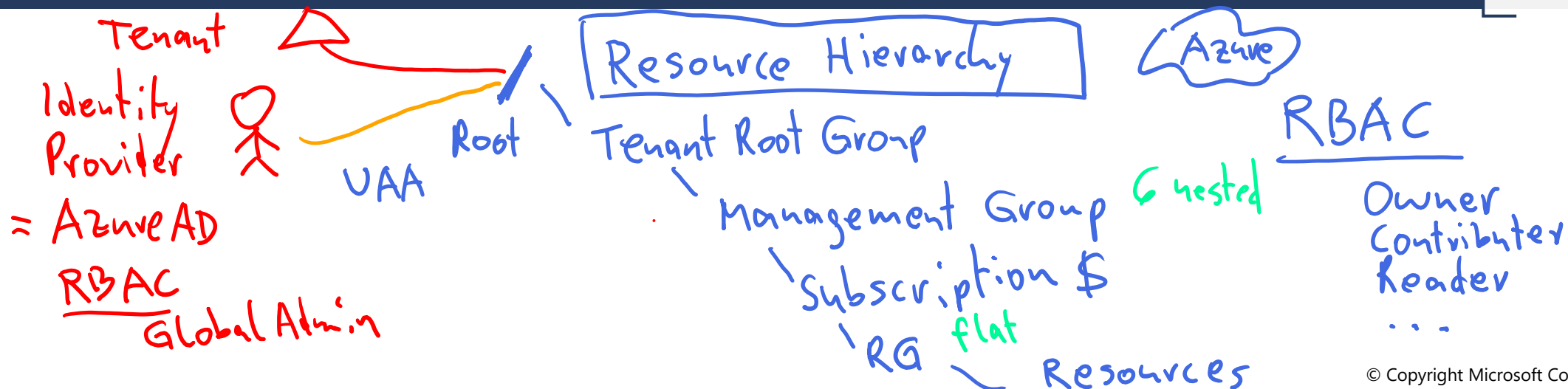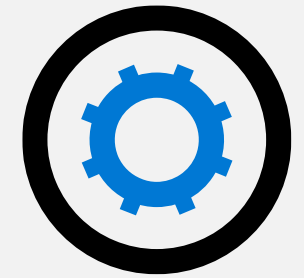
CAF   Cloud Adoption Framework
Landing Zones

Permission
Roles

Policies
Governances

Powershell
Az CLI

Design a governance solution

Tenant

Identity
Provider
= AzureAD
RBAC
Global Admin

UAA

Root

Resource Hierarchy

Tenant Root Group

Management Group   Nested

Subscription $

RG   flat

Resources

Azure

RBAC

Owner
Contributer
Reader
...

Introduction

- Design for governance

- Design for management groups

- Design for Azure subscriptions

- Design for resource groups

- Design for resource tagging

- Design for Azure Policy and RBAC

- Design with Azure Blueprints

- Design for Azure Landing Zones

- Case study

- Summary and resources

AZ-305: Design Identity, Governance, and Monitoring Solutions (25-30%)

Design Governance

- Recommend an organizational and hierarchical structure for Azure resources
- Recommend a solution for enforcing and auditing compliance

Design for governance
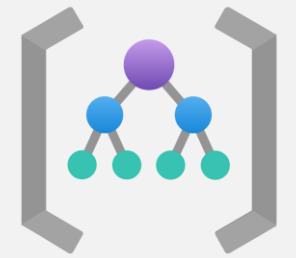
Govern resources in Azure

Governance provides mechanisms and processes to maintain control over your applications and resources in Azure.

- Determine your requirements, plan your initiatives, and set strategic priorities

- Plan for governance at every level
  - Management groups
  - Subscriptions
  - Resource groups
  - Resources
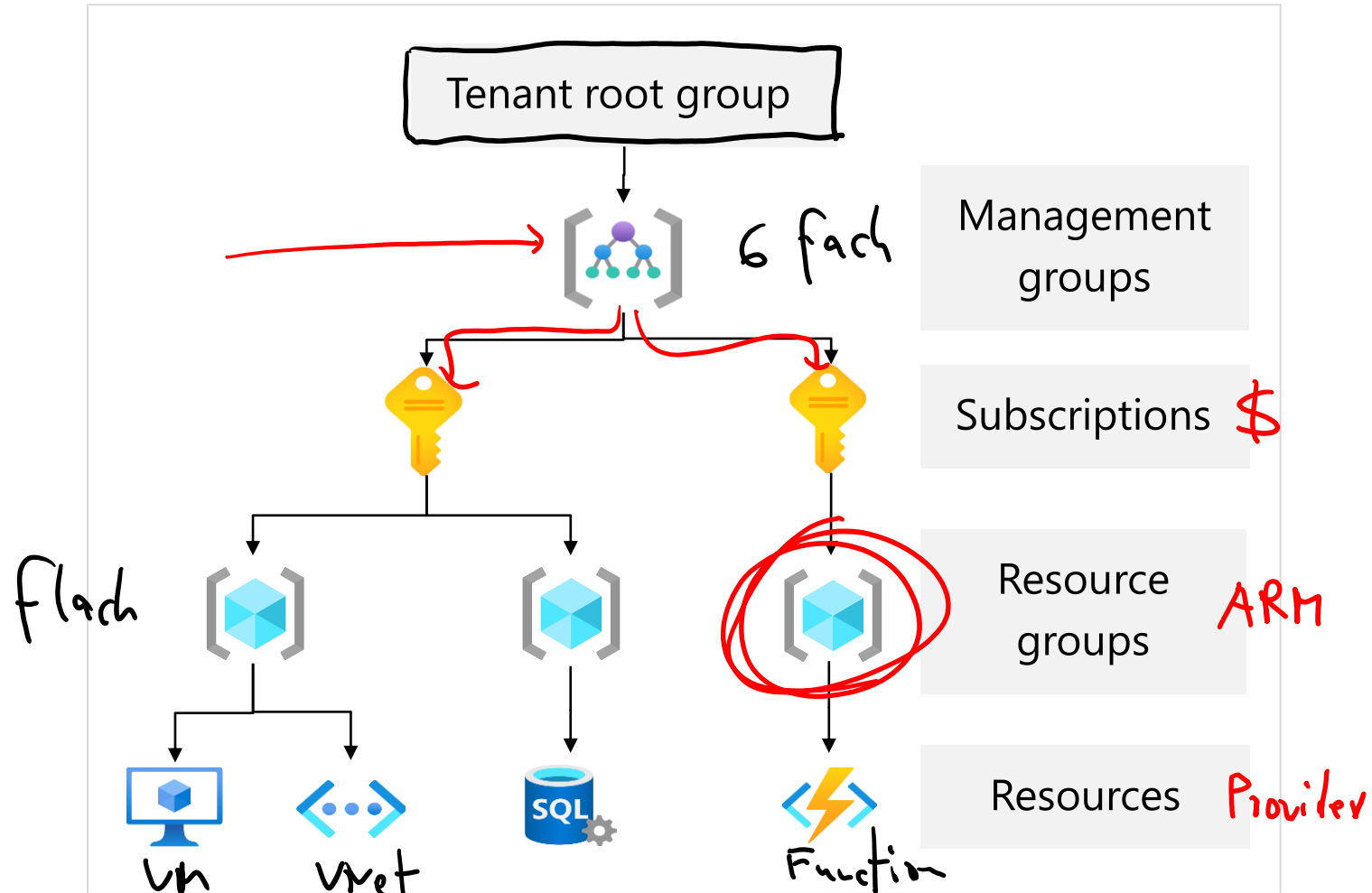
Classic Azure (von ARM)
Deployment → Cloud Service
Classic Roles < Account Admin
Service Admin
Co Admin (200)

Tenant root group

6 fach

Management groups

Subscriptions $

flach

Resource groups   ARM

Resources   Provider

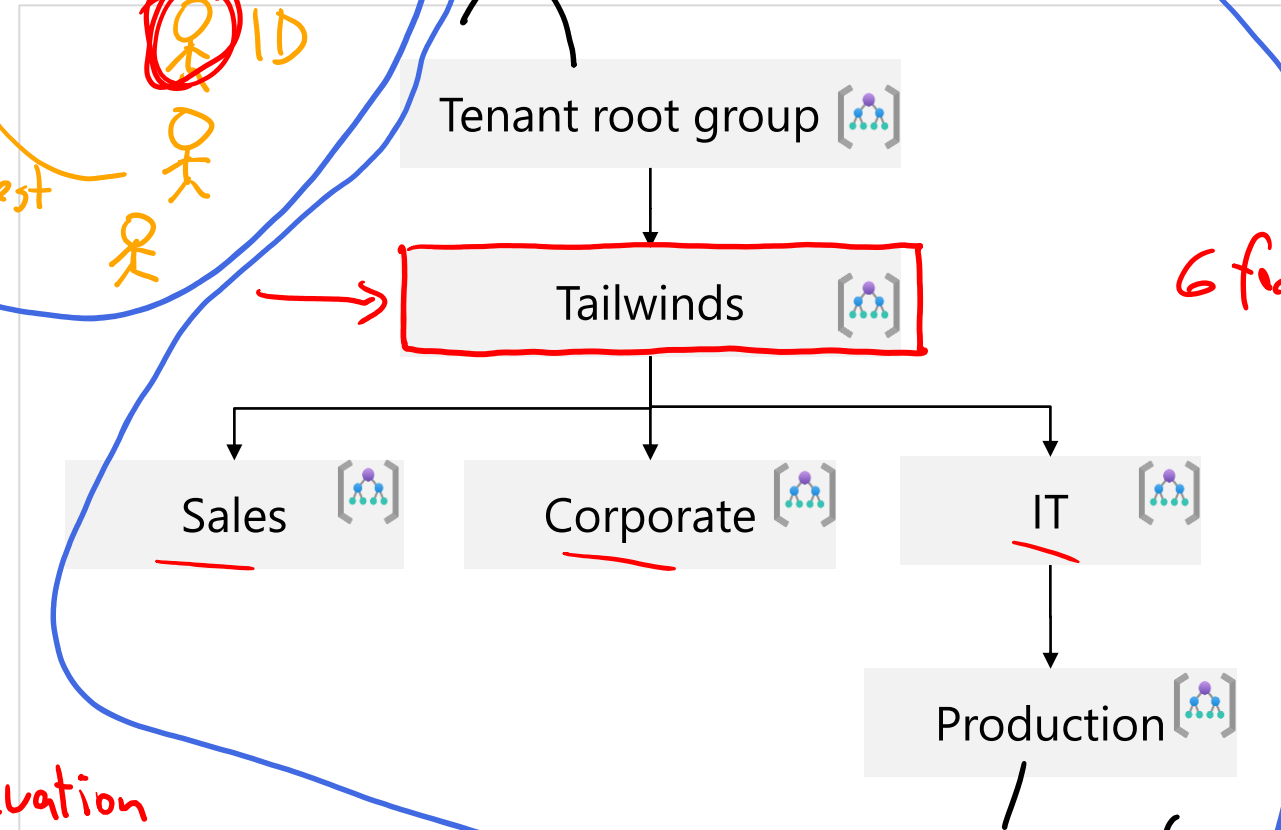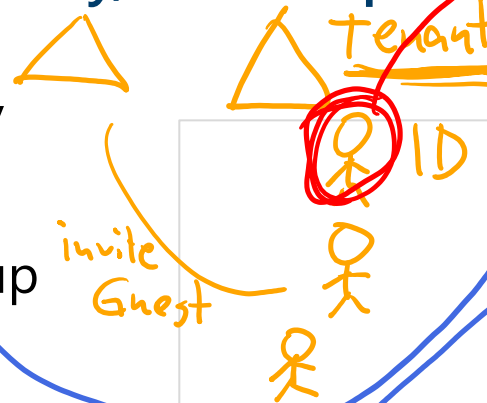vm   vnet   SQL   Function

Design for management groups

Plan your management groups

Management groups manage access, policy, and compliance for multiple subscriptions.

- Keep the management group hierarchy reasonably flat

- Consider a top-level management group

- Consider an organizational or departmental structure

- Consider a geographical structure

- Consider a production management group

- Consider a sandbox management group

- Consider isolating sensitive information in a separate management group
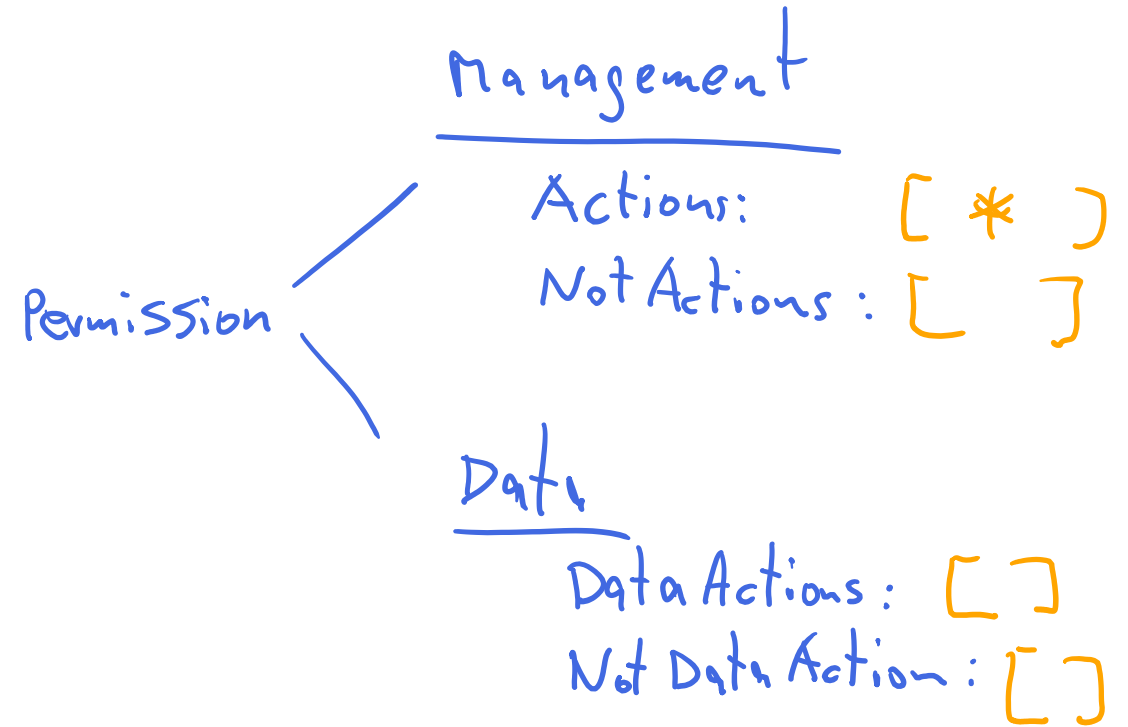
RBAC Global Admin

RBAC Owner

Tenant

ID

invite Guest

Root ← UAA

Tenant root group

Tailwinds

6 fold

Sales   Corporate   IT

Production

Sub $

Self elevation

Global Amin

UAA
User Access Admin

Owner

Role definition
json

Permission

Management

Actions: [*]
Not Actions :   [   ]

Data

Data Actions :   [ ]
Not Data Action : [ ]
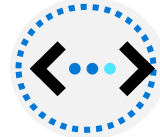
User Access Admin

Design for Azure subscriptions

Designing for multiple subscriptions

Azure subscription are logical containers for management and billing.

Align your subscriptions with business needs and priorities – consider billing and cost reporting

Consider administrative management – centralized or decentralized

Group subscriptions together under management groups – apply common policies and role assignments.

Consider subscription scale limits – specialized workloads, IoT, SAP

Consider a dedicated shared services subscription – common services everyone shares

Make subscription owners aware of their roles and responsibilities

When to use subscriptions - example

- Secure workloads that require additional policies and role-based access control to achieve compliance

- Specialized workloads and the need to scale outside the subscription limits

- Manage and track costs for your organizational structure

- Identify different environments such as development, test, and production that are often isolated from a management perspective
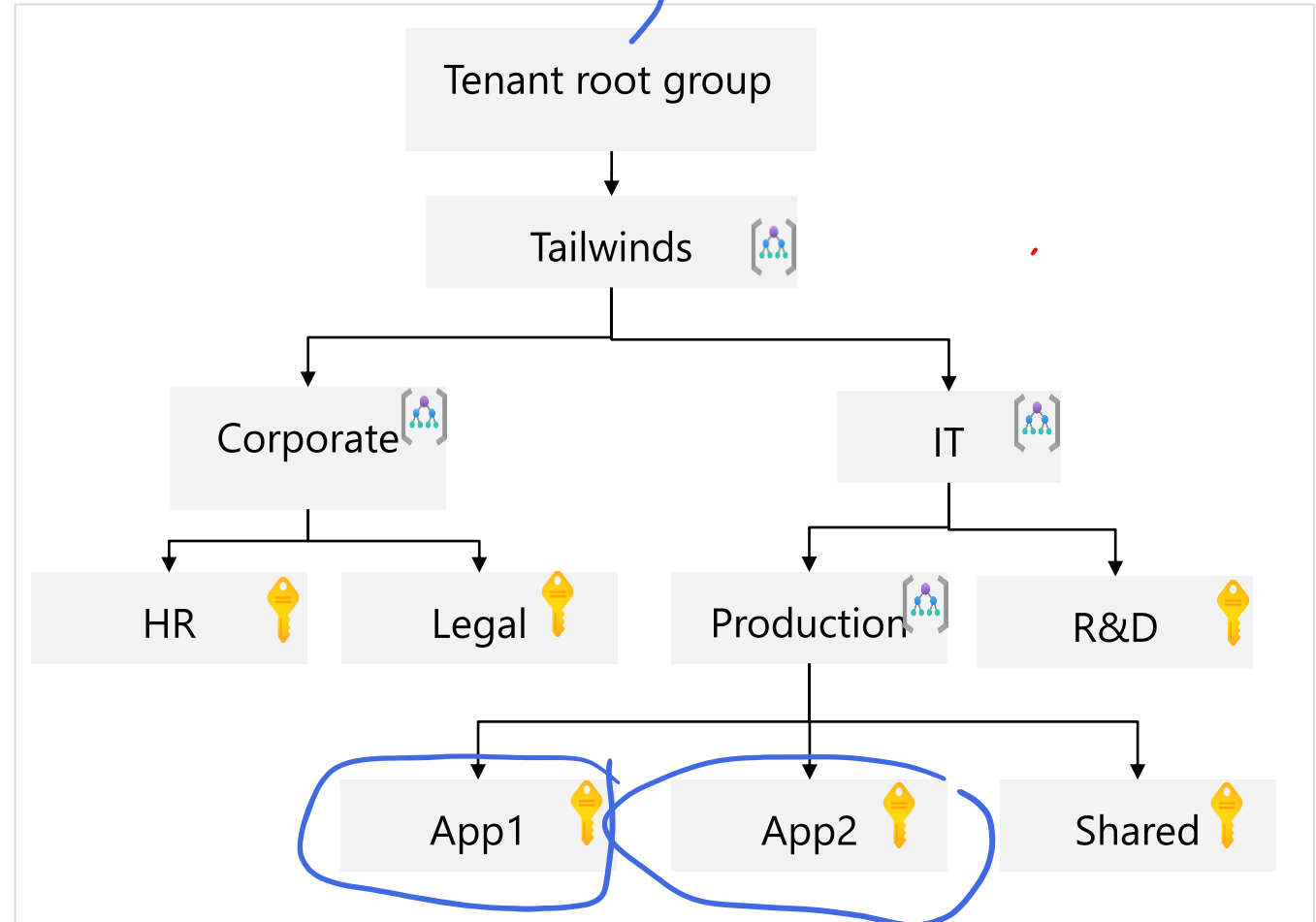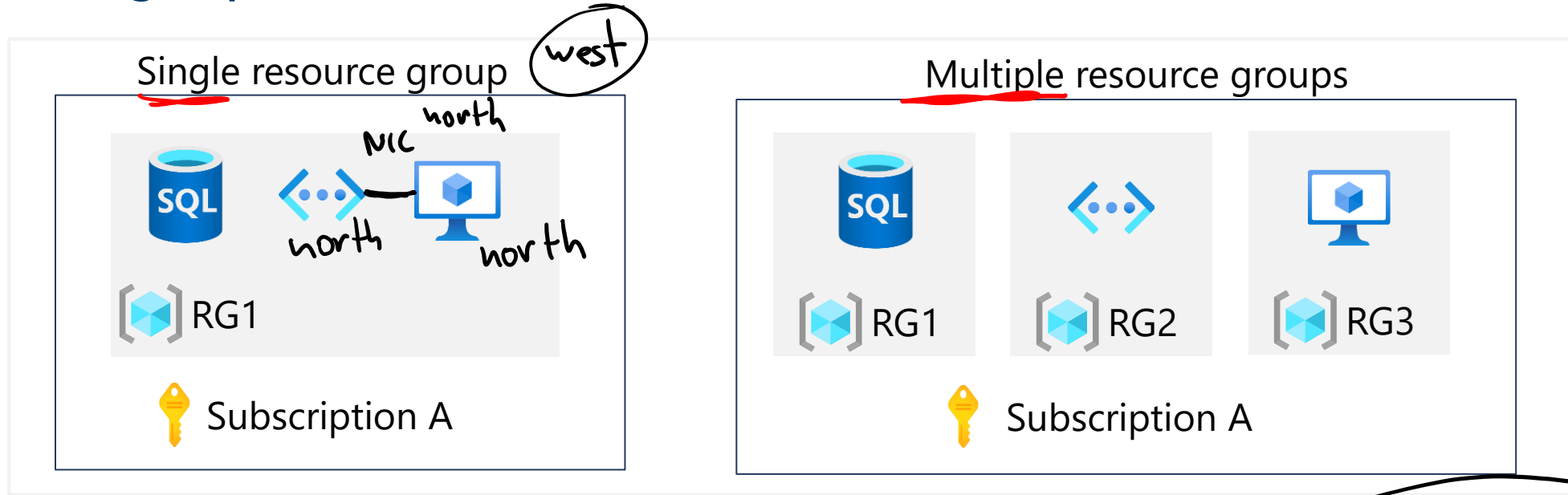
Design for resource groups
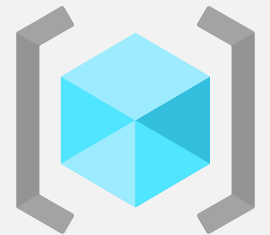
Plan your resource groups

A resource group is a container that holds related resources for an Azure solution.

Region = Location

Single resource group *(west)*

NIC north

SQL north

RG1

🔑 Subscription A

Multiple resource groups

SQL

`<...>`

RG1

RG2

RG3

🔑 Subscription A

RG = lifecycle

- Group resources that share the same life cycle
- Group by type, app, department, location, or billing
- Apply RBAC and policies to a group of resources
- Use resource locks to protect individual resources from deletion or change

RG 1

DB access

Cosmos conn String Token

RG 2

App
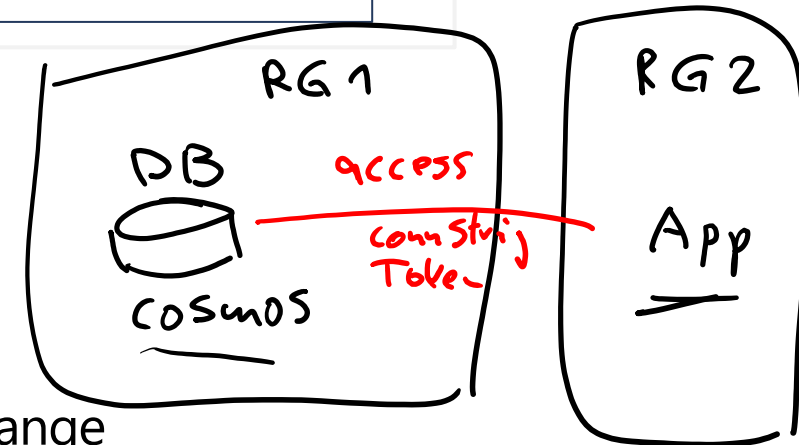
Design for resource tagging

Plan your resource tagging

Resource tagging can be business-aligned or IT-aligned
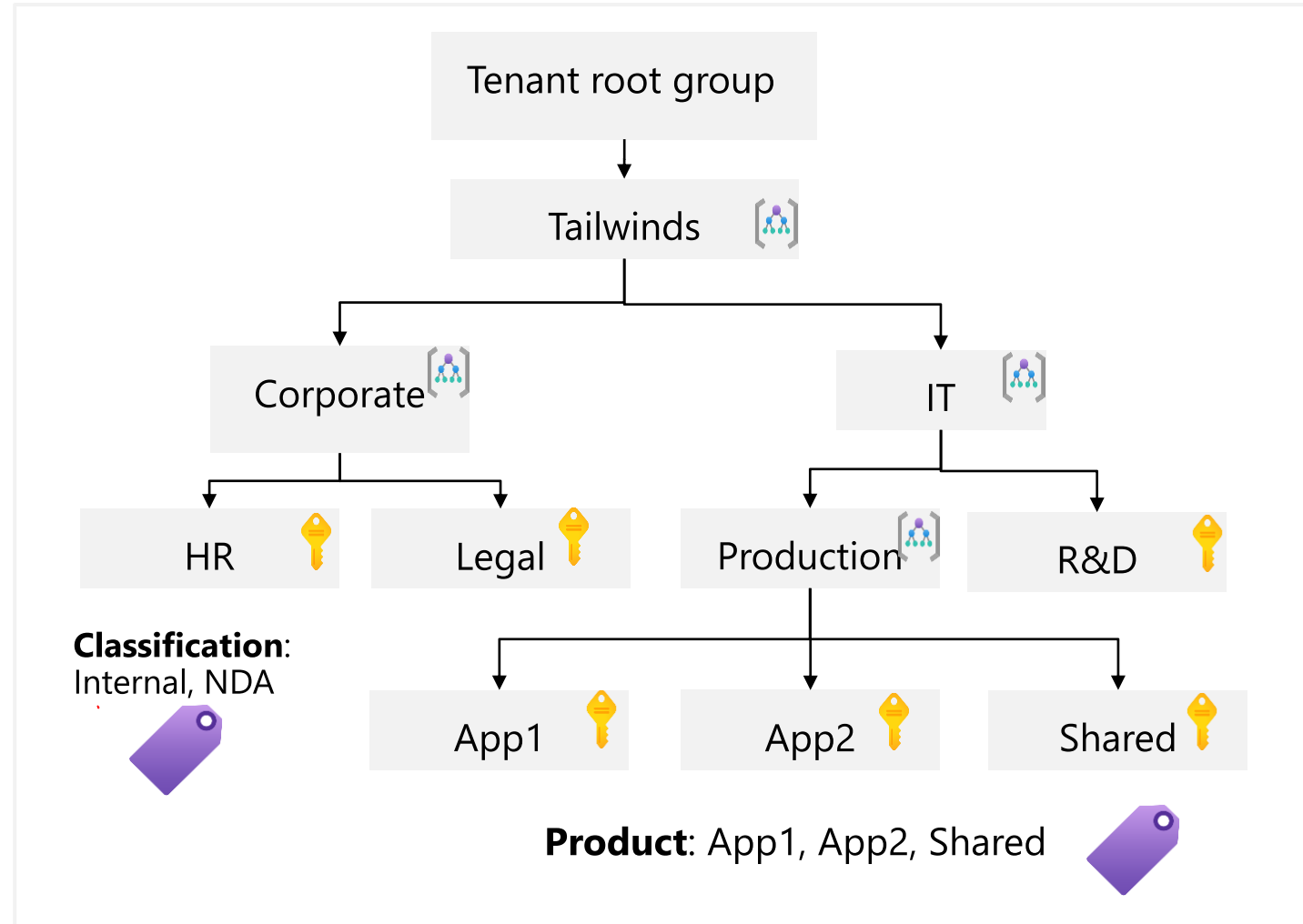
- Consider your organization's taxonomy

- Determine the reason for the tagging - functional, classification, accounting, partnership, or purpose

- Start with a few tags (mission-critical resources) and then scale out

- Policies could be used to apply tags and enforce tagging rules and conventions - mimic inheritance

Tenant root group

Tailwinds

Corporate

IT

HR

Legal

Production

R&D

Classification: Internal, NDA

App1

App2

Shared

Product: App1, App2, Shared

Design for Azure Policy and RBAC
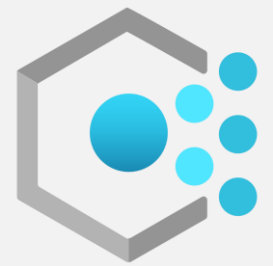
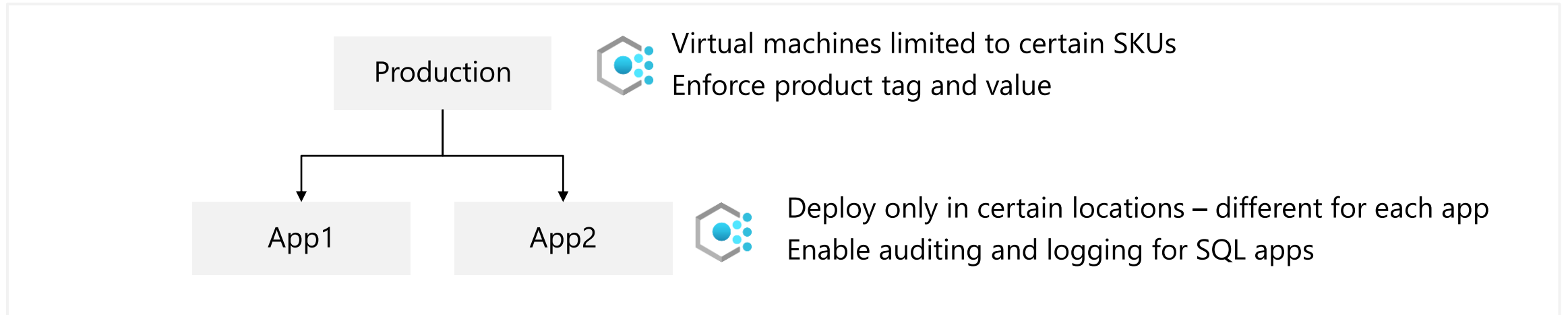# When to use Azure Policy

Azure Policy helps to enforce organizational standards and to assess compliance at-scale.

Production

Virtual machines limited to certain SKUs
Enforce product tag and value

App1   App2

Deploy only in certain locations – different for each app
Enable auditing and logging for SQL apps

- Large number of built-in policies and you can create custom policies

Examples

- Allow only certain virtual machines sizes for your project

- Ensure all resources are correctly tagged – if not, apply the tag

- Recommend system updates on your servers

- Enable multifactor authentication for all subscription accounts

Considerations for Azure Policy

- Apply policy at the highest scope possible

- Know when policies are evaluated

- Decide what to do if a resource is non-compliant

- Consider when to automatically remediate non-compliant resources

- Use the Azure policy compliance dashboard for auditing and review

- Effectively combine Azure policy with RBAC (next slide)

Developers

Operations

Built-in controls through policy instead of workflow
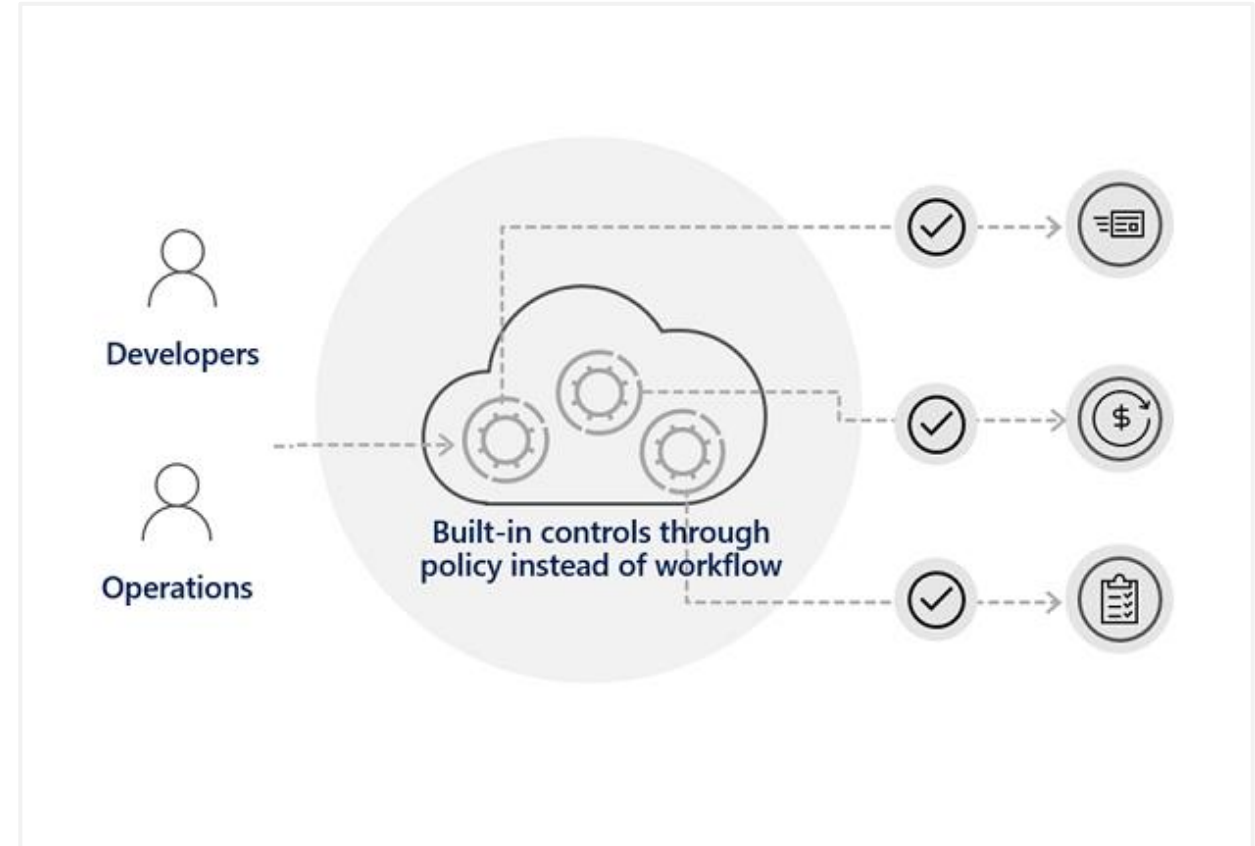
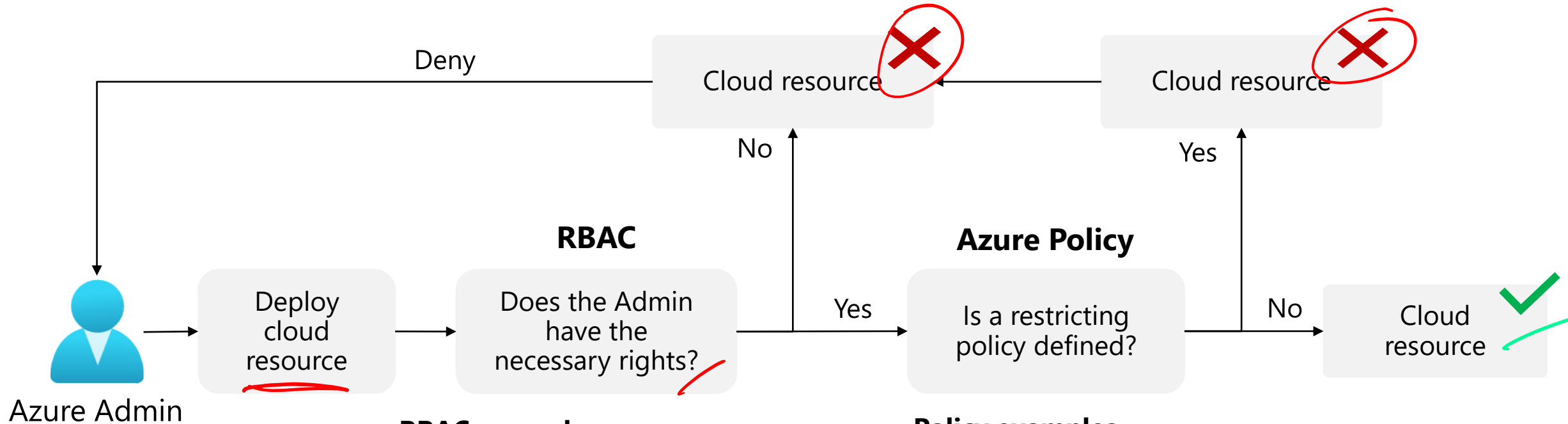# Design for Azure role-based access control (RBAC)
Azure RBAC allows you to grant access to Azure resources that you control.

- Only grant users the access they need

- Assign at the highest scope level that meets the requirements

- Assign roles to groups, not users

- Know when to create a custom role

- Consider what happens if you have overlapping role assignments

When to combine Azure Policy and Azure RBAC

Permission

Deny

Cloud resource ✗

Cloud resource ✗

No

Yes

RBAC

Azure Policy

Azure Admin

Deploy cloud resource

Does the Admin have the necessary rights?

Yes

Is a restricting policy defined?

No

Cloud resource ✓

RBAC examples
- Does the Admin have the right to deploy?
- Does the Admin have the right to deploy this resource type?
- Does the Admin have the right to deploy this resource group?

Policy examples
- Is the region restricted?
- Is the resource type restricted?
- Should a tag be applied?

V1
V2 □ □ □

RG(s)
Role "Reader"

ARM Template(s)

Policies "westeurope"

Design for Azure Blueprints

Bicep → ARM Templates (json)
Terraform

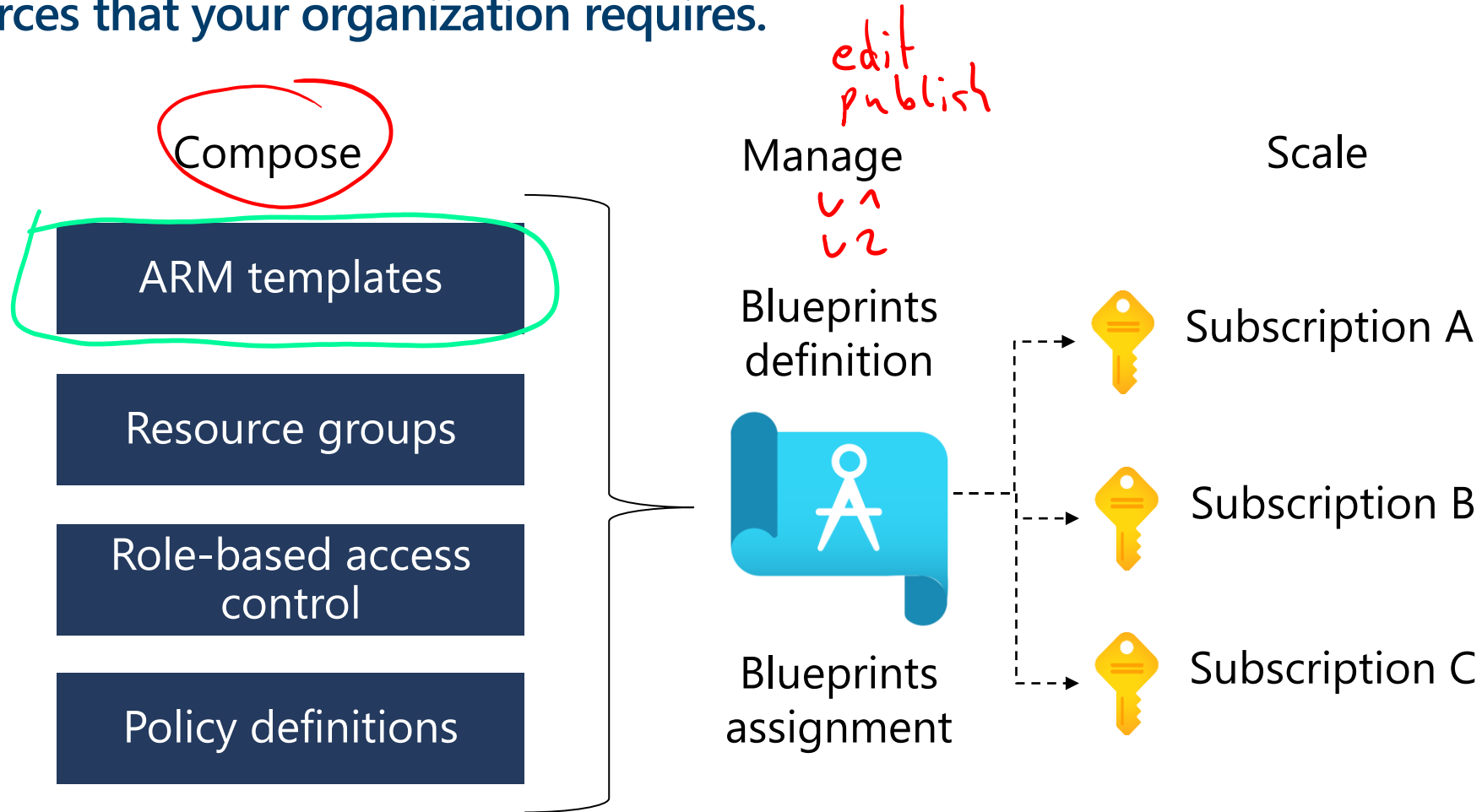# Design with Azure Blueprints

Azure Blueprints lets you define a repeatable set of governance tools and standard Azure resources that your organization requires.


Compose

ARM templates

Resource groups

Role-based access control

Policy definitions

edit
publish

Manage

Blueprints definition

Blueprints assignment

Scale

Subscription A

Subscription B

Subscription C

Design for Landing Zones

Implement Landing Zones

## A landing zone provides an infrastructure environment for hosting your workloads.

- Implements key foundational principles of governance, security, networking, management, and identity

- Pre-provisions the environment through code

- Good for both migrations and green field situations

- You can transition existing architectures

- Part of the Cloud Adoption Framework Ready phase
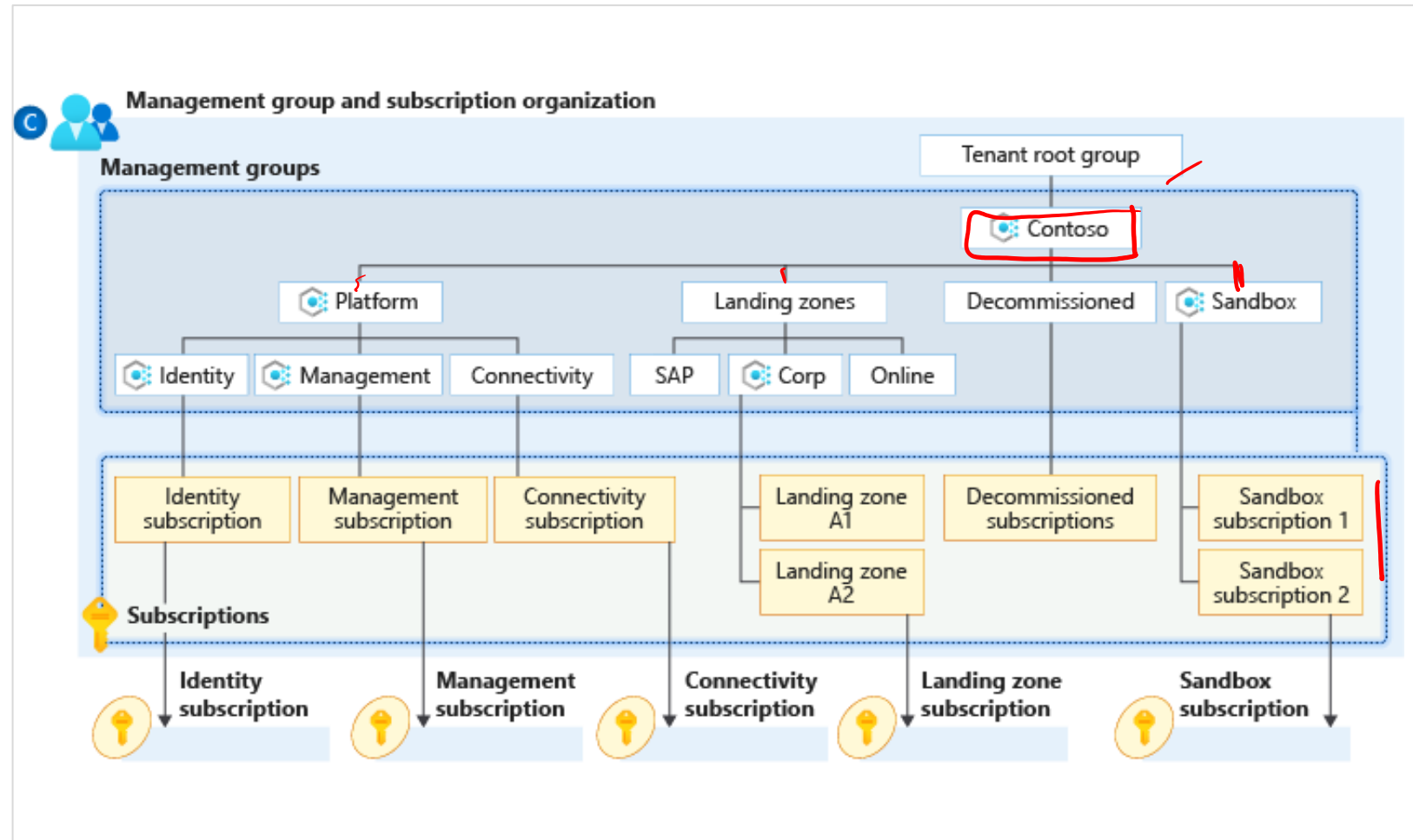
Case Studies and Review
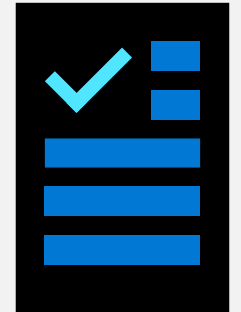
Case study – Cost and accounting

- Tailwind Traders has two main business units that handle Apparel, and Sporting Goods.

- Each of the business units consist of three departments: Product Development, Marketing, and Sales.

- Each business unit and subunit will be responsible for tracking their Azure spend.

- The Enterprise IT team will be responsible for providing company-wide Azure cost reporting.

- What are different ways Tailwind Traders could organize their subscriptions and management groups. Which would be the best to meet their requirements?

- Design two alternative hierarchies and explain your decision-making process.

Case study – New development project

- The company has a new development project for customer feedback.

- The CFO wants to ensure all costs associated with the project are captured.

- For the testing phase workloads should be hosted on lower cost virtual machines.

- The virtual machines should be named to indicate they are part of the project.

- Any instances of non-compliance with resource consistency rules should be automatically identified.

- What are the different way Tailwind Traders could track costs for the new development project?

- How are you ensuring compliance with the requirements for virtual machine sizing and naming?

- Propose at least two ways of meeting the requirements. Explain your final decision.

Summary and resources

Check your knowledge	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Control and organize Azure resources with Azure Resource Manager
	Describe core Azure architectural components
	Build a cloud governance strategy on Azure
	Introduction to enterprise-scale landing zones in the Microsoft Cloud Adoption Framework for Azure
	Choose the best Azure landing zone to support your requirements for cloud operations

Optional hands-on exercise - List access using Azure RBAC and the Azure portal

End of presentation