

AZ-305

Designing Microsoft Azure Infrastructure Solutions



AZ-305 Agenda

- Module 01 Design a governance solution ←
- Module 02 Design a compute solution
- Module 03 Design a non-relational data storage solution
- Module 04 Design a data storage solution for relational data
- Module 05 Design a data integration solution
- Module 06 Design an application architecture solution
- Module 07 Design Authentication and Authorization Solutions
- Module 08 Design a solution to log and monitor Azure resources
- Module 09 Design a network infrastructure solution
- Module 10 Design a business continuity solution
- Module 11 Design a migration solution

Seit 2011
~~ARM~~
(Classic)

- Organisation
Regeln
Vorschriften

Seit 2013

- Extern
Normen

ARM Azure Resource Manager



RBAC

Owner
Contributor
Reader

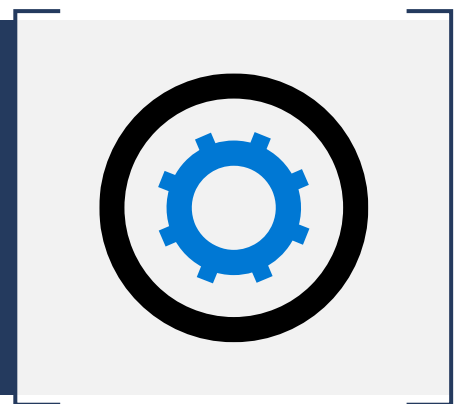
Policy

Allowed Location Deny

Resource Hierarchy

- Scope
- Management Group
 - Subscription
 - Resource Group
 - Resource

Design a governance solution



json ← Bicep Lang (terraform)

Azure Blue Prints
Resource as Code → ARM
Policies → json
Permissions → json

CAF Landing Zone
Cloud Adoption Framework

⇒ - - RG

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

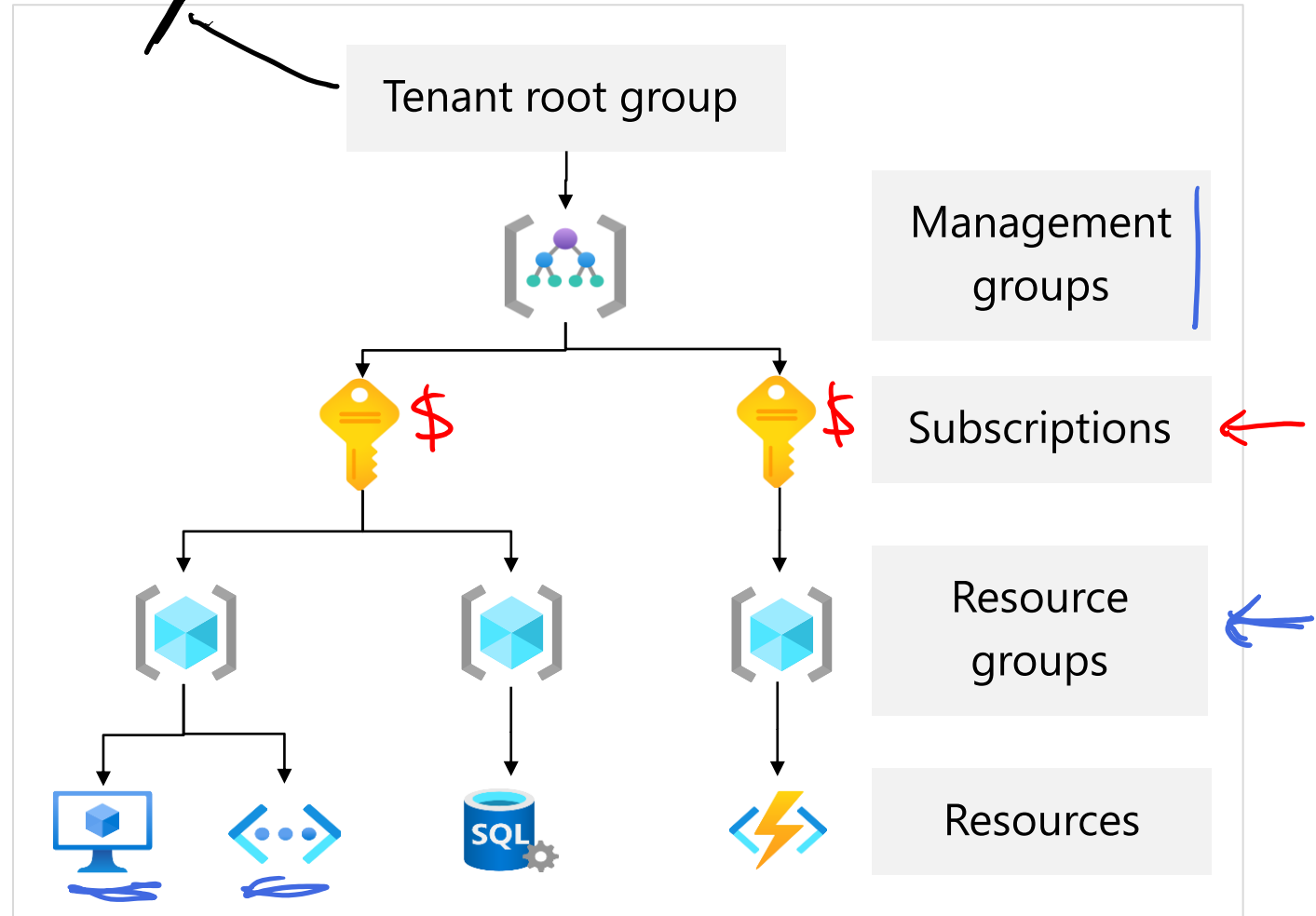


Govern resources in Azure

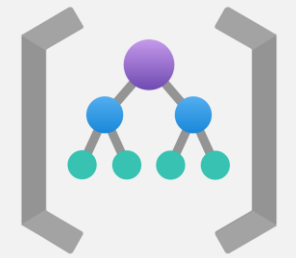
Governance provides mechanisms and processes to maintain control over your applications and resources in Azure.

- Determine your requirements, plan your initiatives, and set strategic priorities
- Plan for governance at every level
 - Management groups
 - Subscriptions
 - Resource groups
 - Resources

ARM



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 **CAF**

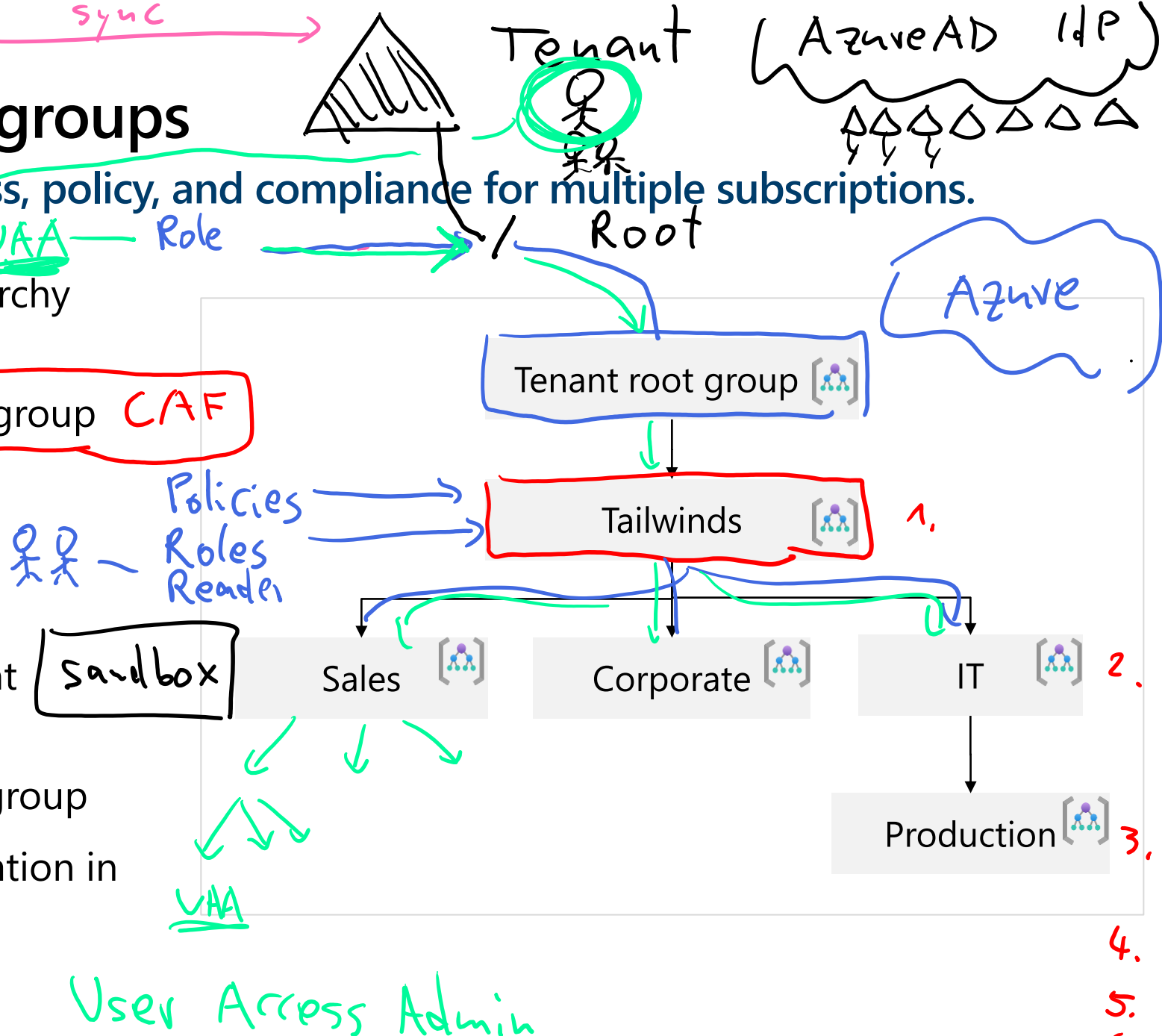
- Consider an organizational or departmental structure

- Consider a geographical structure

- Consider a production management group

- Consider a sandbox management group

- Consider isolating sensitive information in a separate management group


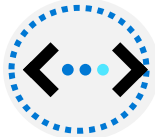






Design for Azure subscriptions



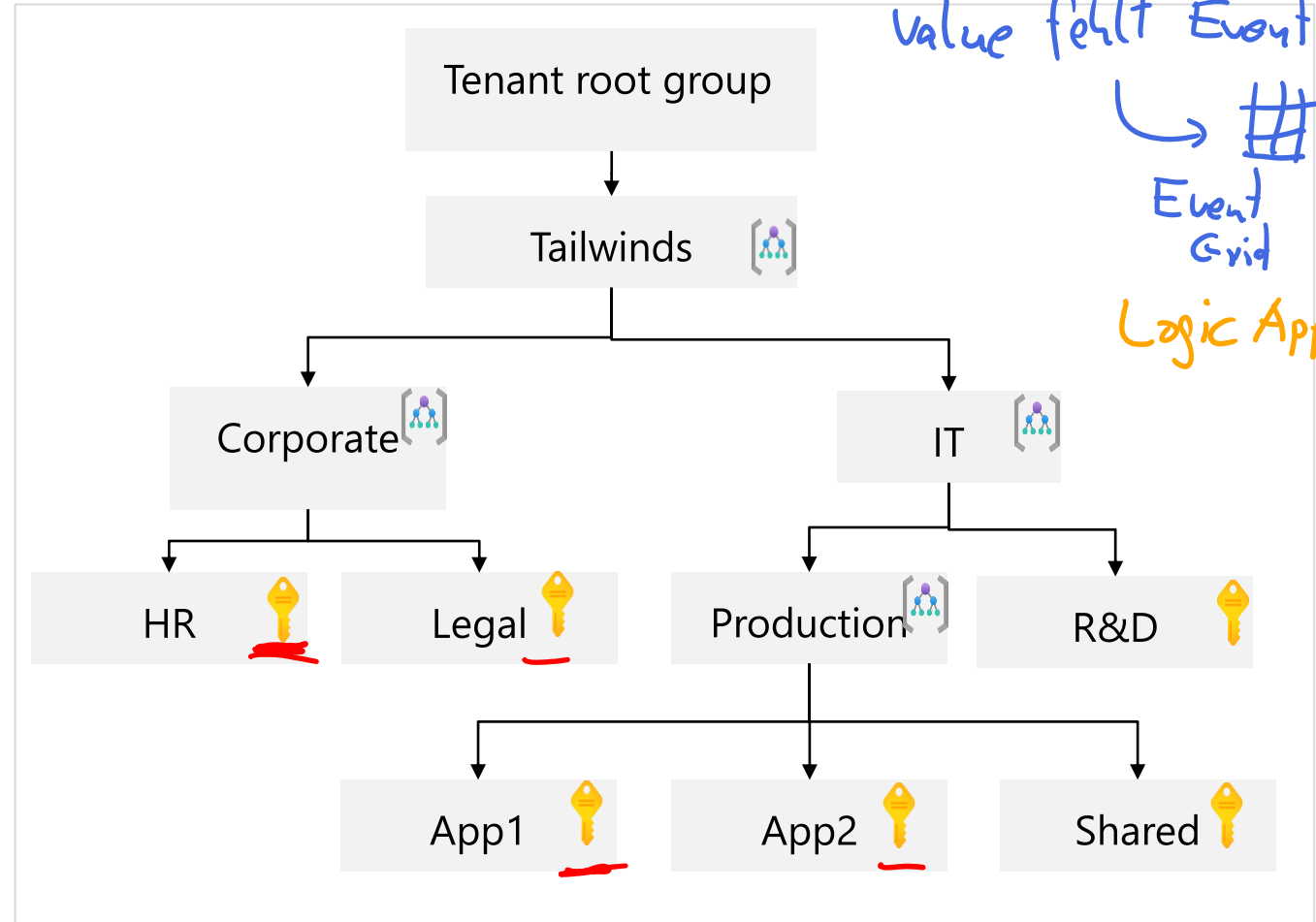
Designing for multiple subscriptions

Azure subscription are logical containers for management and billing.

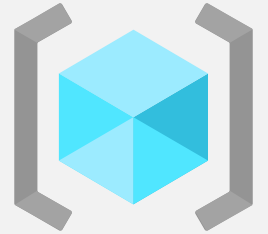
-  Align your subscriptions with business needs and priorities – consider billing and cost reporting
-  Consider subscription scale limits – specialized workloads, IoT, SAP
-  Consider administrative management – centralized or decentralized
-  Consider a dedicated shared services subscription – common services everyone shares
-  Group subscriptions together under management groups – apply common policies and role assignments.
-  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



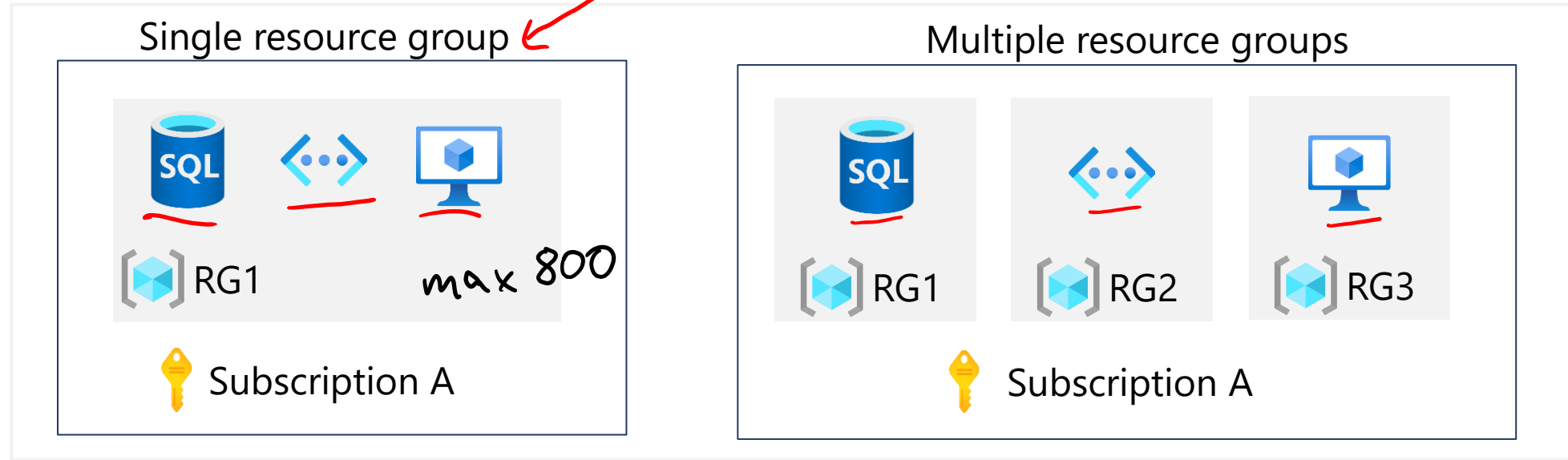
flat

Bicep → ARM Template json

Terraform
IaCode

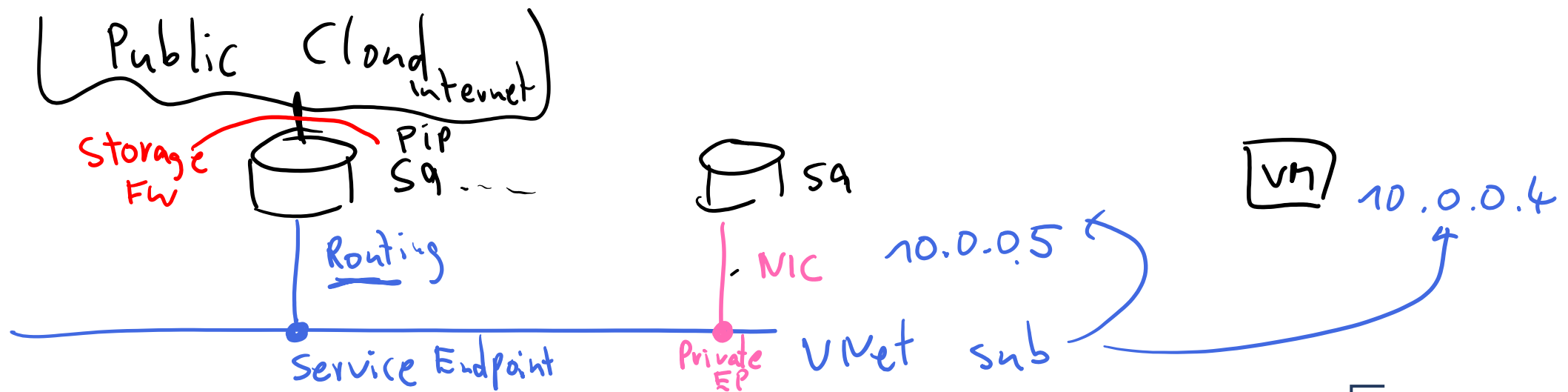
Plan your resource groups

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



- 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

CAF



Design for resource tagging

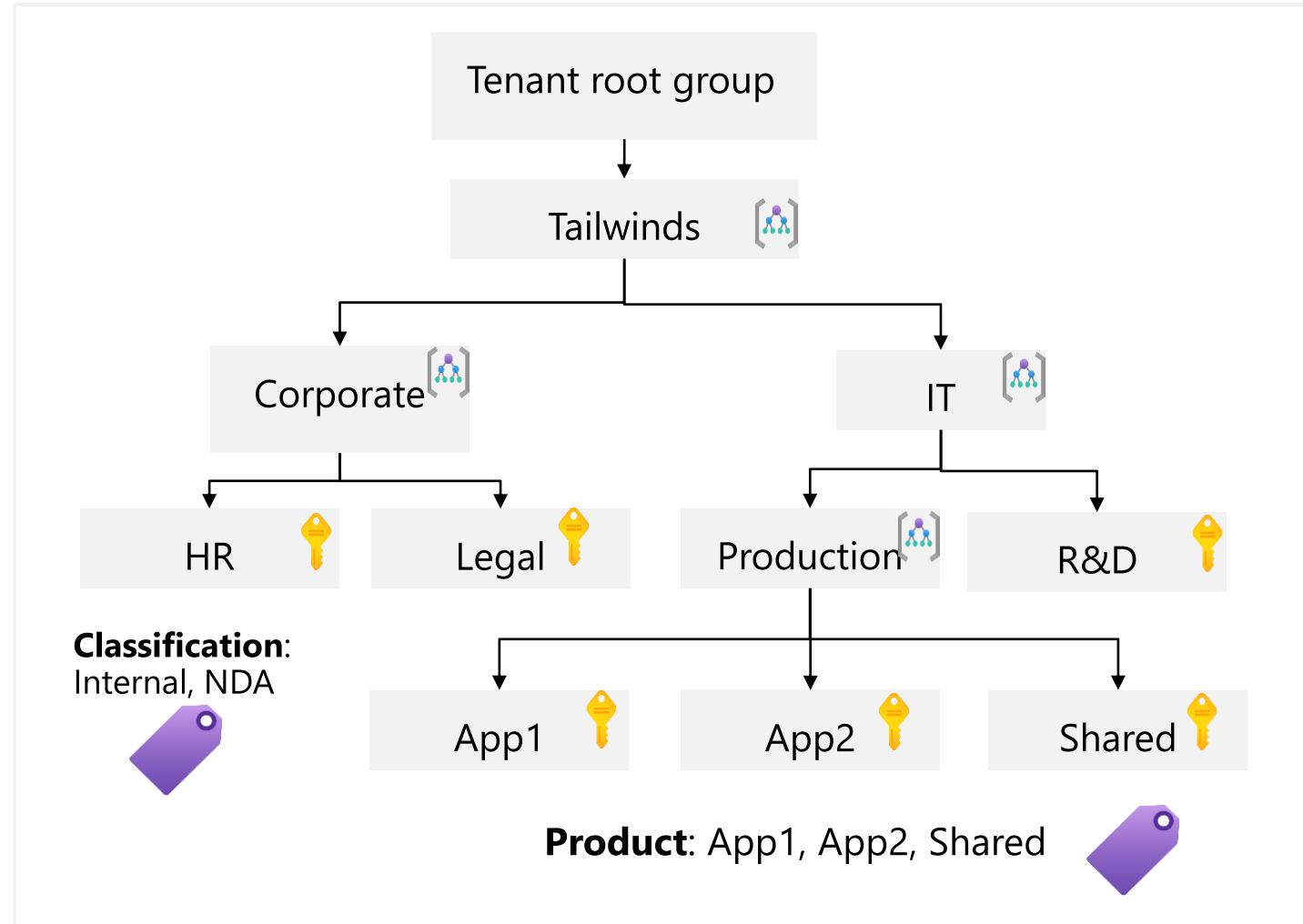


Nomenklatur
Policy mit Regex

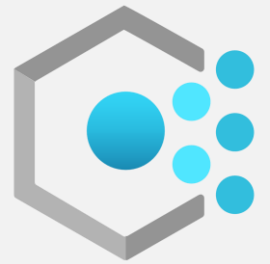
Plan your resource tagging

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



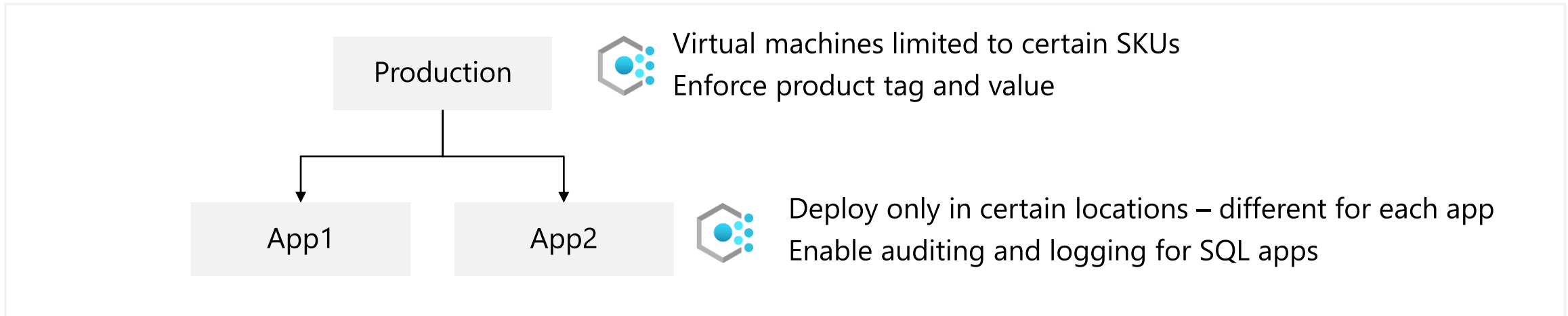
Design for Azure Policy and RBAC



When to use Azure Policy

json

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



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

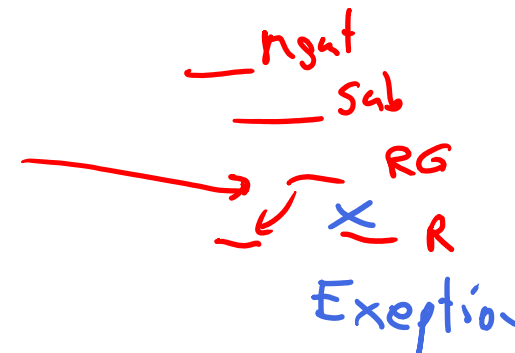
Examples

- 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 ✓

Regions

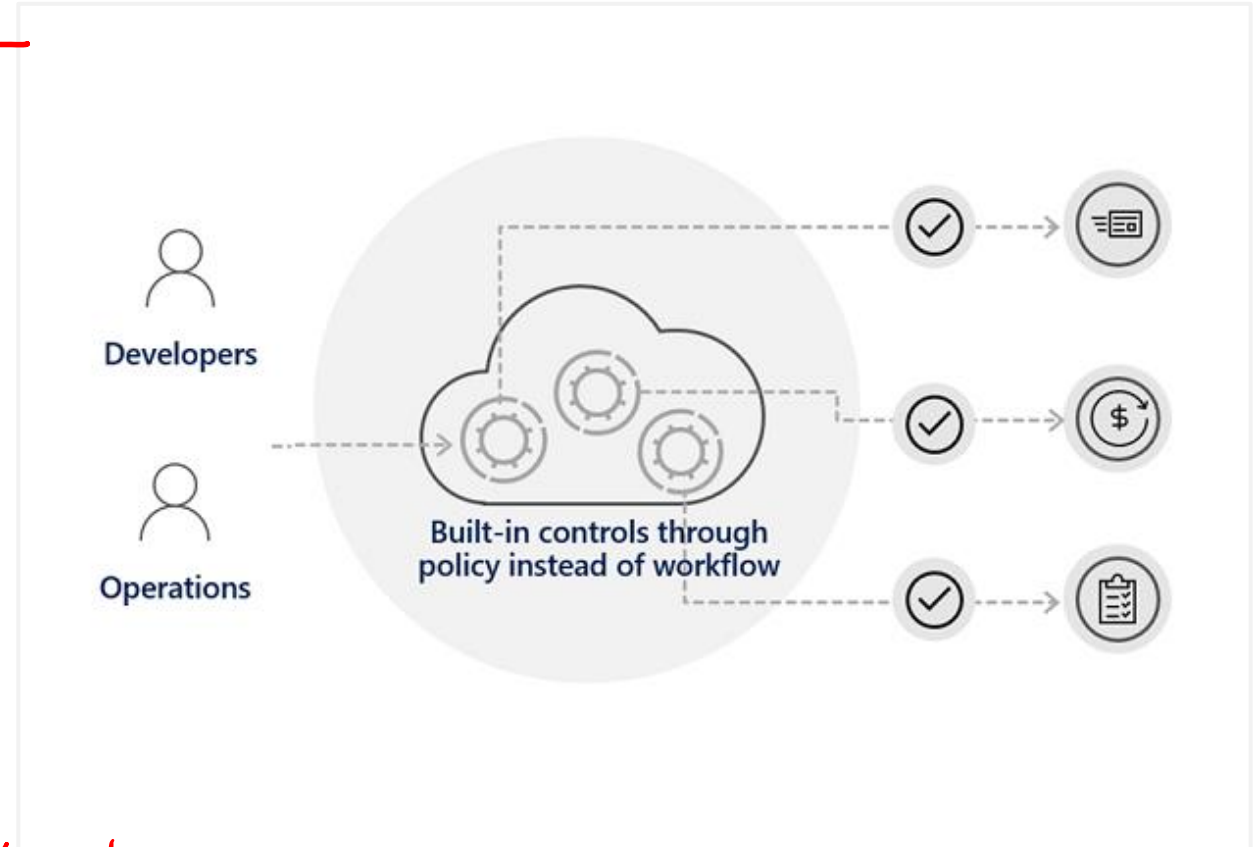
SKU

CA



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)







Defender for Cloud

ASC...

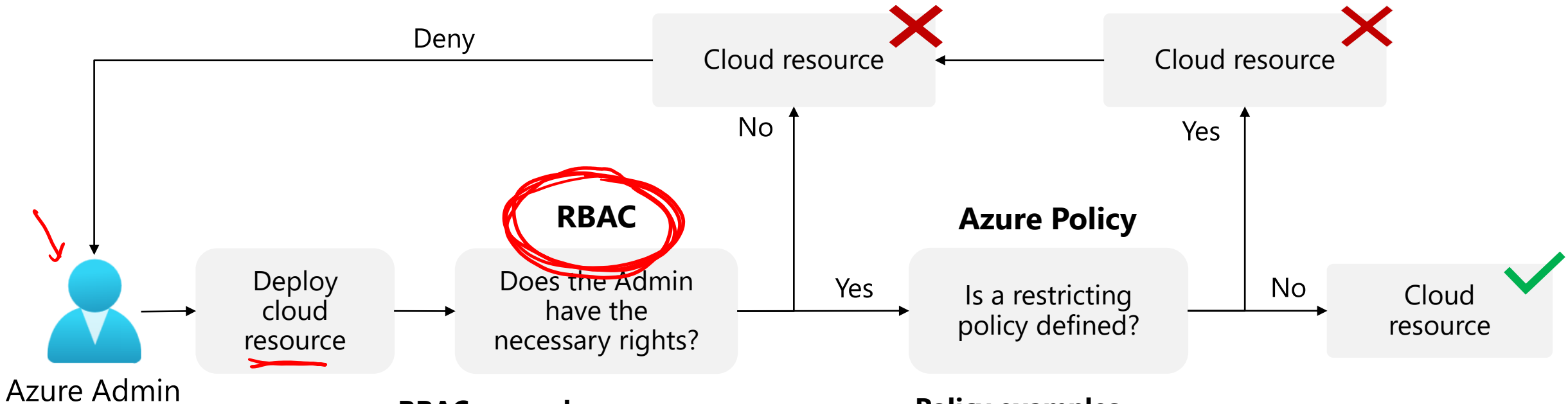
Design for Azure role-based access control (RBAC)

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

	Role				
	Reader	Resource-specific	Custom	Contributor	Owner
 Management group	Observers Auditors Reviewers	Helpdesk personnel Developers Users managing resources			Admins
 Subscription					
 Resource group					
 Resource	Automated processes				

When to combine Azure Policy and Azure RBAC

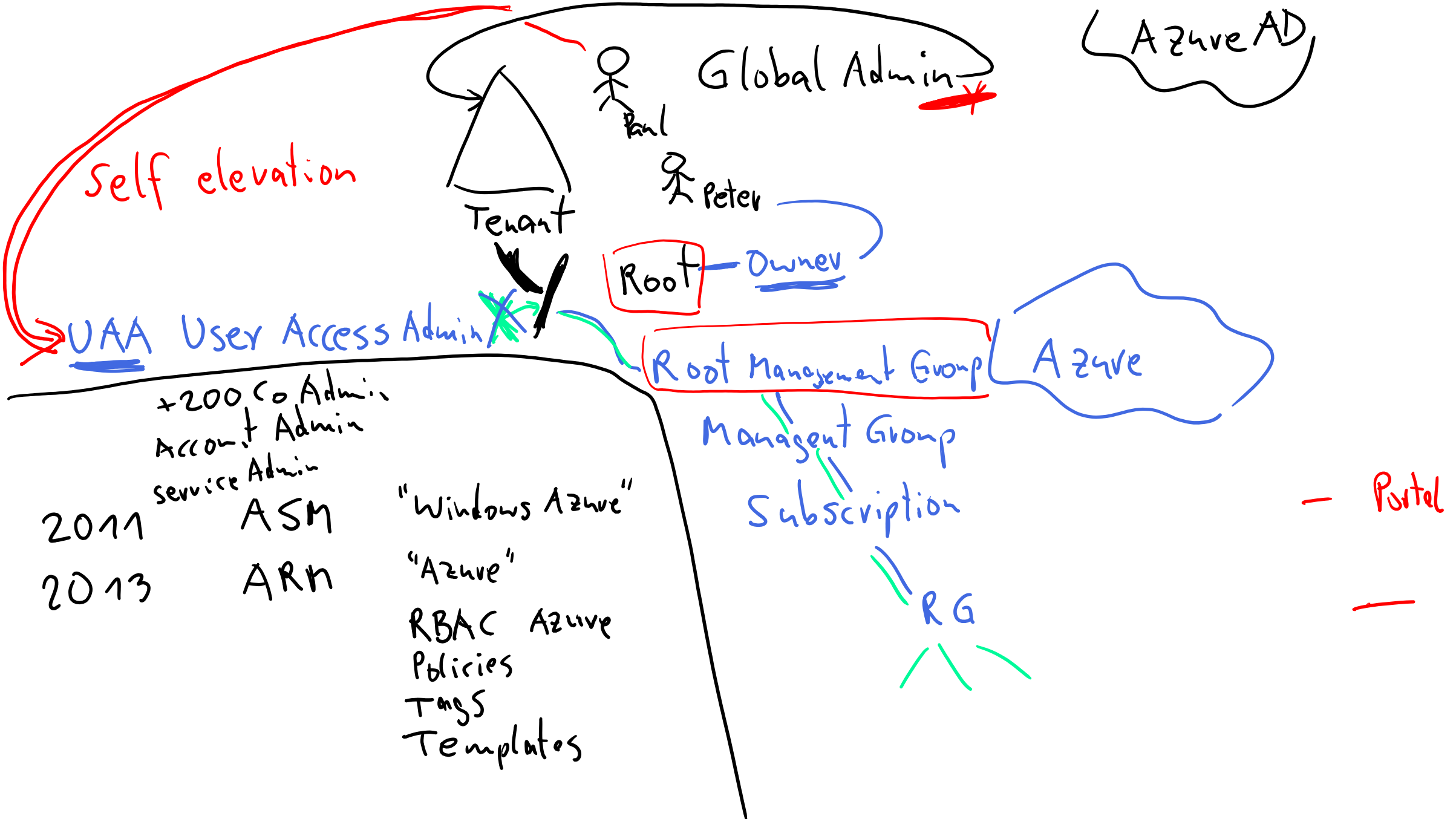


RBAC examples

- 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?

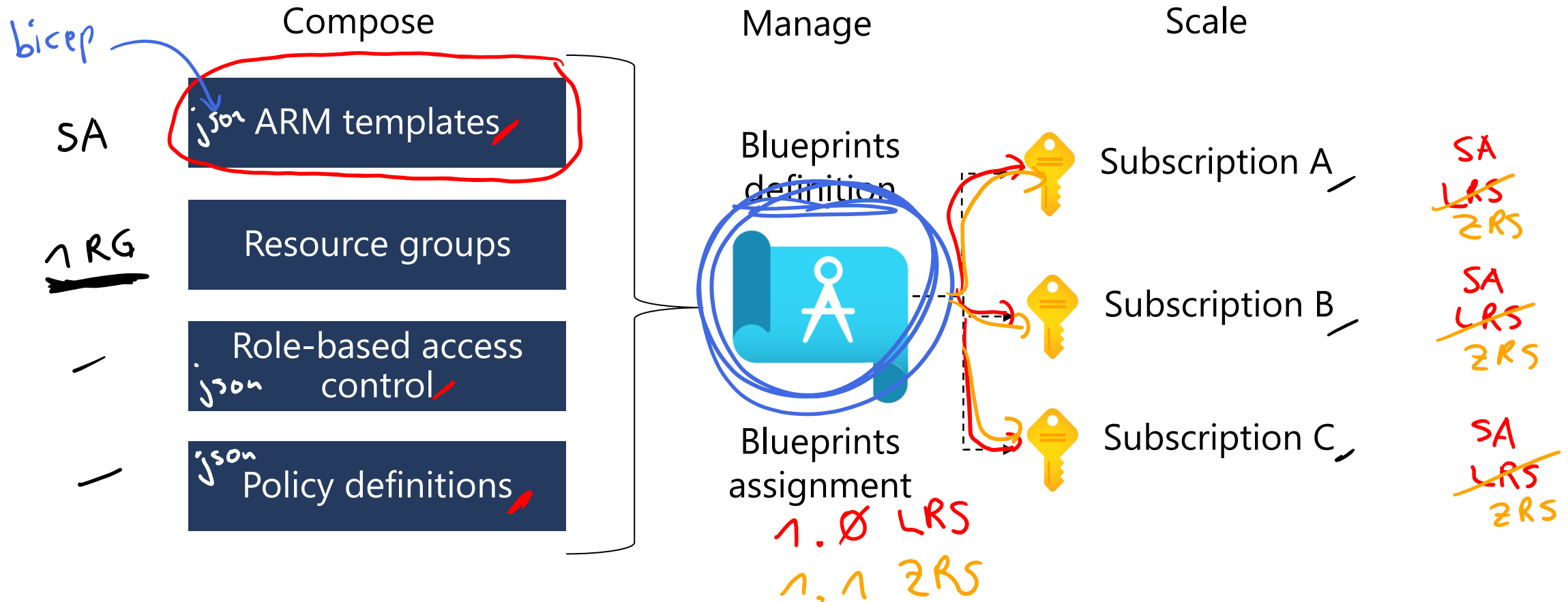


Design for Azure Blueprints



Design with Azure Blueprints

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



CAF

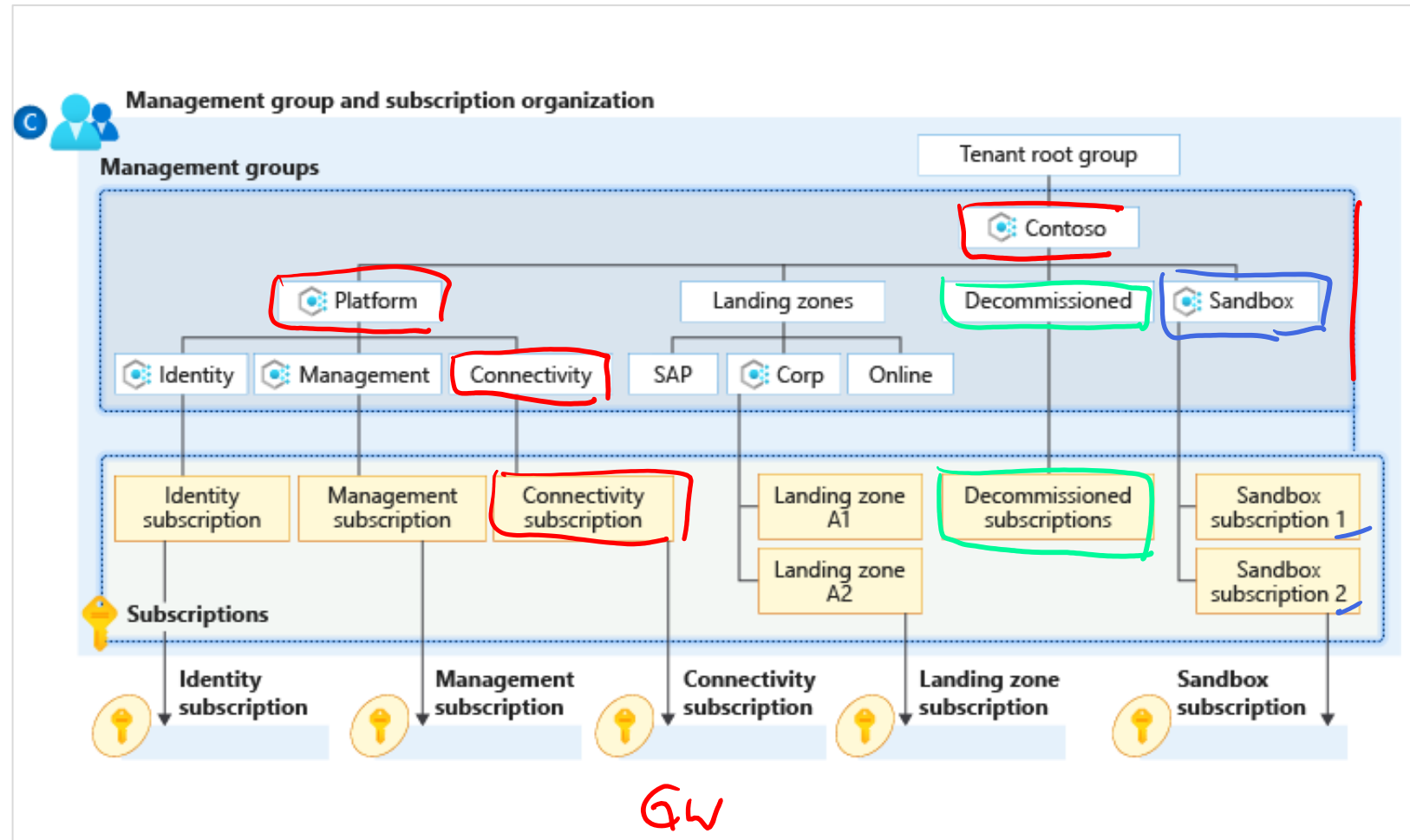
Design for Landing Zones



Implement Landing Zones

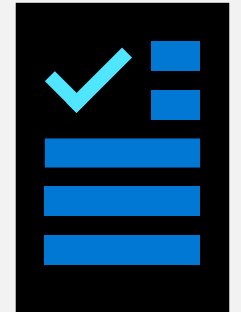
A landing zone provides an infrastructure environment for hosting your workloads.

- 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



GW
Hub-Spoke

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

