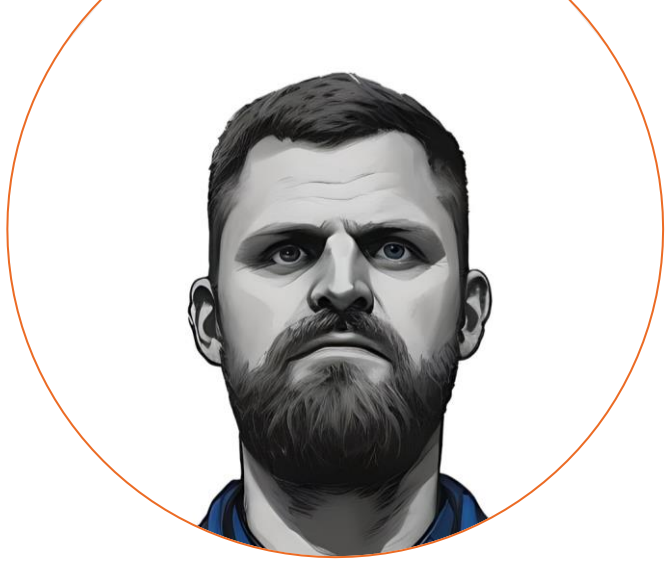
Stefan Rapp

Cloud Solution Architect (CSA)

Azure “Landing Zone” Series 1

Why Governance is essential to provide reliable cloud workloads on Azure.

PROFILE – STEFAN RAPP



Cloud Solution Architect (CSA)

Let's engage: LinkedIn

#AzureRocks 🤘 🧑‍🏭

Mail: info@blog.misterazure.com

LinkedIn: https://www.linkedin.com/in/rapster83

Specializations: *(MS Consultant since 2008)*

- Identity & Access Management (IAM)
- Microsoft Infrastructure
- Azure Governance
- Azure Infrastructure
- Cloud Automation – IaC (with Terraform)
- Cloud Migrations
- Application Modernization

AGENDA

What to expect during this **Series I** (Azure Governance)?

- Introduction
- Azure Governance
- Azure Billing
- Azure Hierarchy
- Naming Convention
- Tag & Lock Strategy
- Azure RBAC
- Azure Policies
- Azure Cost Management
- Wrap up / Summary

INTRODUCTION

Status quo in an organization regarding Azure Governance?

BAD AZURE GOVERNANCE IMPLEMENTATION

Why should your Azure Governance NOT look like this? ☹

Source: https://unsplash.com/photos/GoHaYpu7-ks

SUCCESSFUL AZURE GOVERNANCE IMPLEMENTATION

But more like this. 👍

Source: https://unsplash.com/photos/OHOU-5UVIYQ

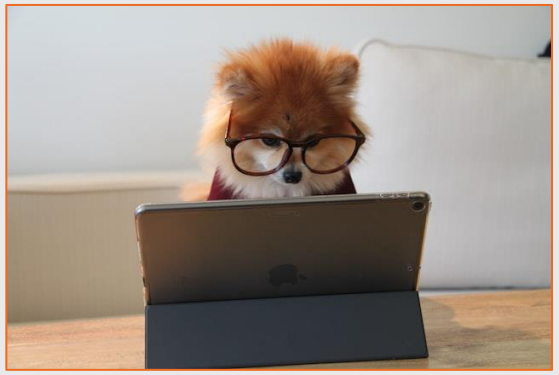
AZURE GOVERNANCE

Which disciplines are important regarding Azure Governance as design area? ⚖️

GOVERNANCE

Why a **governance concept** needed on a cloud platform like **Microsoft Azure**?

- In Azure **easy** to create, read, update, and delete resources
- **Unrestricted** resource access for developers in Azure
  „Let‘s try this fancy Azure feature out“
- **Rapid** creation of resources
- Azure resource often <u>not</u> properly **configured**.
- Leads to unintended **cost** consequences. → $ 💸 $ 💰 → 😱
- **Inefficient** cloud resource usage, security issues & access costs.



Source: https://unsplash.com/photos/gySMaocSdqs

<u>Resource Access Governance:</u>
Managing, monitoring, and auditing the use of Azure resources
to meet the **goals** <u>and</u> **requirements**.

WHY CLOUD GOVERNANCE

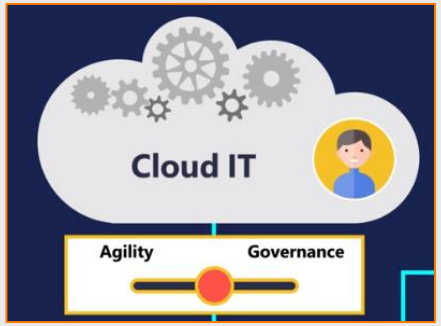
Governance with the Microsoft Cloud Adoption Framework (CAF) for Azure

- What is the challenge? Why does an organization need governance?
- Example: What is the most expensive VM per month in Azure?

Instance	vCPU(s)	RAM	Temporary storage	Pay as you go
M208s v2	208	2,850 GiB	4,096 GiB	€26,577.3681/month
M208ms v2	208	5,700 GiB	4,096 GiB	€46,157.1507/month
M416s v2	416	5,700 GiB	8,192 GiB	€57,507.7493/month
M416ms v2	416	11,400 GiB	8,192 GiB	€101,007.1633/month

Source: https://unsplash.com/photos/npxXWgQ33ZQ

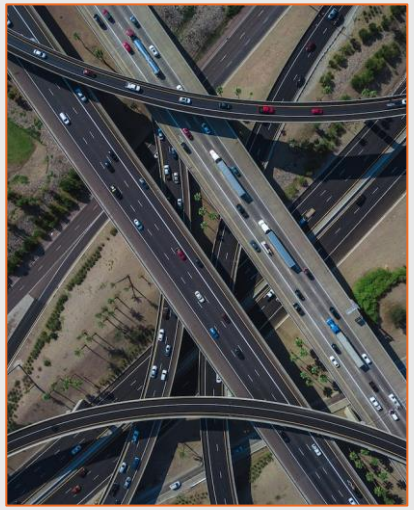
Source: https://unsplash.com/photos/blOLCO2K4M0



- Finding the right **balance** is a big challenge.
- Implementation of a **governance framework** on the Azure Tenant.
- Development of strategies for the **growth** of cloud use cases (“enterprise scale”)

AZURE GOVERNANCE TOPICS

Which **aspects** must be considered regarding Azure Governance?



Source: https://unsplash.com/photos/NSuufgf-BME

Source: https://unsplash.com/photos/Bas44VLlYlA

Important:
Making decisions depend on the organization's governance **needs** and **requirements**!

AZURE GOVERNANCE

What is the definition of **Azure** Governance?

Azure Governance:

*"Azure governance is a **combination** of different Azure **services** and **capabilities**, allowing for the management of all your Azure resources **at scale** and following control guidelines. Azure governance works across **multiple subscriptions** and across **resource groups**, and is based on a combination of Azure **identity**, Role-Based Access Control (**RBAC**), Azure **policies**, and **management groups**. [...] Some customers also consider **cost control** as part of governance processes and best practices. If your organization has a **Security Operations Center** (SOC), this department will most probably take **ownership** of this process, or at least (should) be hugely **involved** in this."*

Source: *Azure Strategy and Implementation Guide – 3rd Edition*

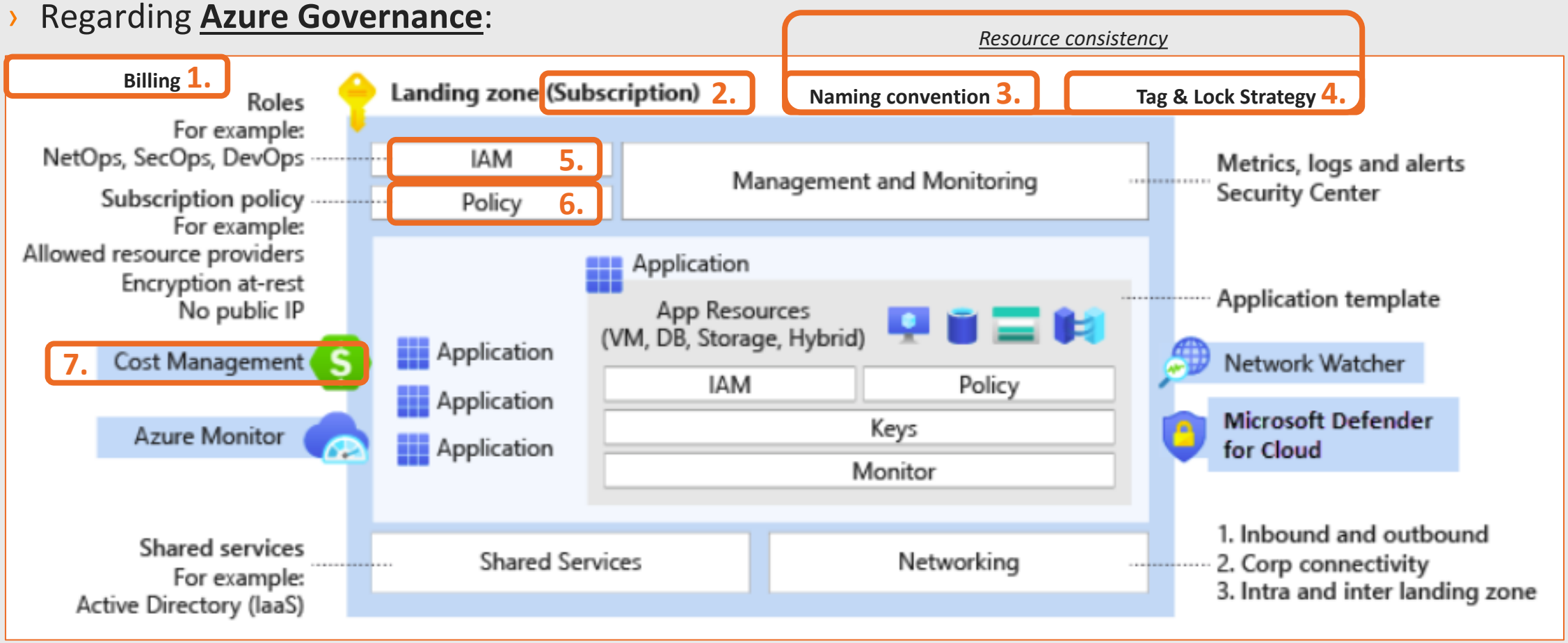
Cloud security framework

Enforcement of the overall security strategy in Azure!

DESIGN AREAS – OVERVIEW

Which design areas must be covered to provide a proper Azure landing zone for an enterprise?

› Regarding **Azure Governance**:



Source: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/governance

1. AZURE BILLING

AZURE BILLING

How Azure Billing can be related to the Azure Tenant(s)?

Azure Billing:
Provides all the tools you need to manage your billing account and pay invoices.

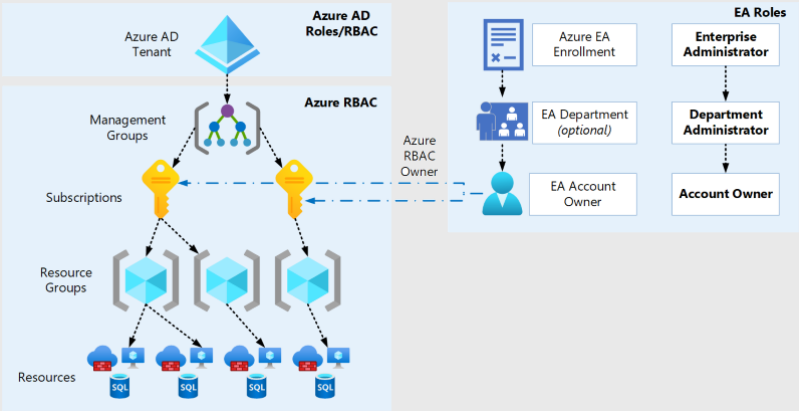
Azure Cost Management:
Set of FinOps tools that enable you to analyze, manage, and optimize your costs.

- Check the Azure Subscription **Offers** → Link
- Offers can be used at the same **time**. That give you flexible billing options!
- Azure "*Landing Zone*" architecture supports subscriptions from any Azure offer!
- **1 Subscription** can only exist within **1 Azure Tenant** (relocation/transfer is possible) – Link
- Place it in the Management Group (MG) **hierarchy** within the Azure tenant.

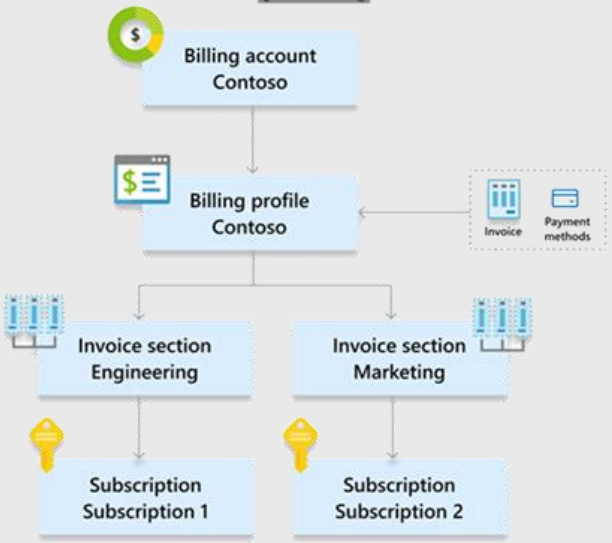
AZURE BILLING MODELS

Where to get the Azure subscription from as a Microsoft customer?

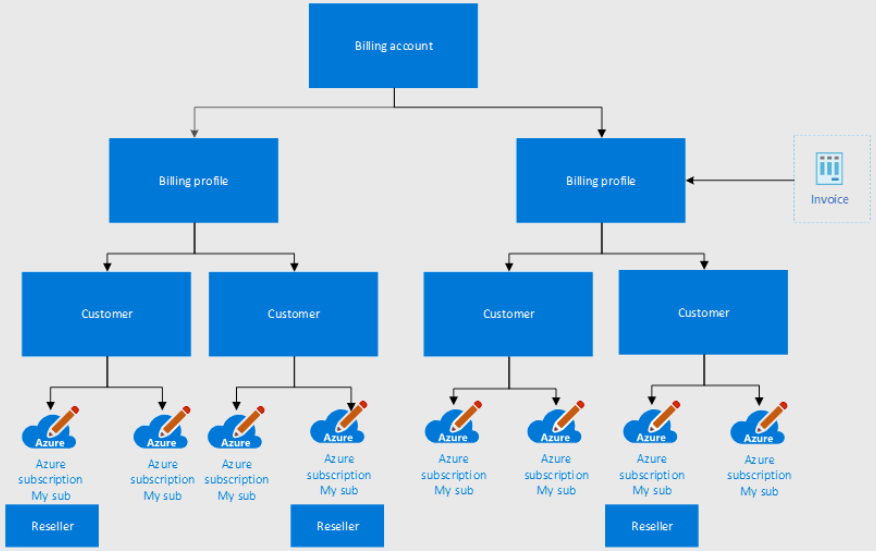
› Enterprise Agreement (EA)



› Microsoft Customer Agreement (MCA)



› Cloud Service Provider (CSP)



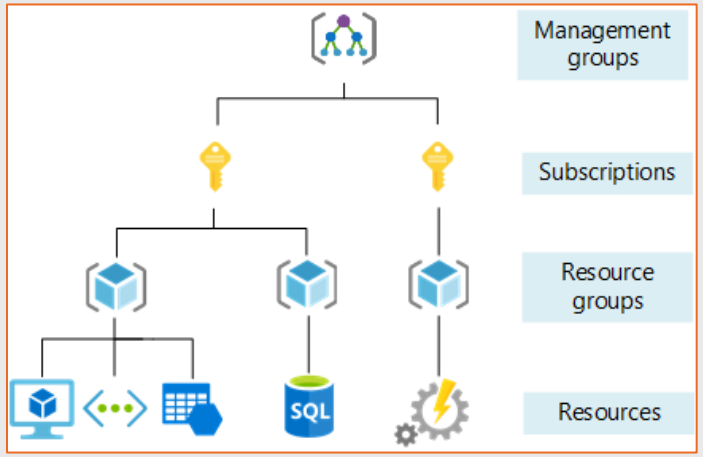
Source: Microsoft Docs

2. AZURE HIERARCHY

AZURE HIERARCHY

Organize your resources in Azure the right way from the beginning.

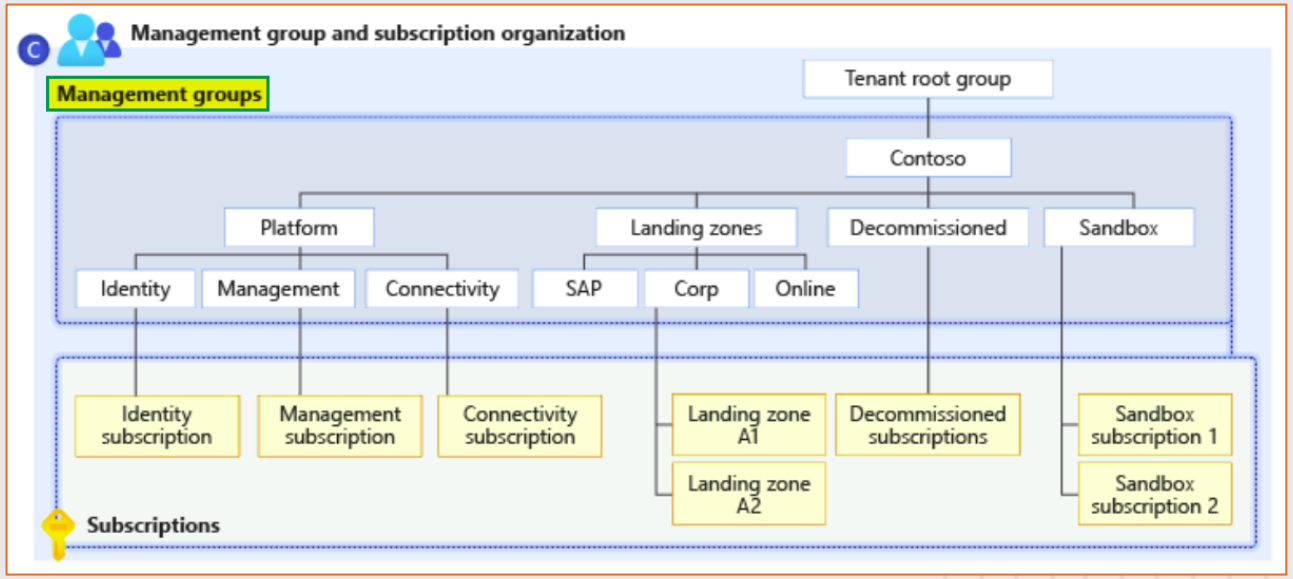
- Resource organization is **essential/critical**.
- Avoid creating scaling constraints on the **Azure Tenant** later.
- Establish consistent **patterns/topologies** for resource organization (basis):
  - Management Group (MG) design
  - Subscription design
  - Naming Convention
  - Tagging
- Alignment with the "*Landing Zone*" conceptual **architecture**
- Supports **separation/segregation** of duties (permissions)
- Approach: "*Think big, start small*" (grow over time, but scale quickly)
- Keep environment **growth** and **changes** of business organizations in mind ("*enterprise scale*")
- Key: Simplify management across the environment



AZURE MANAGEMENT GROUPS

Which aspects to consider architecting Azure hierarchy with MGs

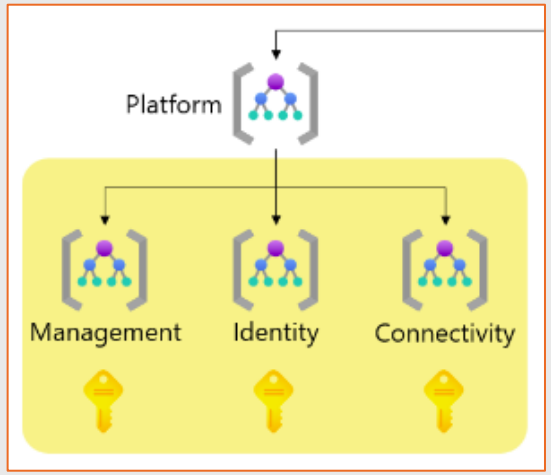
- Use MGs to structure the cloud environment on the Azure Tenant
- The MG structure must **support** "*organizational*" mapping of the enterprise
- The "*Tenant Root Group*" (TRG) is built-in. Maximum of **6 levels** of depth (without the TRG)
- A **new** subscription will be placed under the TRG by **default**
- Keep it flat. Not more than 3-4 levels
- Used for **cost management**, **policies** & **IAM**
- Same **security**, **compliance**, **connectivity**, etc.
- Group **type** of workloads (isolation)
- Avoid **policies** or **permissions** on the TRG
- Protect MGs with **Azure RBAC**
- Do <u>NOT</u> do **Stages** (DEV, TEST, PROD) as MGs



AZURE SUBSCRIPTIONS

Use subscription as a democratized **unit of management** aligned with the business **needs** and **priorities**.

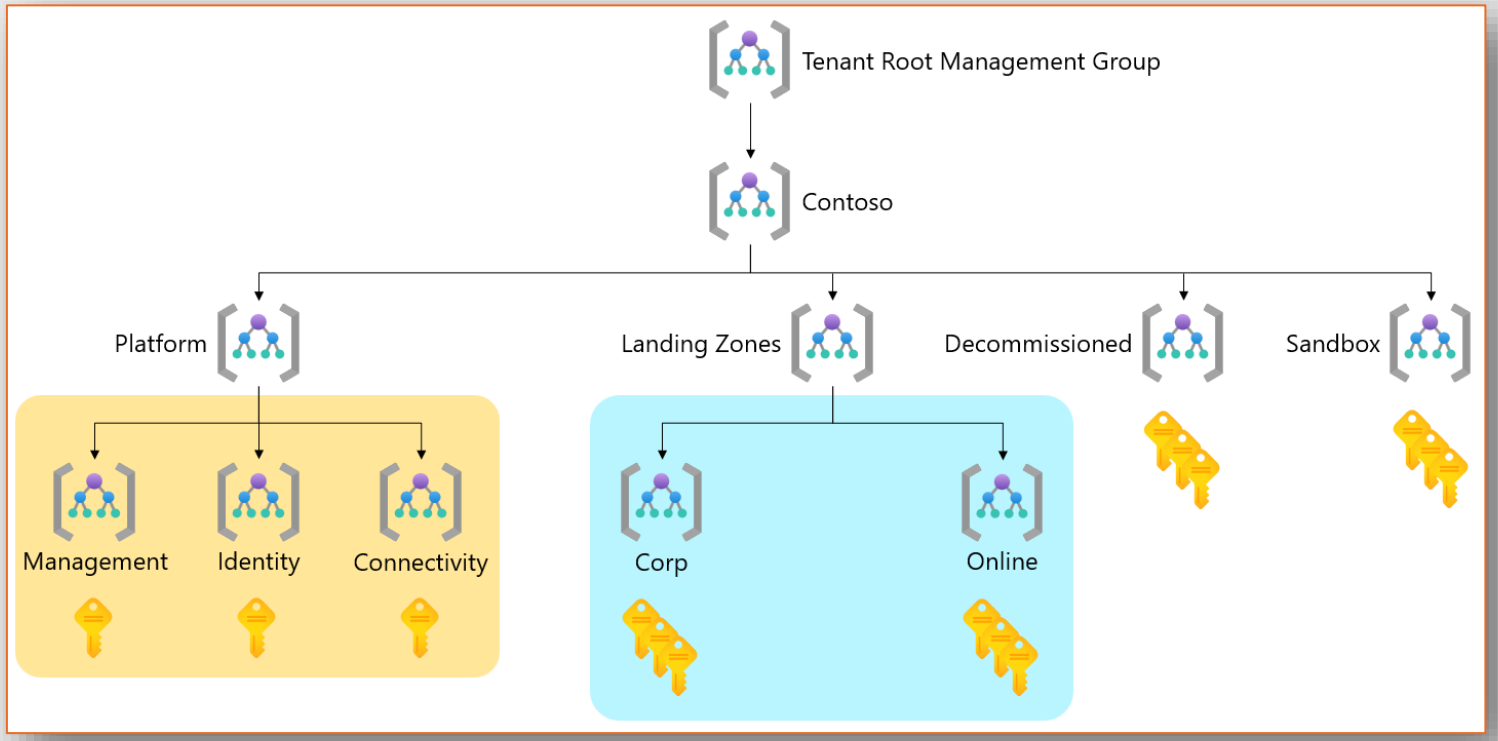
- **Boundaries** for management, policies, RBAC, governance, isolation, chargeback models
- Unit of cost management & billing within Azure
- **Scale unit** within platform subscription **limits** (**quota** & **capacity**)
- Requirements and design target subscriptions based on **critical factors**:
  - environment type
  - ownership and governance model
  - organizational structure
  - application portfolios
- The **Azure Tenant** linked to the Azure subscription can be **changed** (e.g., MDSN, VS Benefit)
- Subscription related **areas** are reserved instances (RI), support requests and quotas



EXAMPLES – AZURE HIERARCHY

How can an Azure hierarchy can look like as an **example** or in a **customer** real-life organization?

- Close relationship between **MG** and **landing zone archetypes** (*policies*, *RBAC*, *central network*)
- Resultant set of **Azure Policy** and access control (**IAM**) assignments on certain level (**inheritance**)



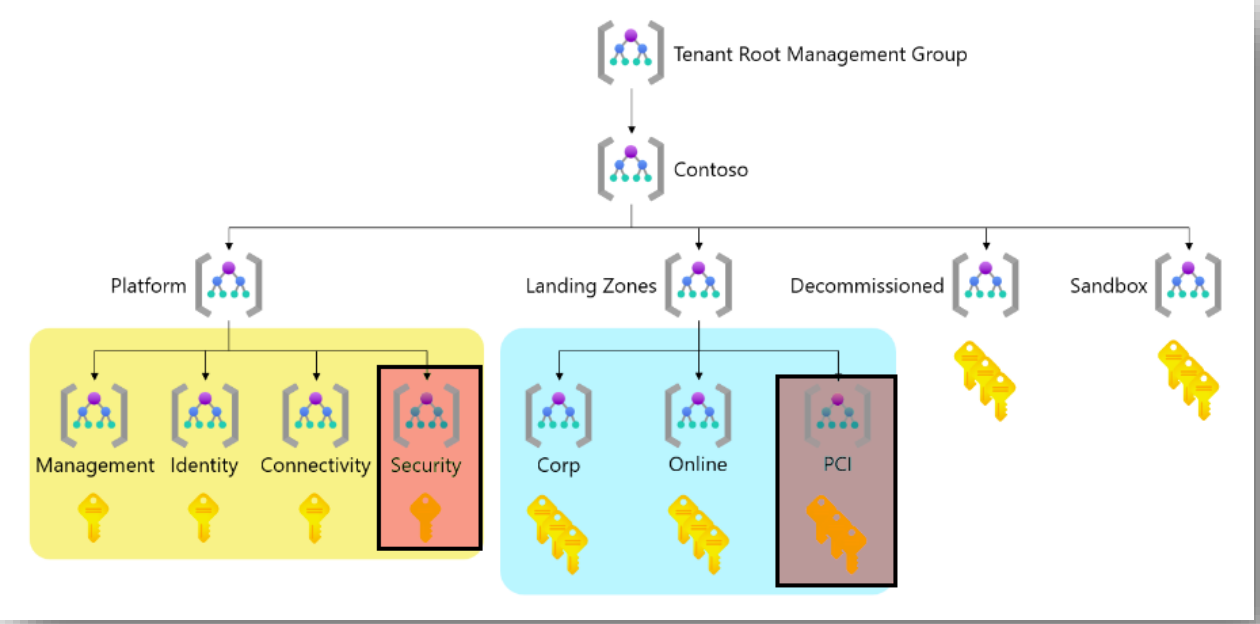
Important:

Your **Landing zone** conceptual architecture and Azure **hierarchy** **interact** with each other!

EXAMPLE – AZURE HIERARCHY EXTENSION

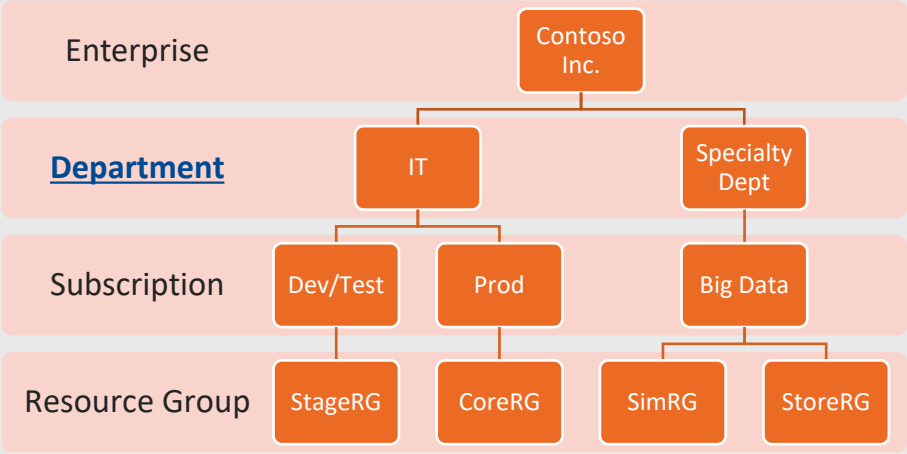
How to **extend** the Azure hierarchy with new landing zone archetypes

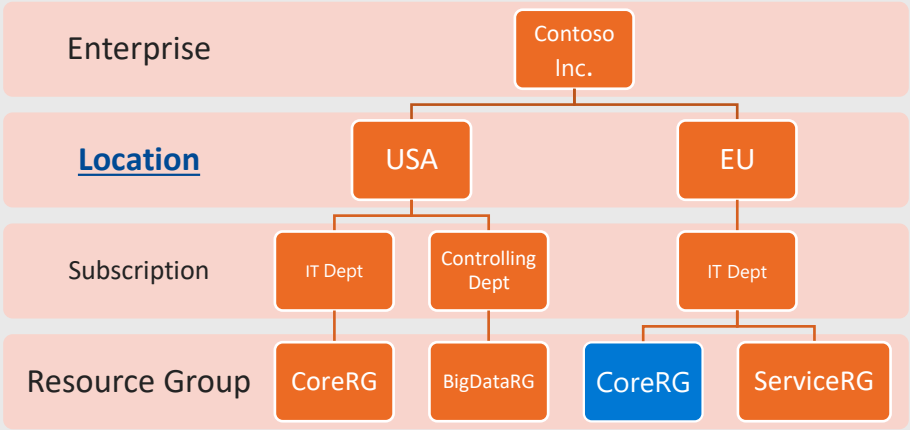
- Add **new** archetypes to the configured Azure hierarchy like the screenshot illustrates
- Only create new archetypes when they are **truly** needed.
- Avoid going beyond a hierarchy **depth**, **complexity** and unnecessary **exclusions** (expand horizontally!)
- Do not create archetypes for **stages** (DEV, TEST, PROD)



EXAMPLE – AZURE HIERARCHY

How to structure an Azure Hierarchy? Which **characteristics** can influence the Azure Hierarchy?





Characteristics:

- Departments
- Geographically (Locations)
- Application Workload
- Stages (DEV, TEST, PROD)
- etc.

influence →

MGs:

- ✓ Management **at scale**
- ✓ **Cross**-subscription assignments

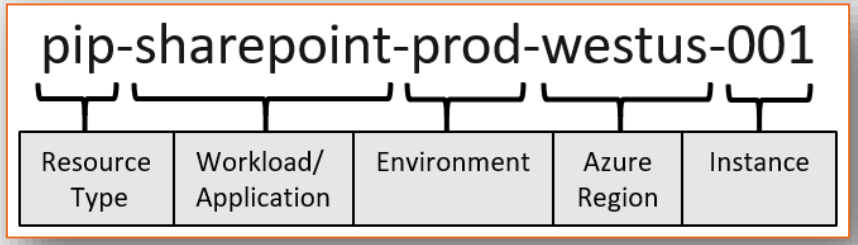
3. NAMING CONVENTION

NAMING CONVENTIONS – GENERAL

Use comprehensive & effective **naming conventions** to organize the cloud assets in Azure.

- Names cannot be **changed** on Azure (recreation needed!)
- Azure has built-in **naming rules** and **restrictions** for Azure resources (*storage account*, *key vault*, etc.)
- Well-defined **naming** and metadata **tagging** conventions to **locate** resources (“*What is it good for?*”)
- Must include the **organizational** information the IT needs to identify resources.
- **Define**, **document** and **implement** the naming and tagging strategy **from the beginning**!
- Challenge naming conventions with the **cloud adoption** teams.
- Use **tools** to enforce naming conventions on the Azure Tenant (*policies*, *naming module*, *template*)
- Use naming patterns based on Microsoft best practices (Azure Naming Tool v2 as docker image)

Microsoft Excel Worksheet



NAMING CONVENTION – ELEMENTS

Which components must be considered in a **standardized** naming convention.

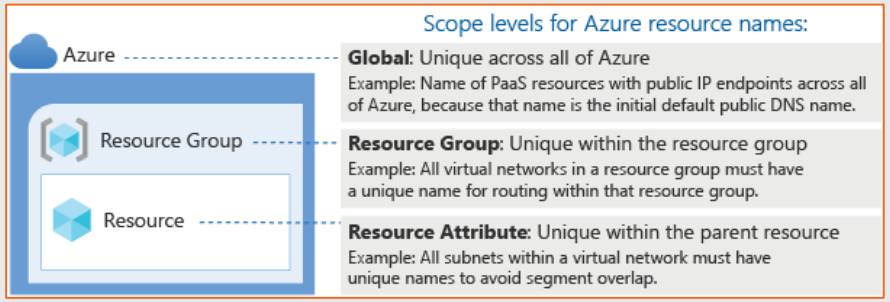
- Identify the **key pieces** of information that need to be reflected in the resource name.
- Different Azure **resource types** need different **information**. – Standard naming convention!
- A resource must have a **unique name** within its scope.

Naming components:

- Organization
- Business unit
- Resource type
- Project, application, service name
- Stage/Environment
- Location
- VM Role, NetBIOS
- Instance #

Naming considerations:

- Order (sorting)
- Delimiters
- Naming rules
- Resource types
- Abbreviations
- Readability



NAMING CONVENTION – BEST PRACTICES

How to implement proper naming conventions in real-life **scenarios** of an enterprise

- Use **on-premise** naming convention as possible **starting point** (orientation)
- Be aware of central **inventory tools** for IT assets in an organization
- Names must be readable by **automation processes** an **IT operations** as well
- Use **instance #** (e.g., `001`, `002`, etc.) or short IDs to identify the resource **uniquely**

Resource	Resource provider namespace	Abbreviation
Application gateway	`Microsoft.Network/applicationGateways`	`agw`
Application security group (ASG)	`Microsoft.Network/applicationSecurityGroups`	`asg`
Bastion	`Microsoft.Network/bastionHosts`	`bas`
CDN profile	`Microsoft.Cdn/profiles`	`cdnp`
CDN endpoint	`Microsoft.Cdn/profiles/endpoints`	`cdne`
Connections	`Microsoft.Network/connections`	`con`

Asset type	Scope	Format and examples
Virtual network	Resource group	*vnet-<subscription purpose>-<region>-<###>* • `vnet-shared-eastus2-001` • `vnet-prod-westus-001` • `vnet-client-eastus2-001`
Subnet	Virtual network	*snet-<subscription purpose>-<region>-<###>* • `snet-shared-eastus2-001` • `snet-prod-westus-001` • `snet-client-eastus2-001`
Network interface (NIC)	Resource group	*nic-<##>-<vm name>-<subscription purpose>-<###>* • `nic-01-dc1-shared-001` • `nic-02-vmhadoop1-prod-001` • `nic-02-vmtest1-client-001`

Source: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-abbreviations

4. TAG & LOCK STRATEGY

TAG STRATEGY

Usage of metadata tags on Azure Resources for certain reasons

- Use metadata tags to the cloud resources **from the beginning**.
- Containing information that cannot be **included** in the resource name (variable content).
- Azure Tags are changeable! (*key-value-pairs*) - Sophisticated **filtering** and **reporting** on resources.
- Context of workload/application, operational requirements, automation and ownership information.
- Define which tags **must be** applied to resources and what tags are **required** or optional (Azure Policy)

Tagging Examples:

- Workload Name
- Data Classification
- Business Criticality
- Business Unit/Department
- Operations Commitment
- Operations Team
- Cost Center
- Backup class
- …etc.

Used for…:

- ✓ Changeable Information
- ✓ Describes context
- ✓ Increase visibility
- ✓ Resource Management
- ✓ Automation processes
- ✓ Filtering & Reporting
- ✓ Cost Management

LOCK STRATEGY

How to **protect** resources on Azure?

- Azure Locks = **Protect** infrastructure resources on Azure
- Protect them from accidental user **deletions** and/or **modifications**.
- 2 Types of Azure Locks:
  - Delete (`CanNotDelete`) → read and modify, but cannot delete.
  - Read-Only (`ReadOnly`) → read, but cannot delete or modify it.
- Scope:
  - Azure Subscriptions
  - Resource Groups (RG)
  - Resources
- **Lock** inheritance → Most restrictive lock takes **precedence**! No partial deletion.
- A resource lock does not block the subscription **cancellation**.
- **Be aware!** → Locks can lead to unexpected results (e.g., Azure Data Factory)

Source: https://unsplash.com/photos/_-uN7DbAE-o

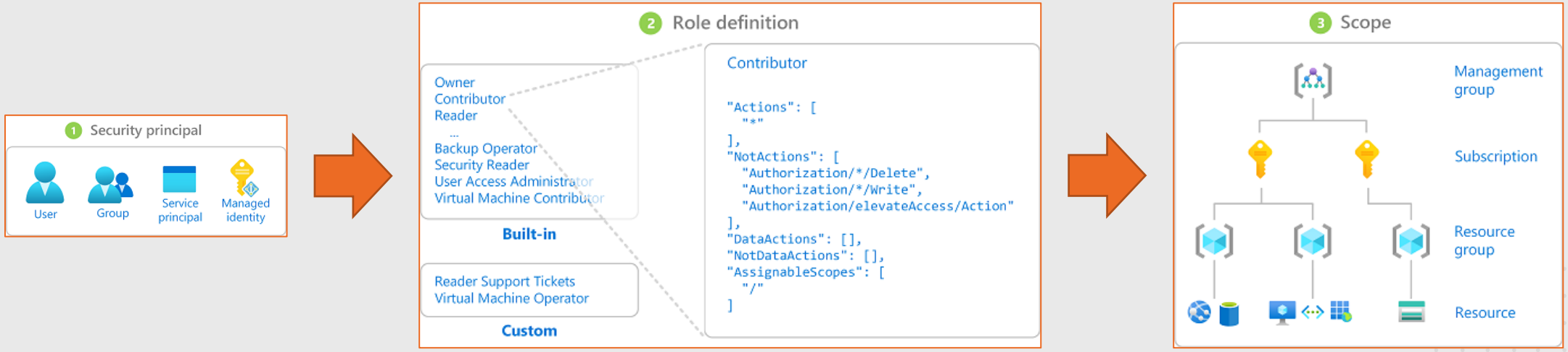
5. AZURE RBAC

AZURE IDENTITY & AZURE IAM (RBAC)

How to setup fine-grained access management to Azure resources?

- Identity is **king** in a public cloud platform:
  - **who** … → **Security Principal** *(person, group or service principal)*
  - can do **what** … → **Role** *(built-in or custom)*
  - and **where** … → **Scope** *(MGs, Subscriptions, RGs, Resources)*

  … in Azure?
- Ensure that Azure identities are **following** the defined Azure governance.



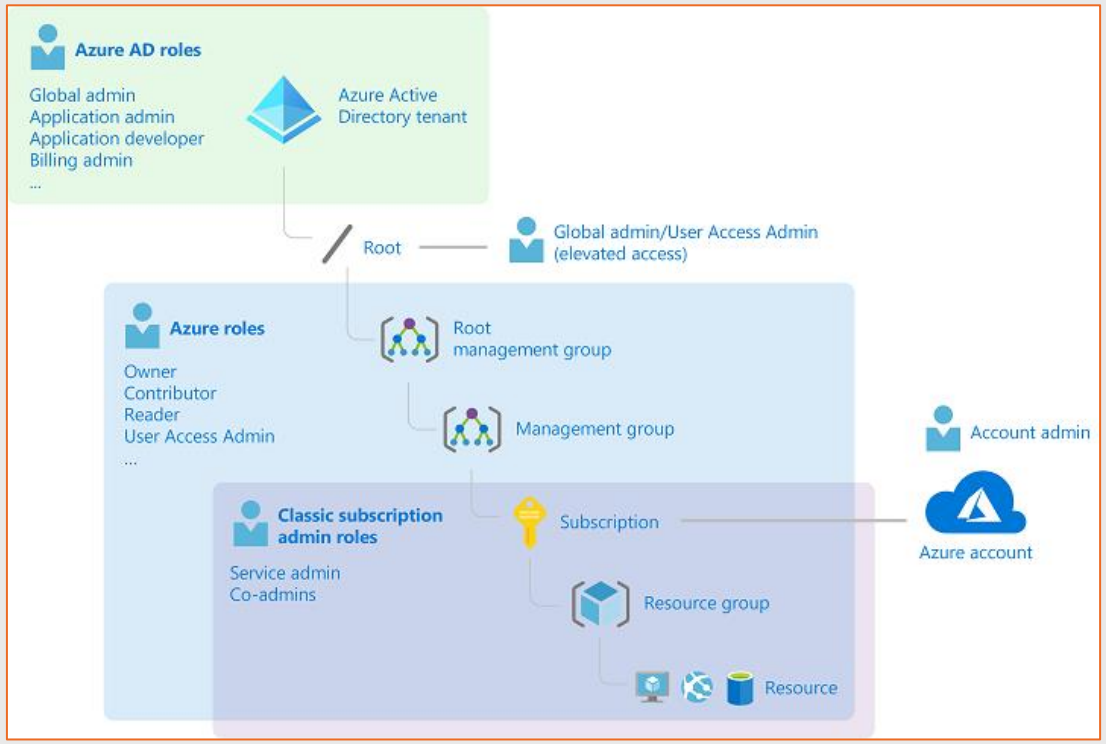
AZURE RBAC – USE CASES

Examples of Azure RBAC in real life.

1. Allow one user to manage **Azure VMs** in a subscription and another user to manage **Azure VNETs**.
2. Allow a **DBA group** to manage SQL databases in a subscription.
3. Allow a user to manage **all resources** in a resource group (RG), such as VMs, websites, and subnets
4. Allow an application to access **all resources** in a resource group (RG).

AZURE RBAC MODEL

How the permission model for **Azure AD** and **Azure resources** work?



- Role assignments are **transitive** for groups
- Azure RBAC is an **additive** model
- RBAC = `Allow` & `Deny` model
- Effective permissions are the **sum** of the users' role assignments
- `Deny` assignments take **precedence** over `Allow` assignments.

6. AZURE POLICIES

AZURE POLICIES

How to enforce your defined standards regarding Azure Resource configuration

Azure Policy:
Policy is focused on the **properties** of resources.

Azure RBAC:
RBAC focuses on what resources the users can **access**.

- Enforce organizational **standards** with Azure Policies.
- Evaluate the overall **state** of your Azure environment.
- Goals: resource consistency, regulatory compliance, security, cost, and management.
- Tools:
  - Policy Definitions (built-in / custom)
  - Policy Assignments
  - Compliance Dashboard
  - Bulk Remediation
- Collect Policy Definition to Policy Sets (policy initiative)

7. AZURE COST MANAGEMENT

COST MANAGEMENT (CM) – OVERVIEW

What needs to be considered for cost management (CM) on the Azure platform?

- CM begins **before** you spend money on cloud resources
- Build cost-consciousness – Managing cost is a **team** activity
- We need **visibility** and properly defined **access** to cost-related data
- Create **tracking** mechanisms to monitor costs & apply fundamental concepts to provide **cost visibility**.
- Setup a well-managed environment – **classify** and **organize** all assets (Azure resources)
- Provide the right level of **cost access** (*Roles* & *Scope*)
- Roles:
  - Owner, Contributor, Reader
  - Cost Management Contributor/Reader
- Scope:
  - Cloud Adoption Team
  - Cloud Strategy Team
  - Cloud Governance Team & CCoE

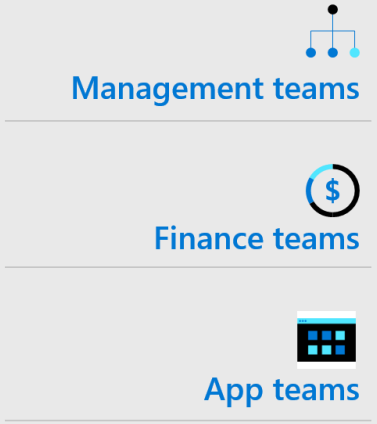
CM = Tools to **plan**, **analyze** and **reduce** your spending to **optimize** your cloud investment!

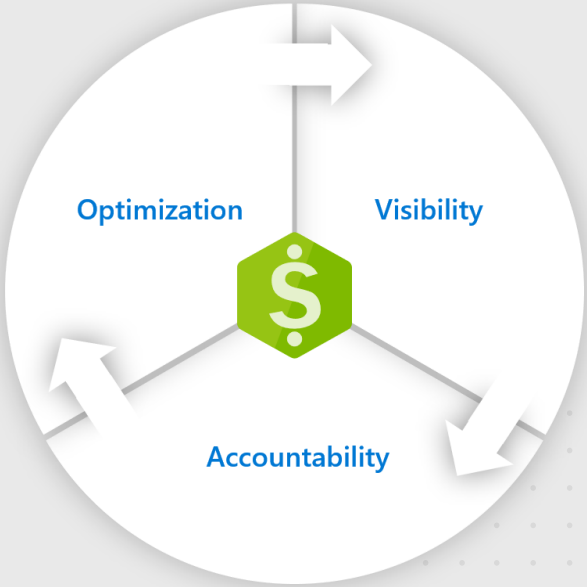
Classification	Organization
• Naming Convention • Tagging Standard	• Hierarchy Level • Resources Orga

COST MANAGEMENT (CM) – BEST PRACTICES

Iterations of Cost Management (CM) in 4 Steps.

- Be prepared with the proper **tools**
- Be **accountable** for costs
- Take appropriate action to **optimize** spending
- Iterations: (“*CM lifecycle*”)
  1. Planning (up-front, assess business requirements) – **Azure Pricing Calculator**
  2. Visibility (inform where the money is spent – insights)
  3. Accountability (responsibility, organize resources)
  4. Optimization (reduce spending)





SUMMARY

WRAP UP – AZURE GOVERNANCE

Define your **own** Azure Governance specification.

- Governance is an **ever-evolving** process of **standardization** and **compliance** enforcement
  - Not: "*one and done*" or "*set it and forget it*" proposition
  - Provides **mechanisms** and **processes** for maintaining control over **platforms**, **applications**, and **resources**
- Establishes the **tooling** needed to support cloud **governance**, compliance **auditing**, and **automation**
- **Roles & Functions**:
  - Led by general cloud governance
  - CCoE, cloud security, central IT or cloud operations
  - Cloud platform – implement technical requirements to **enforce** governance
- **Scope**:
  - Review decisions (of *identity*, *network*, *security* and *management*)
  - Map requirements of Azure landing zone concept
- Azure governance establishes the foundation for networking
- Recommendation: Follow Microsoft **best-practice** governance guidance

Let‘s connect

Stefan Rapp

Cloud Solution Architect (CSA)

https://www.linkedin.com/in/rapster83

info@blog.misterazure.com

https://blog.misterazure.com

https://github.com/rapster83

https://www.linkedin.com/in/rapster83

Let’s connect!