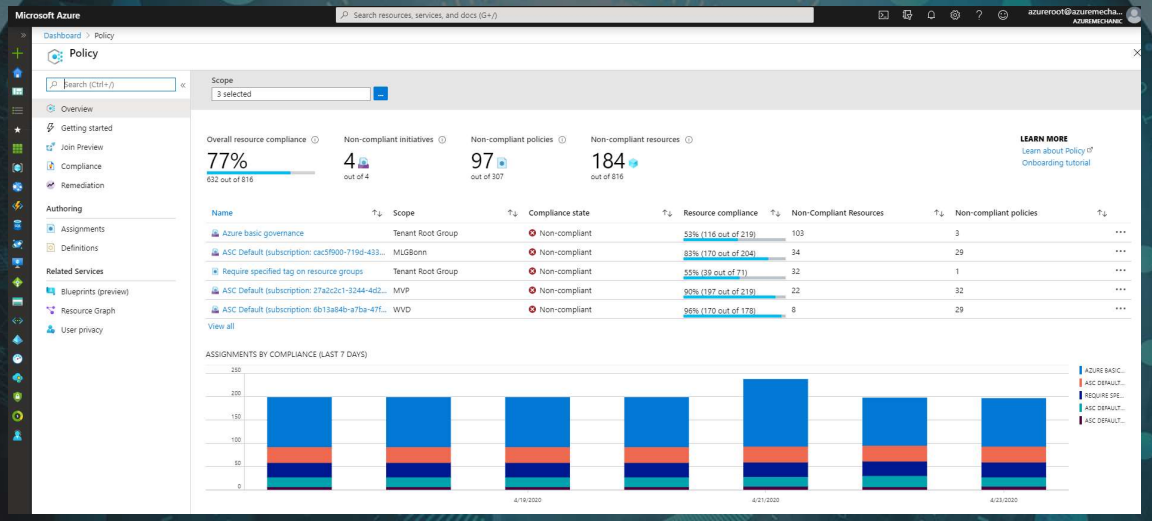



# Azure Governance Best Practices

by Thomas Naunheim & Gregor Reimling

# Gregor Reimling


Cloud Consultant @Sepago


Cloud and Datacenter, Governance


Azure Infrastructure (Governance, IaaS, Security)


info@reimling.eu


@GregorReimling | @AzureBonn


www.reimling.eu | www.neutralien.com




www.AzureBonn.de

# Thomas Naunheim


Cloud Engineer

(Identity + Azure Security)


Azure Cloud Platform, PaaS, Security


thomas@naunheim.net


@Thomas_Live | @AzureBonn


www.cloud-architekt.net

Azure Meetup BONN

MVP Microsoft® Most Valuable Professional

Azure Meetup BONN

www.AzureBonn.de

# General


- Fragen sind ausdrücklich erwünscht – gerne Stummschaltung aufheben oder via Chat
- Im Chat werden die Links zu den aktuellen Slides geteilt, damit die Themen im Selbststudium begleitbar sind
- Bevor wir starten -> bitte www.menti.com aufrufen!
- Nun viel Spaß und Fragen fragen ☺

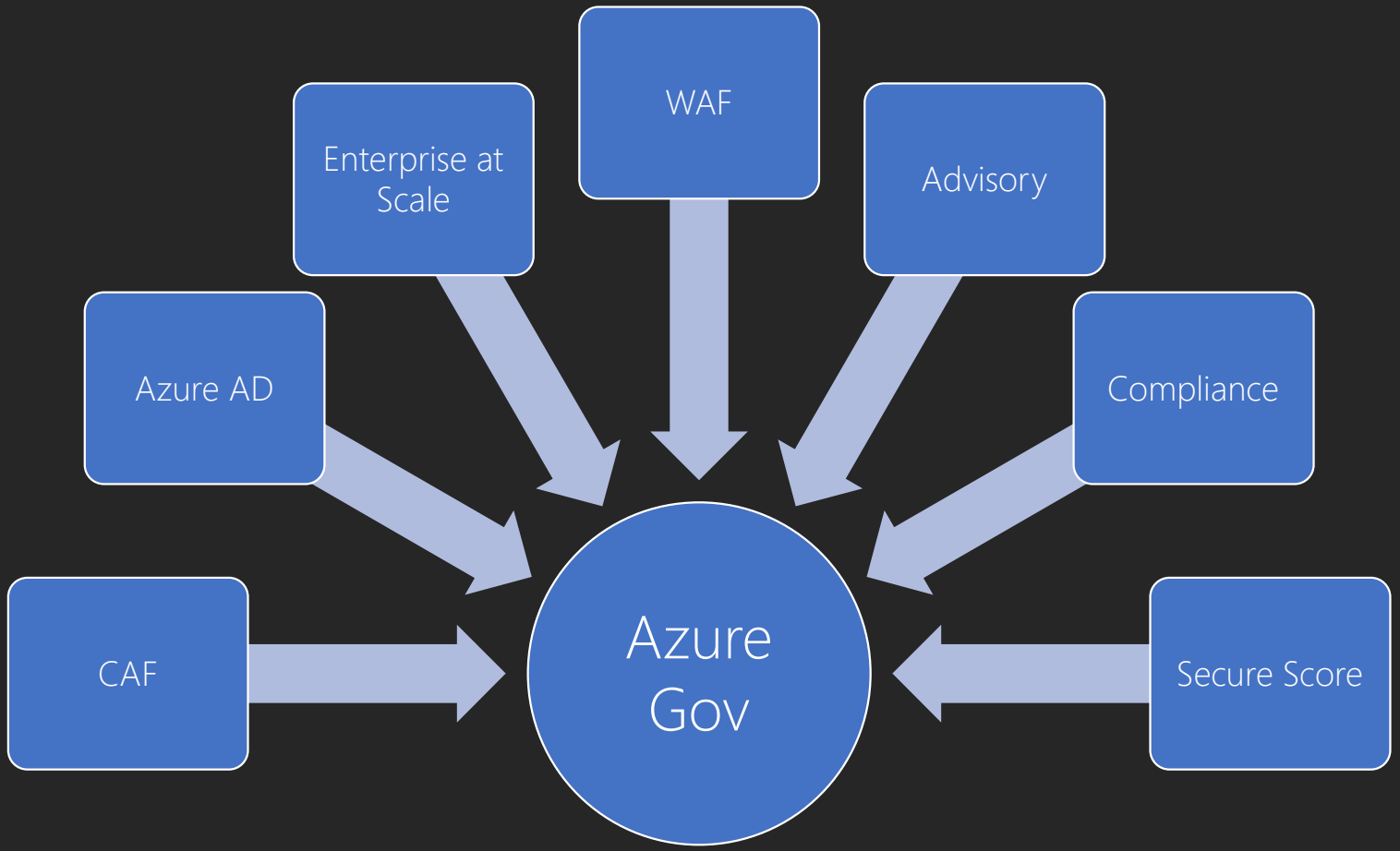
# Agenda

- Overview of Cloud Adoption Framework and Well-architecture Framework
- Management of Compliance and Security Status
- Azure Enterprise-Scale Landing Zone
- AzOps: "Operationalize" Azure environment at scale

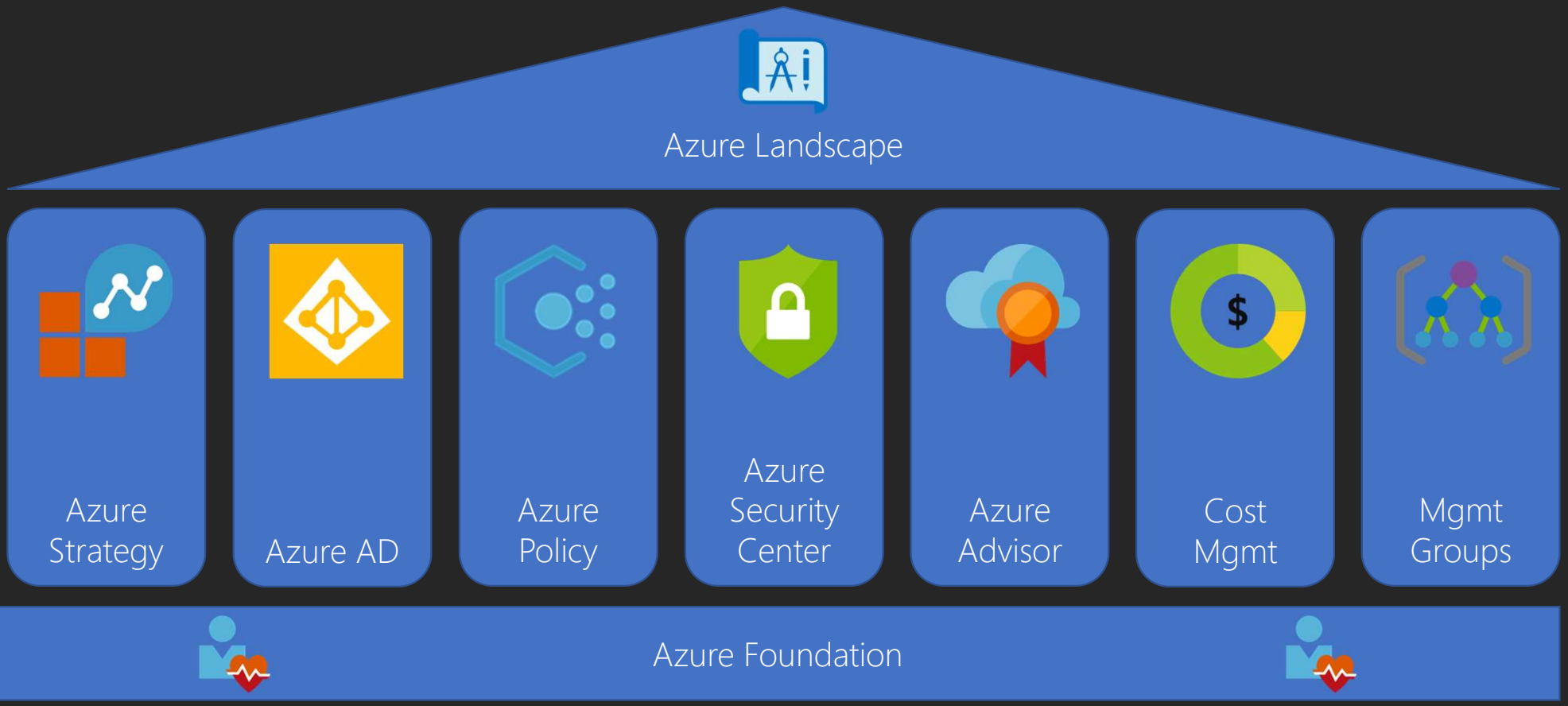
Lot of DEMOs

Azure Meetup BONN

# Topic Overview



# Azure Governance House




# Overview of CAF and WAF

# Azure Cloud Adoption Framework (CAF)


„The Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate your cloud adoption journey."

# Azure Well-Architected Framework (WAF)

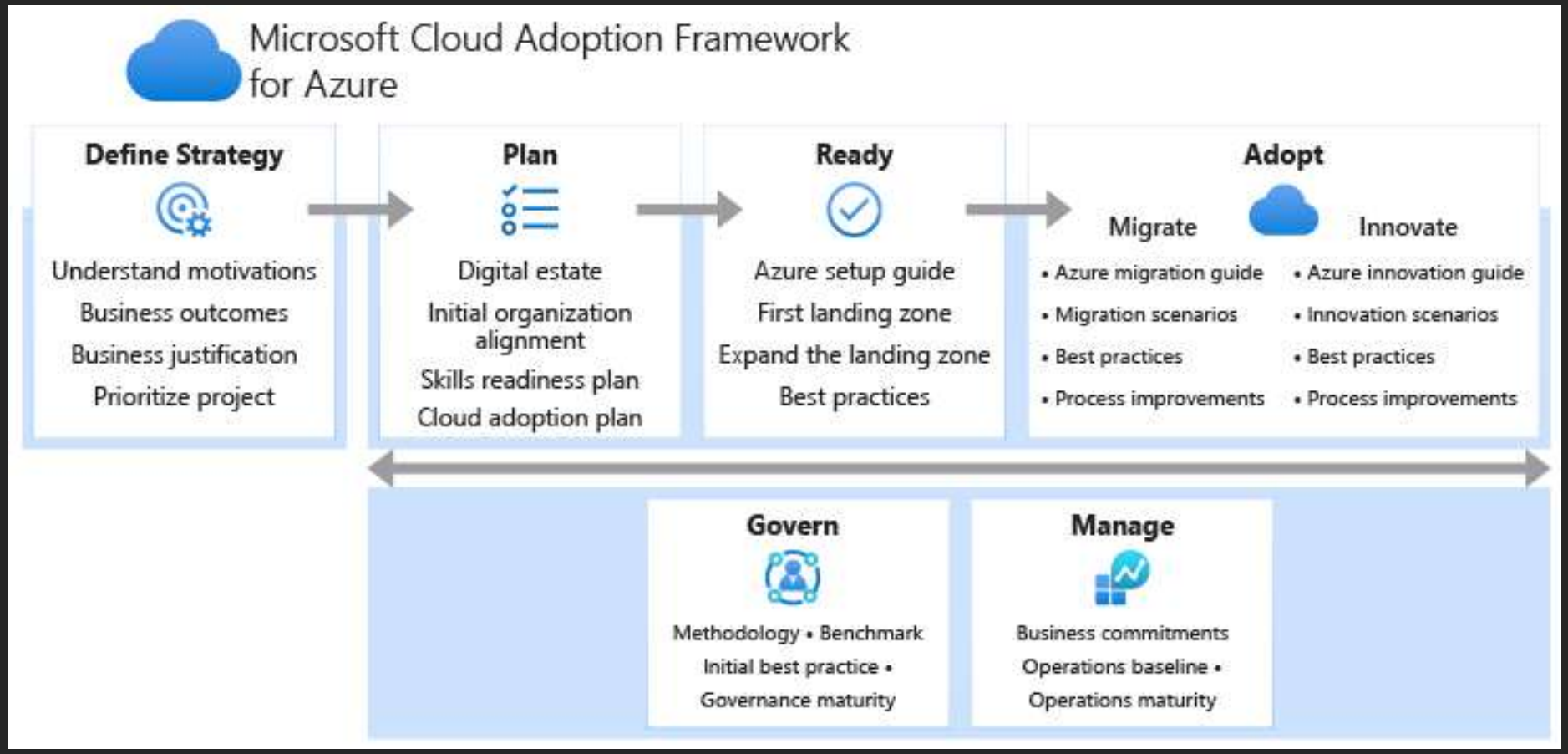
"The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload."

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/

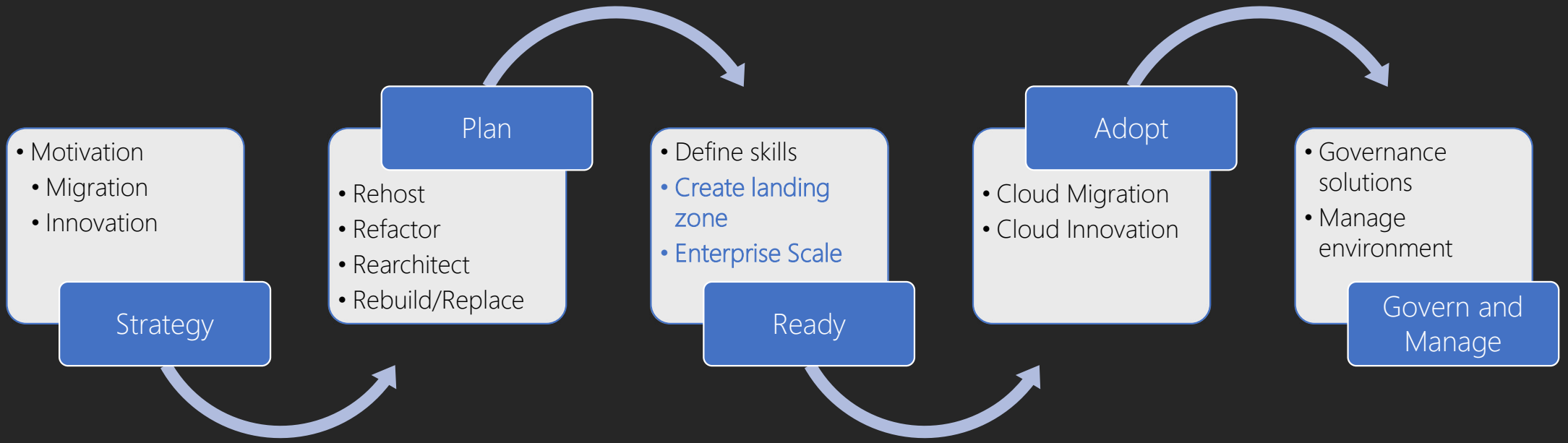
# Cloud Adoption Framework


https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/

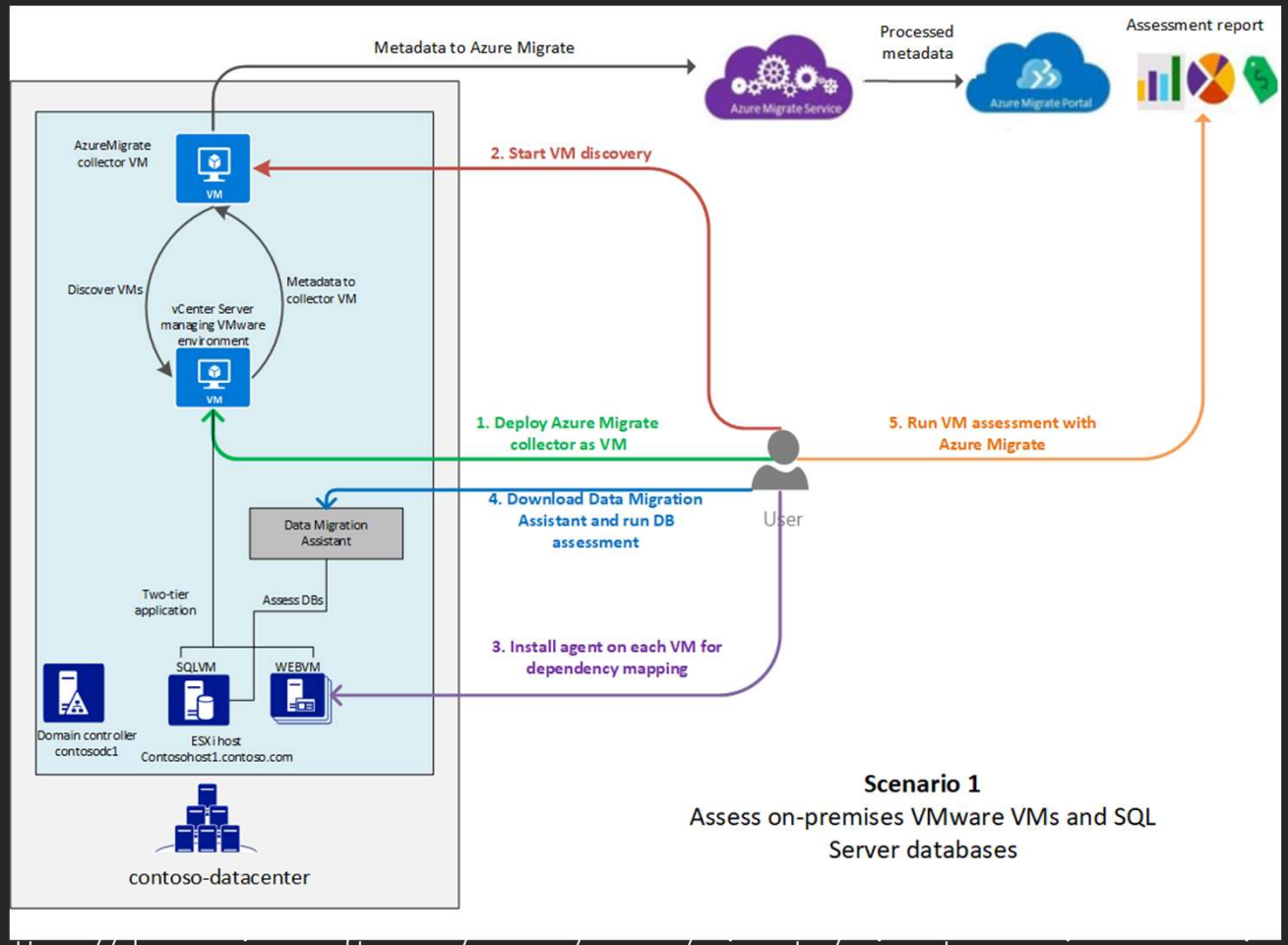
# CAF Overview



# CAF Flow

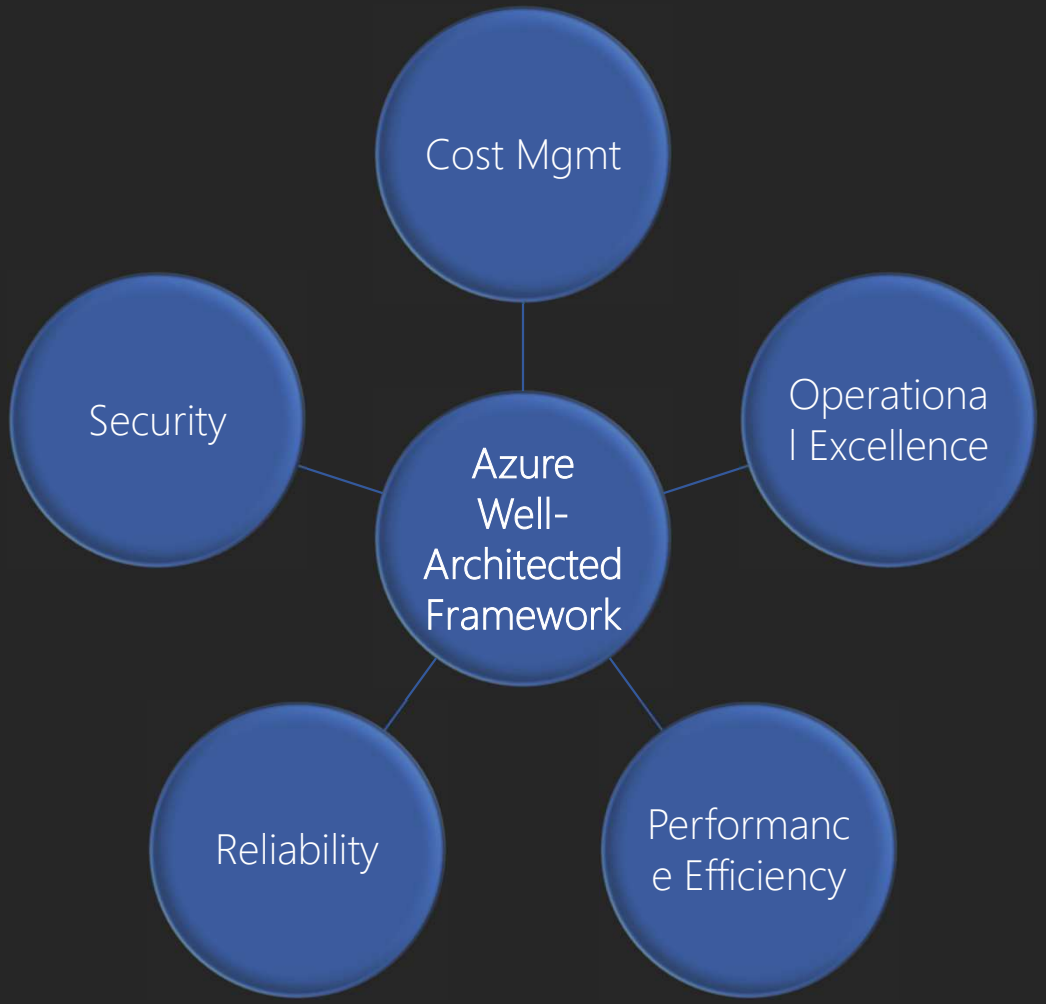

• Motivation
• Migration
• Innovation
Strategy
Plan
• Rehost
• Refactor
• Rearchitect
• Rebuild/Replace
• Define skills
• Create landing zone
• Enterprise Scale
Ready
Adopt
• Cloud Migration
• Cloud Innovation
• Governance solutions
• Manage environment
Govern and Manage

# CAF Assessment with Azure Migrate




https://docs.microsoft.com/en-us/azure/migrate/migrate-services-overview

"The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload."




https://docs.microsoft.com/en-us/azure/architecture/framework/

Security

- What design considerations did you make in your workload in regards to security?
- What considerations for compliance and governance do you need to take?
- How are you managing encryption for this workload?
- How are you managing identity for this workload?
- How have you secured the network of your workload?
- What tradeoffs do you need to make to meet your security goals?
- * How are you ensuring your critical accounts are protected?

# Microsoft Assessments Azure Well-Architected Review

Examine your workload through the lenses of reliability, cost management, operational excellence, security and performance efficiency [20 minutes].

## Assessment name *

Microsoft Azure Well-Architected Review - Aug 24, 2020 - 7:43:58 PM

## Choose your interests

- [ ] **Cost Optimization**

  An effective architecture achieves business goals and ROI requirements while keeping costs within the allocated budget.

- [ ] **Operational Excellence**

  To ensure that your application is running effectively over time, consider multiple perspectives, from both an application and infrastructure angles. Your strategy must include the processes that you implement so that your users are getting the right experience.

- [ ] **Performance Efficiency**

  Prioritize scalability as you design and implement phases. Scalability leads to lower maintenance costs, better user experience, and higher agility.

- [ ] **Reliability**

  In a cloud environment you scale out rather than buying higher-end hardware to scale up. While it's always desirable to prevent all failure, focus your efforts in minimizing the effects of a single failing component.

- [x] **Security**

  Security is one of the most important aspects of any architecture. It provides confidentiality, integrity, and availability assurances against deliberate attacks and abuse of your valuable data and systems. Losing these assurances can negatively impact your business operations and revenue, as well as your organization's reputation in the marketplace. In the following series of articles, we'll discuss key architectural considerations and principles for security and how they apply to Azure.

Next →

# Cloud Adoption Framework
# Well Architecture Framework

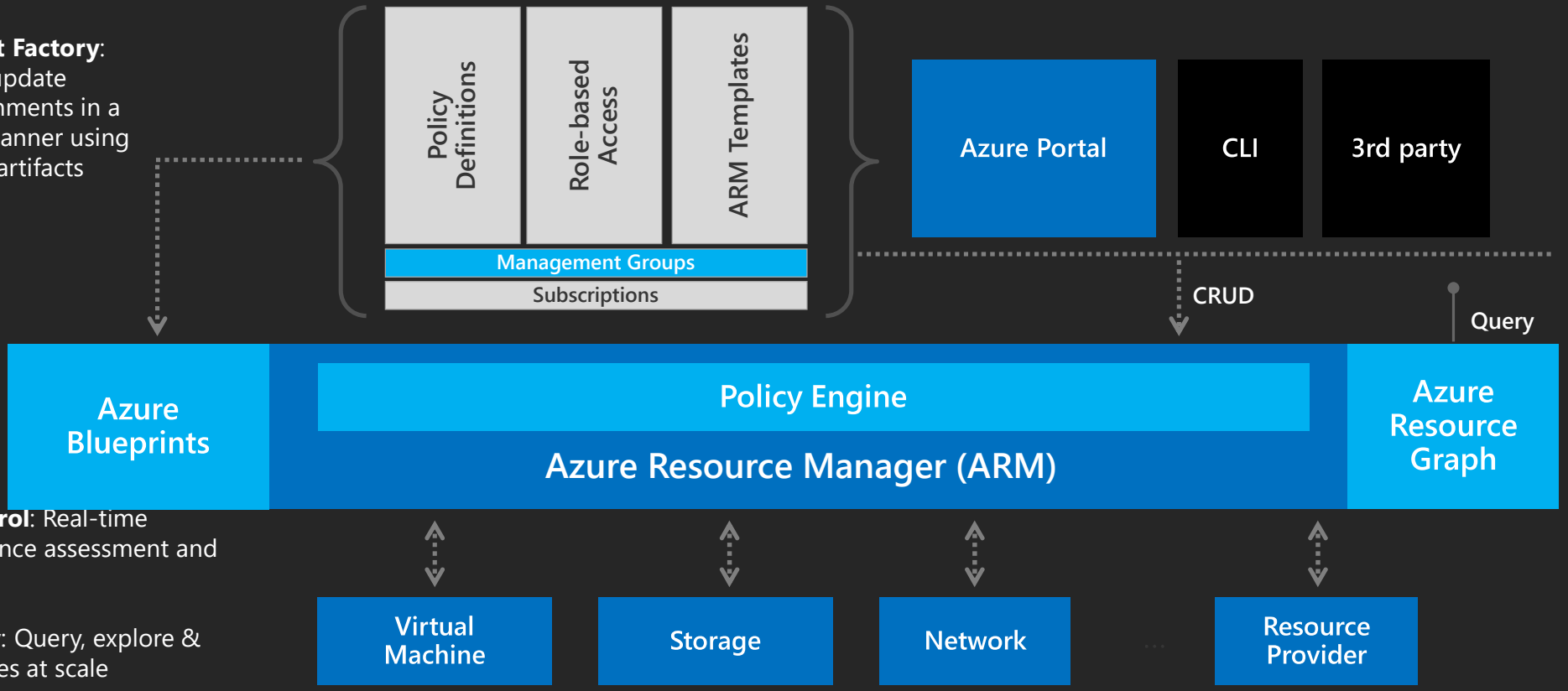
DEMO

# Management of Compliance and Security Status

# Azure Governance Architecture

providing control over the cloud environment, without sacrificing developer agility

**1. Environment Factory**: Deploy and update cloud environments in a repeatable manner using composable artifacts




**2. Policy-based Control**: Real-time enforcement, compliance assessment and remediation at scale

**3. Resource Visibility**: Query, explore & analyze cloud resources at scale

Azure Meetup BONN

# Azure Policy Concepts 

- Part of CAF to support WAF
- Create, assign and manage policies
- Enforce rules to ensure your ressoures are compliant
- Focus on ressource properties for new and existing deployments
- A definition is a set of conditions in audit or deny mode
- An assignment is a policy definition placed on a specific scope
- An initiative is a collection of policies

https://docs.microsoft.com/en-us/azure/governance/policy/overview

# Azure Policy

Azure Meetup BONN

- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation
- VM In-Guest Policy (**NEW**)

**Enforcement & Compliance**

- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

**Apply policies at scale**

- Real time remediation
- Remediation on existing resources (**NEW**)

**Remediation**

# Leverage built-in initiative & policies

Azure Meetup BONN

| Security | Regulatory Compliance | Tags | Resource standardization | Cost |
|---|---|---|---|---|
| Azure Security Center | NIST SP 800-53 R4 | Require specified tag | Allowed/ not allowed RP | Allowed VM SKUs |
| Guest Config baselines | ISO 27001:2013 | Add or replace a tag | Allowed locations | Allowed Storage SKUs |
| Key Vault certificate | CIS | Inherit a tag from the RG | Naming convention | |
| NSG rules | PCI v3.2.1:2018 | Append a tag | Back up VMs | |
| AKS & AKS Engine | FedRAMP Moderate | | Allowed images for AKS | |
| RBAC role assignment | Canada Federal PBMM | | | |
| | SWIFT CSP-CSCF v2020 | | | |
| | UK Official and UK NHS | | | |
| | IRS 1075 | | | |

# Azure Policy

DEMO

# Policy


- 250 policy definitions per scope
- 100 policy set definitions per scope
- 1000 policy set definitions per tenant
- 100 policyDefinition references per policySetDefinition
- 100 policy assignments per scope
- 250 notScopes per policyAssignment
- https://github.com/Azure/azure-policy

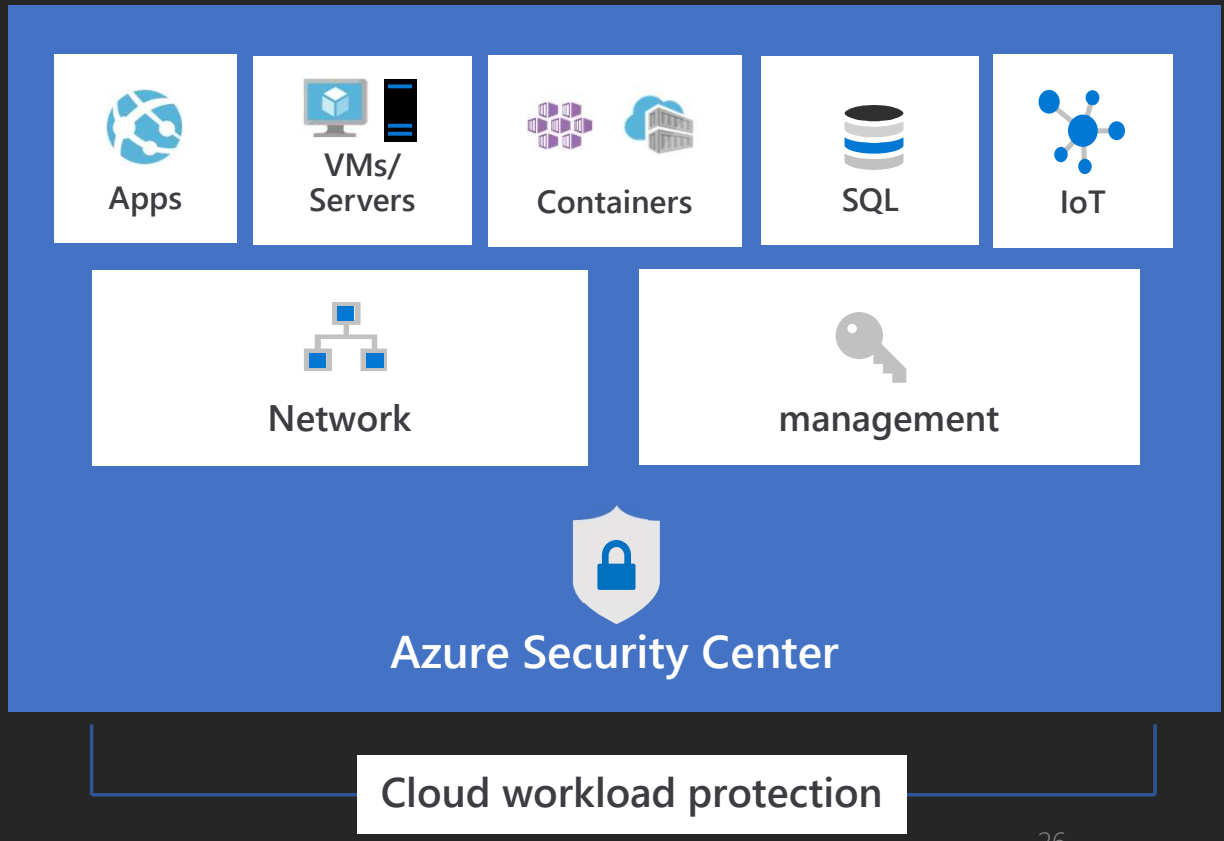
# Azure Security Center

# Azure Security Center


- A service to strengthen your security posture
- Available in two Tiers – Basic and ~~Standard~~ -> changed to Azure Defender
- Basic -> Free – Activated by default for all subscriptions
- Based on an security score – scope based
- Available for all workloads (Server, Container, SQL, IoT and more)

# Protect your workloads

- Detect & block advanced malware and threats for Linux and Windows Servers on any cloud
- Protect cloud-native services from threats
- Protect data services against malicious attacks
- Protect your Azure IoT solutions with near real time monitoring
- Service layer detections: Azure network layer and Azure management layer (ARM)



# Azure Security Center

DEMO

# How it works together

- All Azure Security Center recommendations based on Azure Policy
- Secure score is result of Azure Policy settings
- Recommendations are a result of Azure Policy
- All Azure Policies are defined in Compliance mode

# Azure Policy Recap

- Powerful solution to define Cloud Guards for own Tenant
- Start with an audit effect instead of a deny effect
- Define Management Groups to group subscriptions and set RBAC, Policies and more at Higher level
- Use Deny effect for Production workloads with wisdom
- Creating initivatives even for single policy definition
- Integrate Azure Policy in your regulary Azure check

# Azure Security Center

START WITH ASC TO GET A SECURITY OVERVIEW

USE ASC TO STRENGTHEN YOUR INFRASTRUCTURE

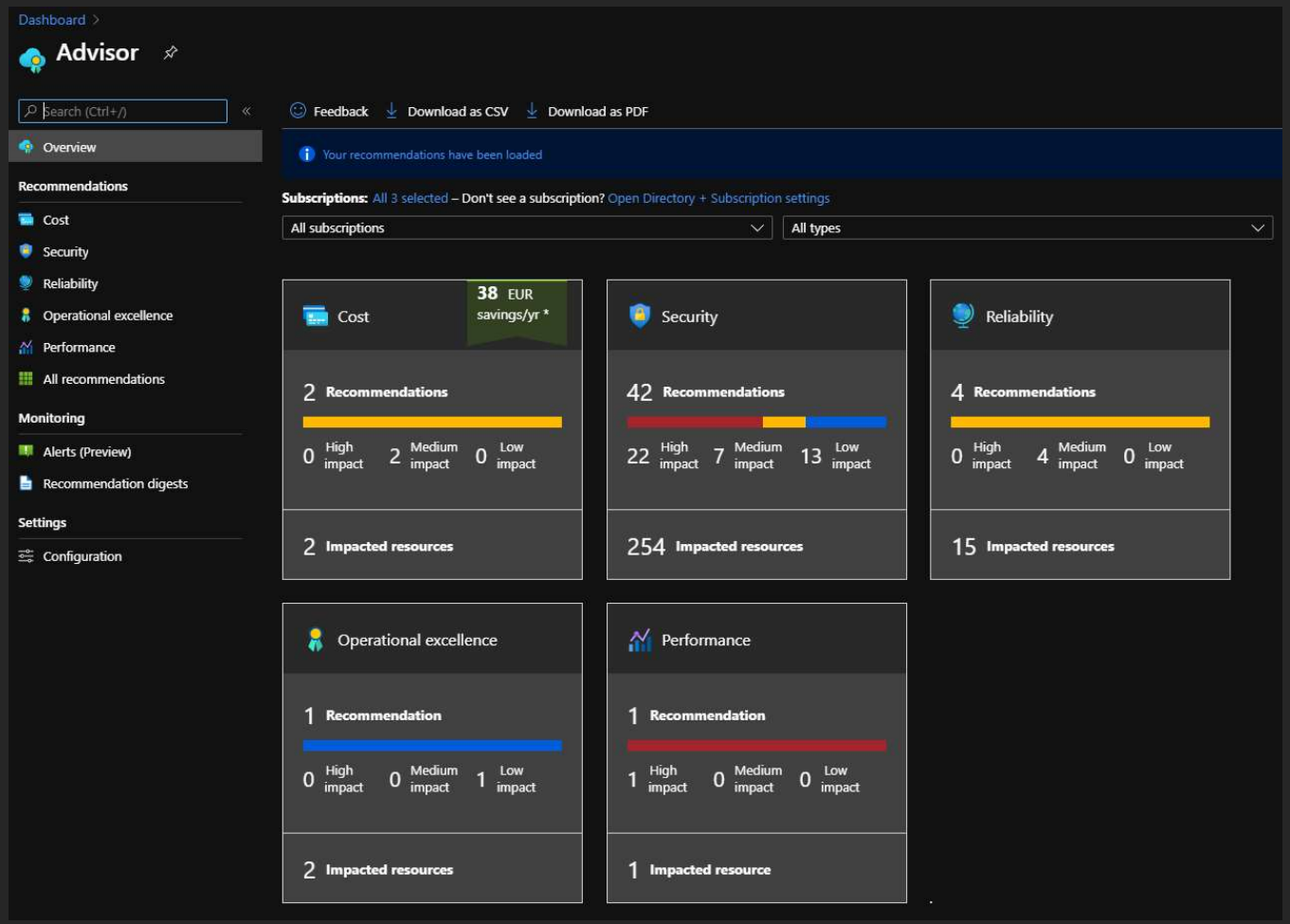
CHECK THE STATUS IN ASC REGULARLY

CREATE OWN SECURITY POLICIES FOR SECURE SCORE

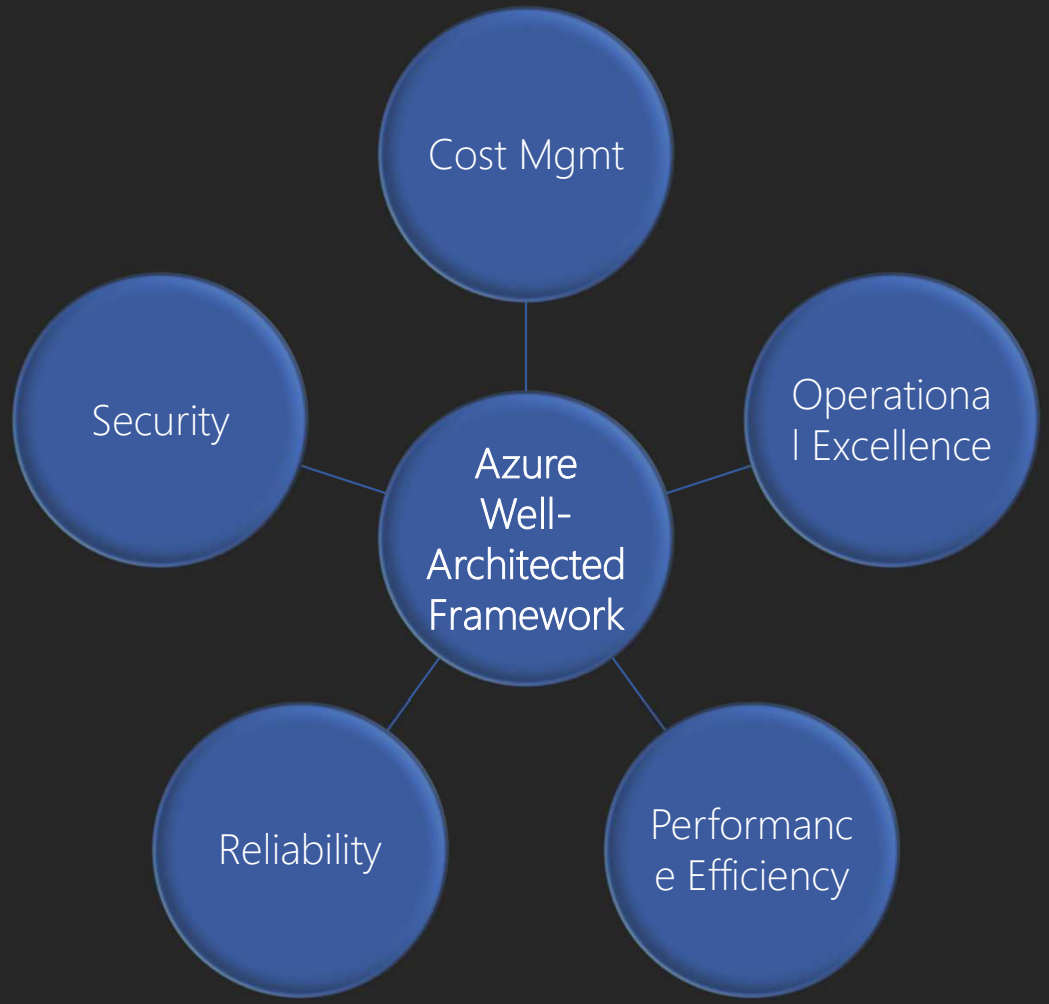
USE ASC TO PROOF YOUR INFRASTRUCTURE

INTEGRATE AZURE POLICY IN YOUR REGULARY AZURE CHECK

Azure Meetup BONN



"The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload."




https://docs.microsoft.com/en-us/azure/architecture/framework/

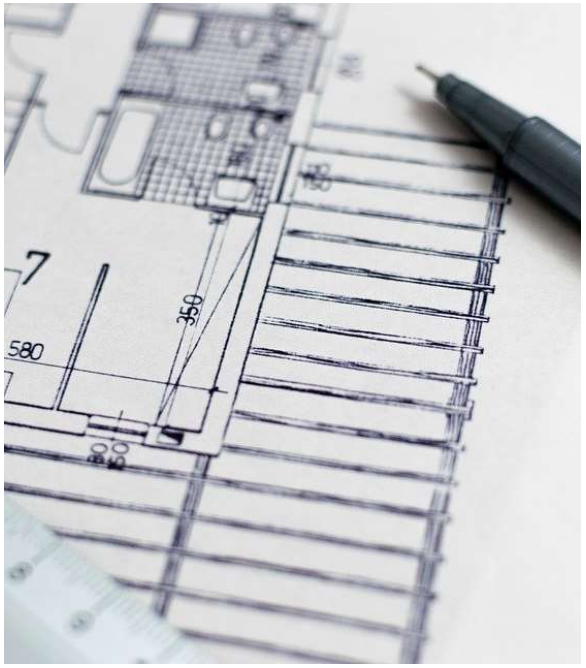
# Azure Enterprise-Scale Architecture

## Introduction and Implementation

Azure Meetup BONN

# What is Enterprise-Scale?

Azure Meetup BONN



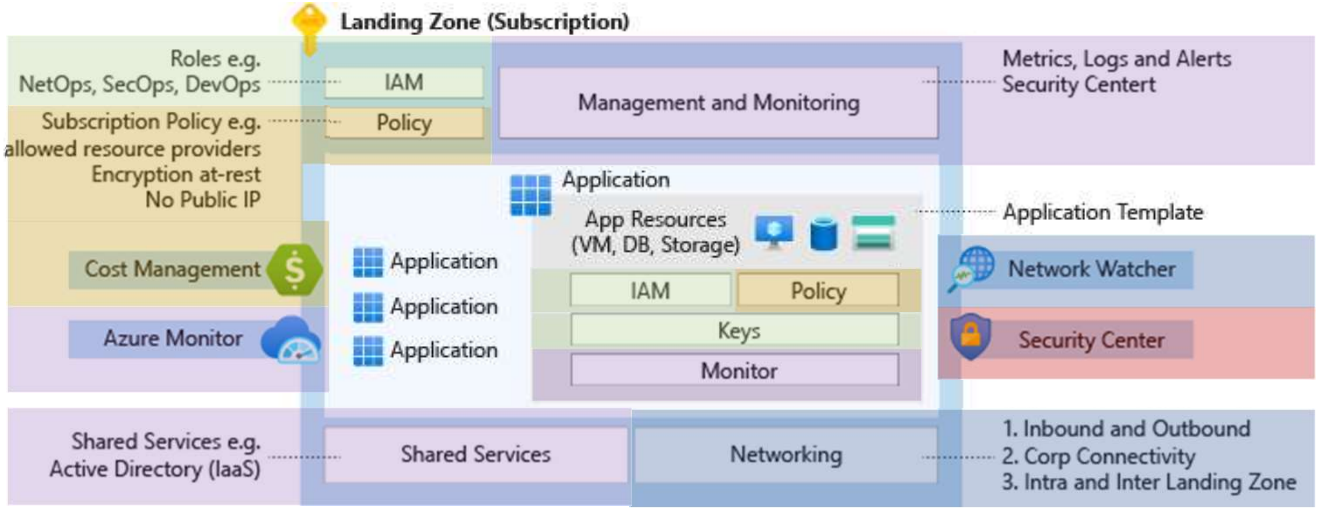

# What is Enterprise-Scale?


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

„Draw on Microsoft's proven technical guidance, resources, and templates, to guide your customers through iteration and learning as they gain confidence and successfully adopt Azure."

Source: Cloud Adoption Framework enterprise-scale landing zone architecture

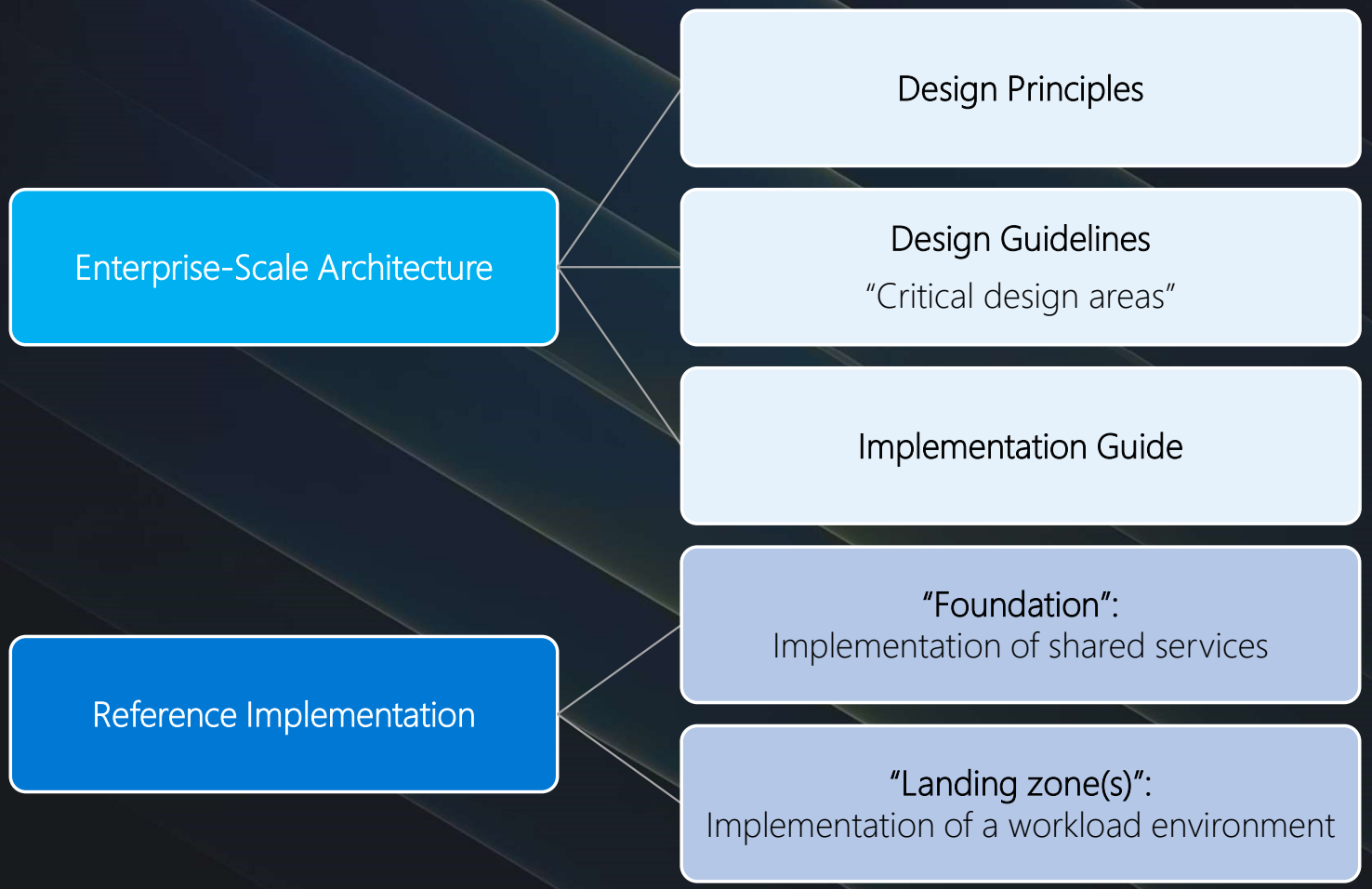
# Design areas of Landing Zone(s)



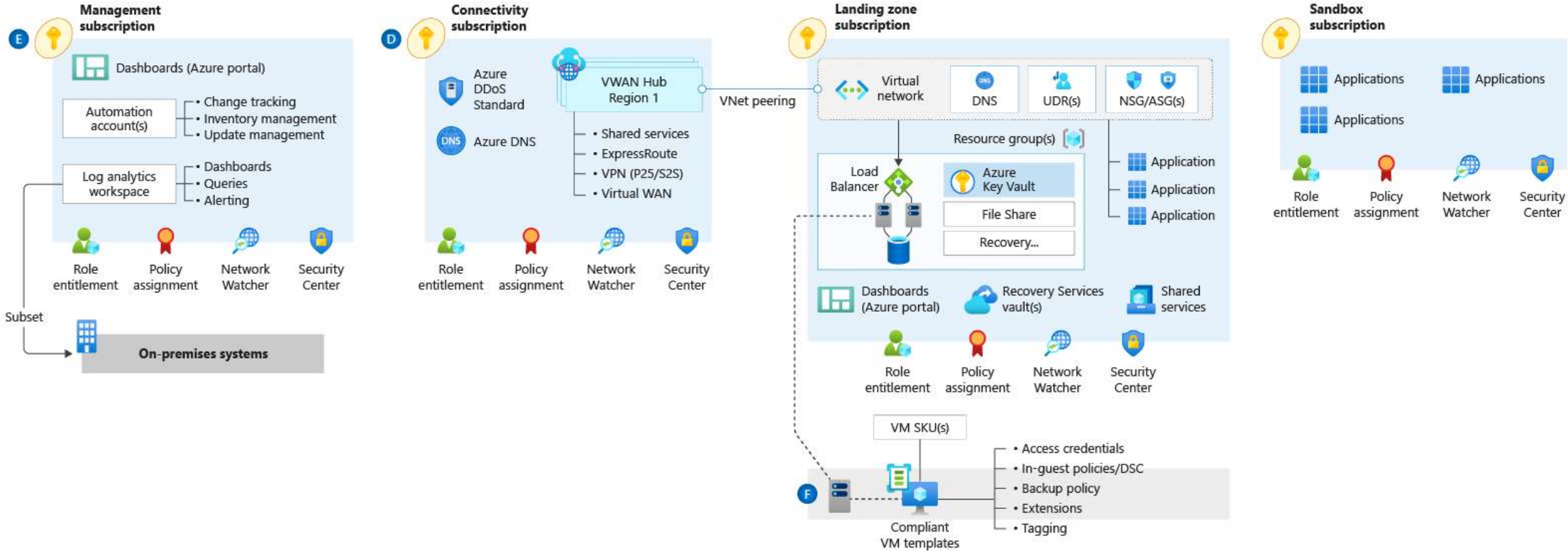

Connectivity, Identity, Governance, Operations and Security

Source: Cloud Adoption Framework enterprise-scale landing zone architecture

# **Enterprise-Scale** Architecture & Reference

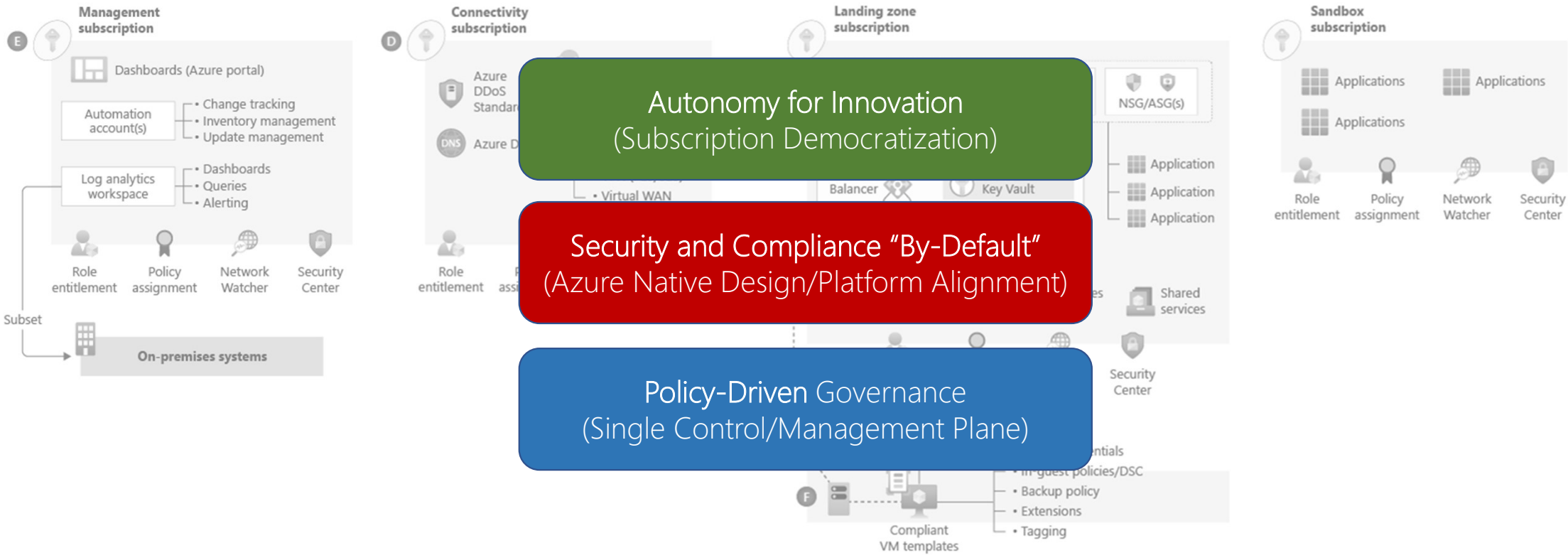


# **Enterprise-Scale** Implementation



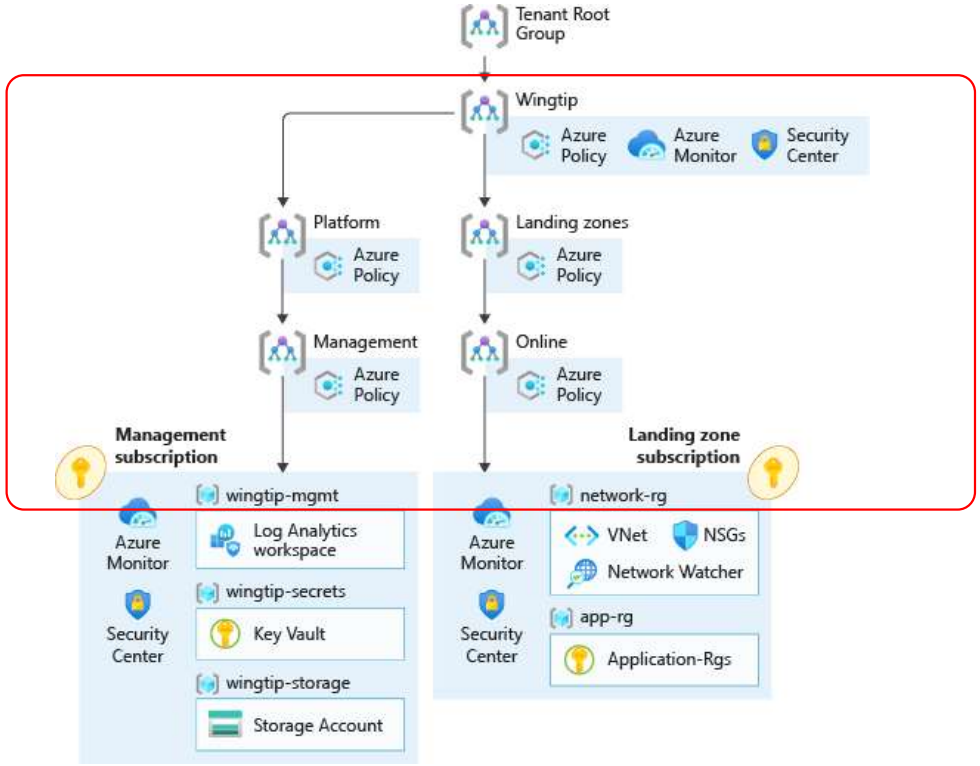

Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

# **Enterprise-Scale** Design Principles




Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

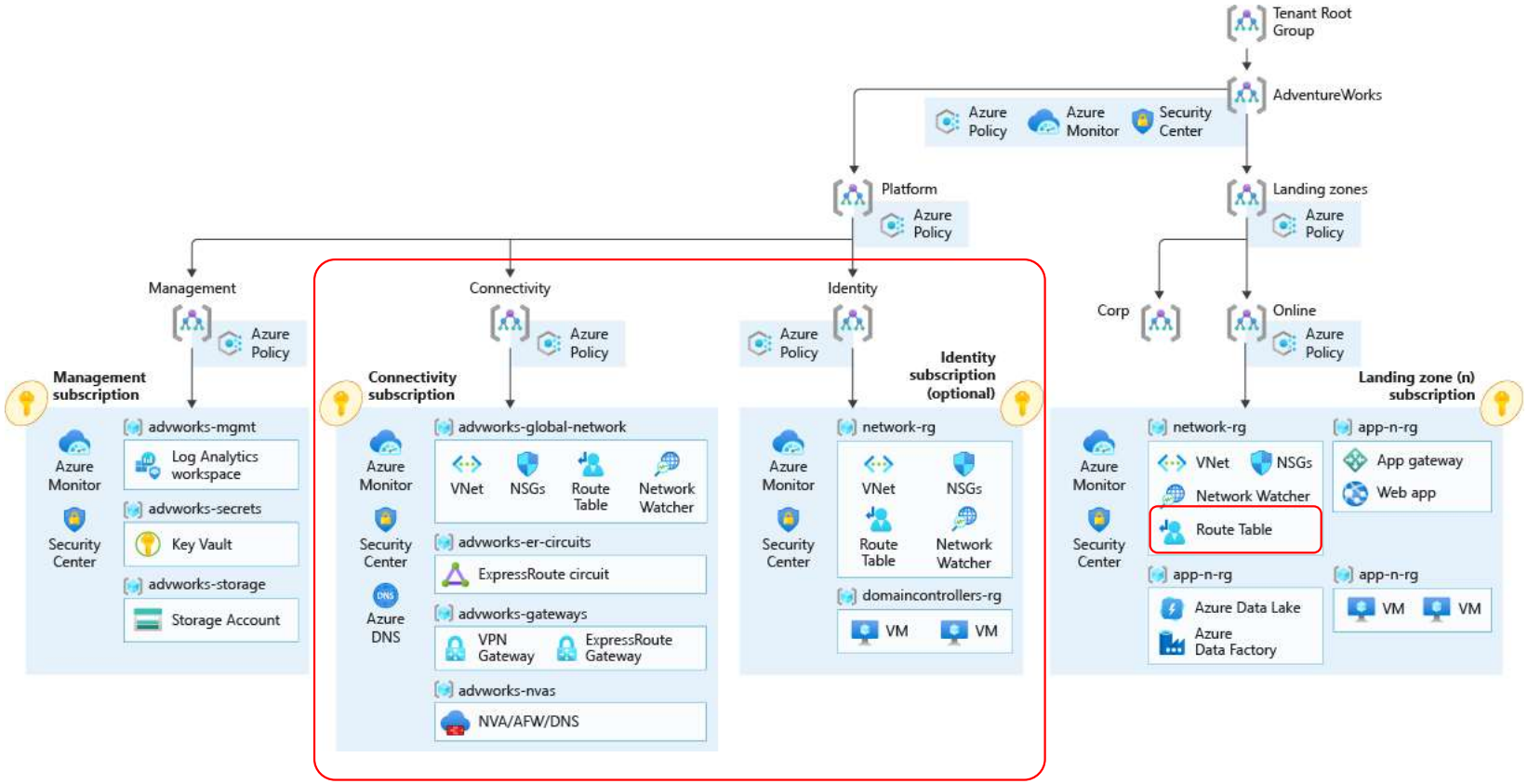
# **Enterprise-Scale** Reference Implementation
## Foundation without hybrid connectivity




Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

# **Enterprise-Scale** Reference Implementation
## Foundation with Hub and Spoke Connectivity

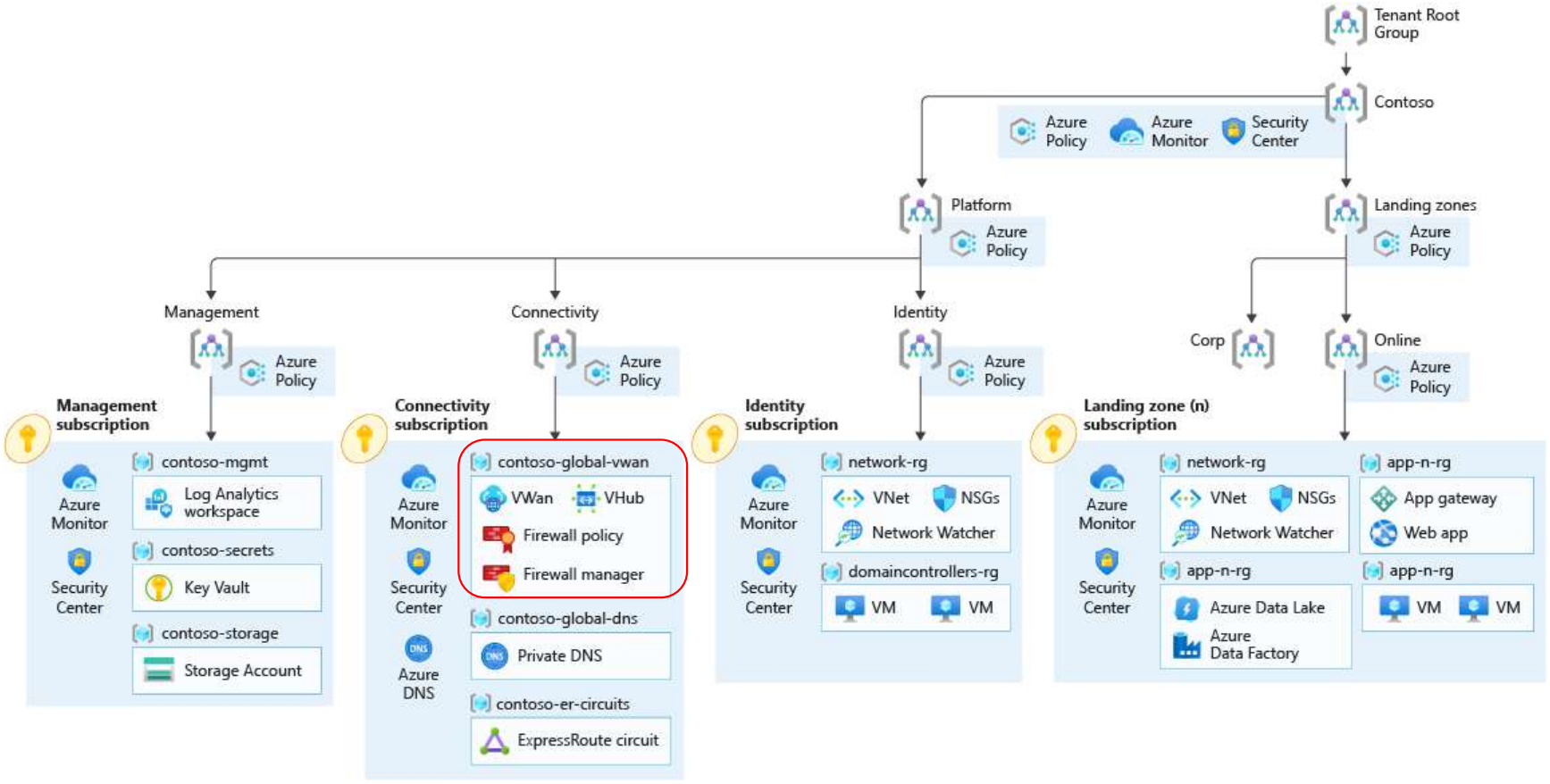
Azure Meetup BONN




Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale with hub and spoke architecture

# **Enterprise-Scale** Reference Implementation
## Foundation with Azure VWAN Connectivity

Azure Meetup BONN




Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale with hub and spoke architecture

# **Enterprise-Scale**
# Deployment and Policies

DEMO

# Enterprise-Scale and AzOps

Azure Meetup BONN

| Git->Clone->Azure/Northstar |
| --- |
| **Git -> Commit is new "az deploy"** |
| Git repository scoped at customer AAD tenant for all Azure infrastructure |
| Discover existing Azure environment as-is |
| Turn-on the lights for existing resources and configuration |

| ARM as orchestrator to declare Goal-state at all 4 scopes: Tenant -> MGs -> Subs -> RGs |
| --- |
| **E2E orchestration for "North Star" to create Landing Zones** |
| Integrated CI/CD pipeline with File->New Regions and Landing Zones i.e. subscriptions |
| Autonomous Landing Zones - enforced by Azure Policy in platform |
| Azure Engineering and platform roadmap aligned |

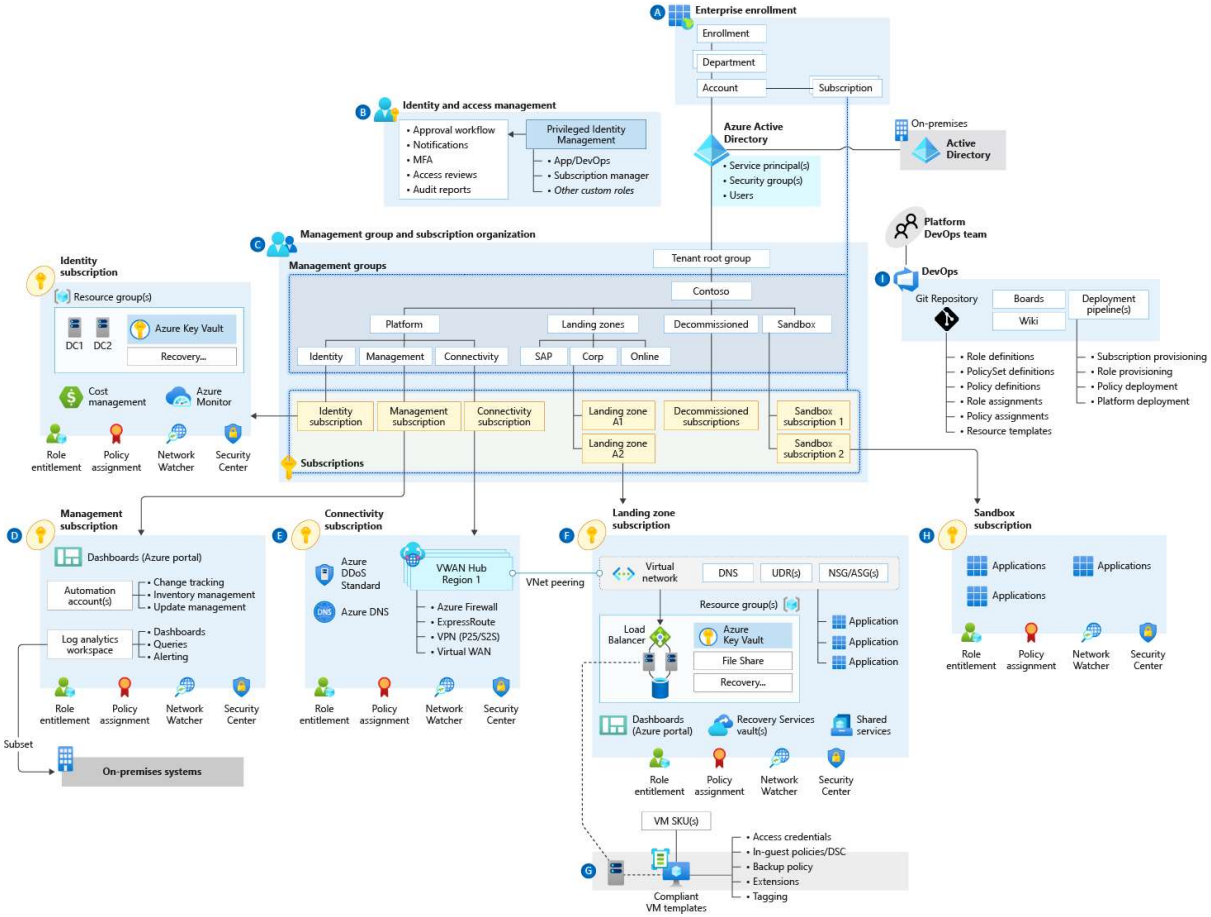
| Operationalize: Configuration Drift and Reconciliation |
| --- |
| **Azure-Native immutable configuration in Git** |
| Native platform capabilities for what-if, rollback, rollforward and complete mode |
| Inclusive of DevOps (Git) and ITPros (Portal) |
| Consistent export of all resources at all scopes across the tenant with implicit dependencies |

Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

# AzOps
## Repository and CI/CD Pipelines

DEMO

# Enterprise-Scale Architecture




Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

# Enterprise-Scale **Critical Design Areas**

Enterprise Enrollment & Azure AD Tenants

Identity & Access Management

Management Group & Subscription Organization

Network Topology & Connectivity

Management & Monitoring

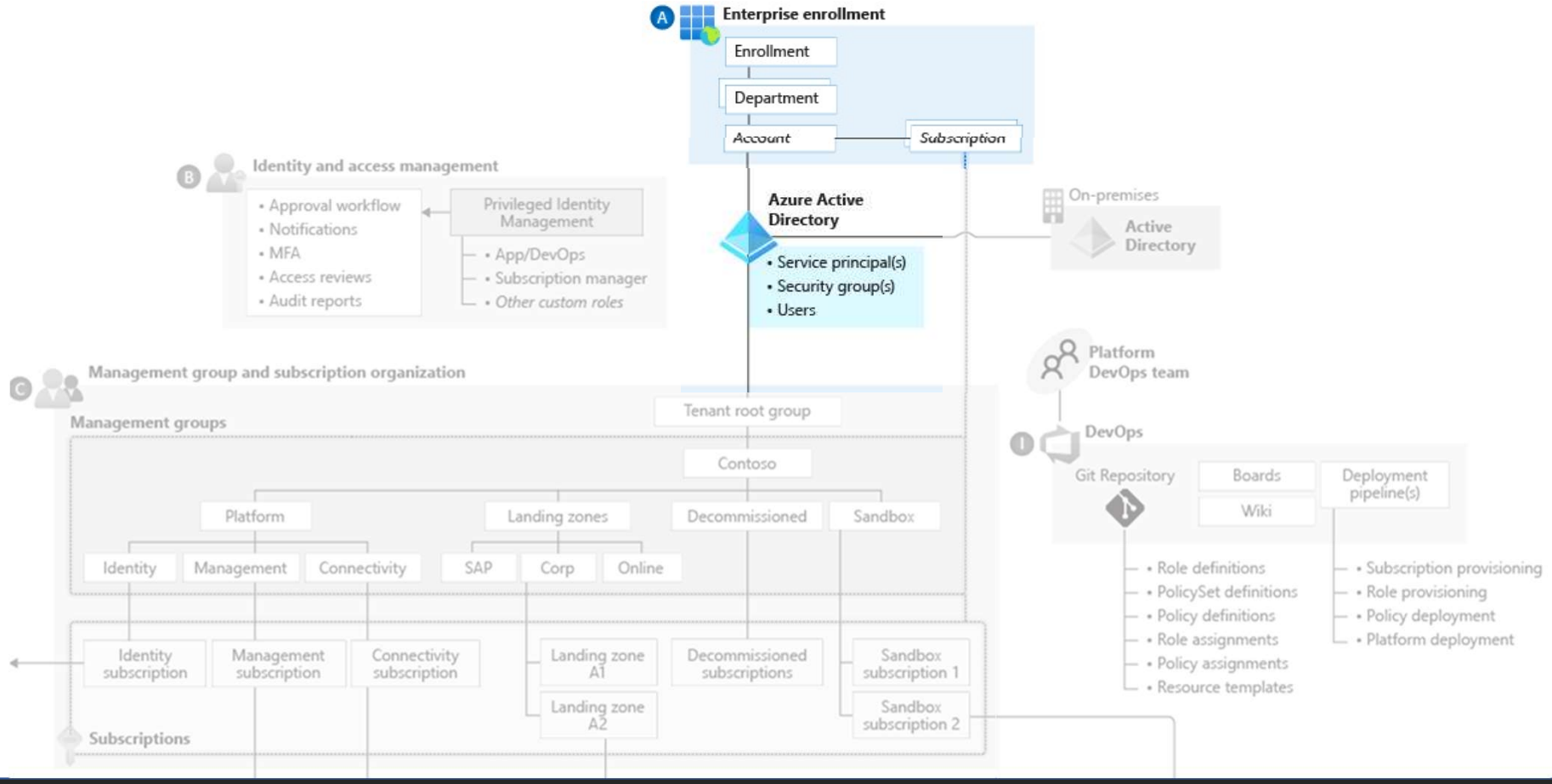
Business Continuity & Disaster Recovery

Security, Governance & Compliance

Platform Automation & DevOps

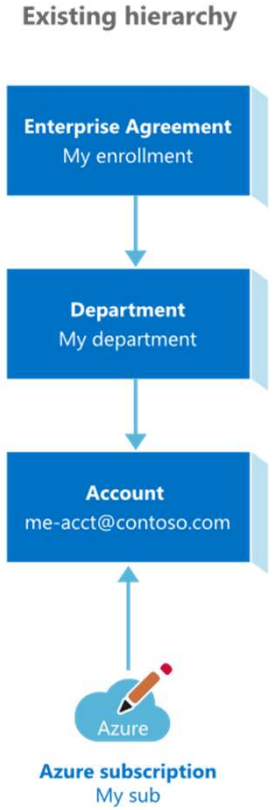
Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

# **Critical Design Areas:** Enrollment and Tenants




Source: Start with Cloud Adoption Framework enterprise-scale landing zones

# Critical Design Areas: Enrollment and Tenants
## Customer and Enterprise Agreement Hierarchy

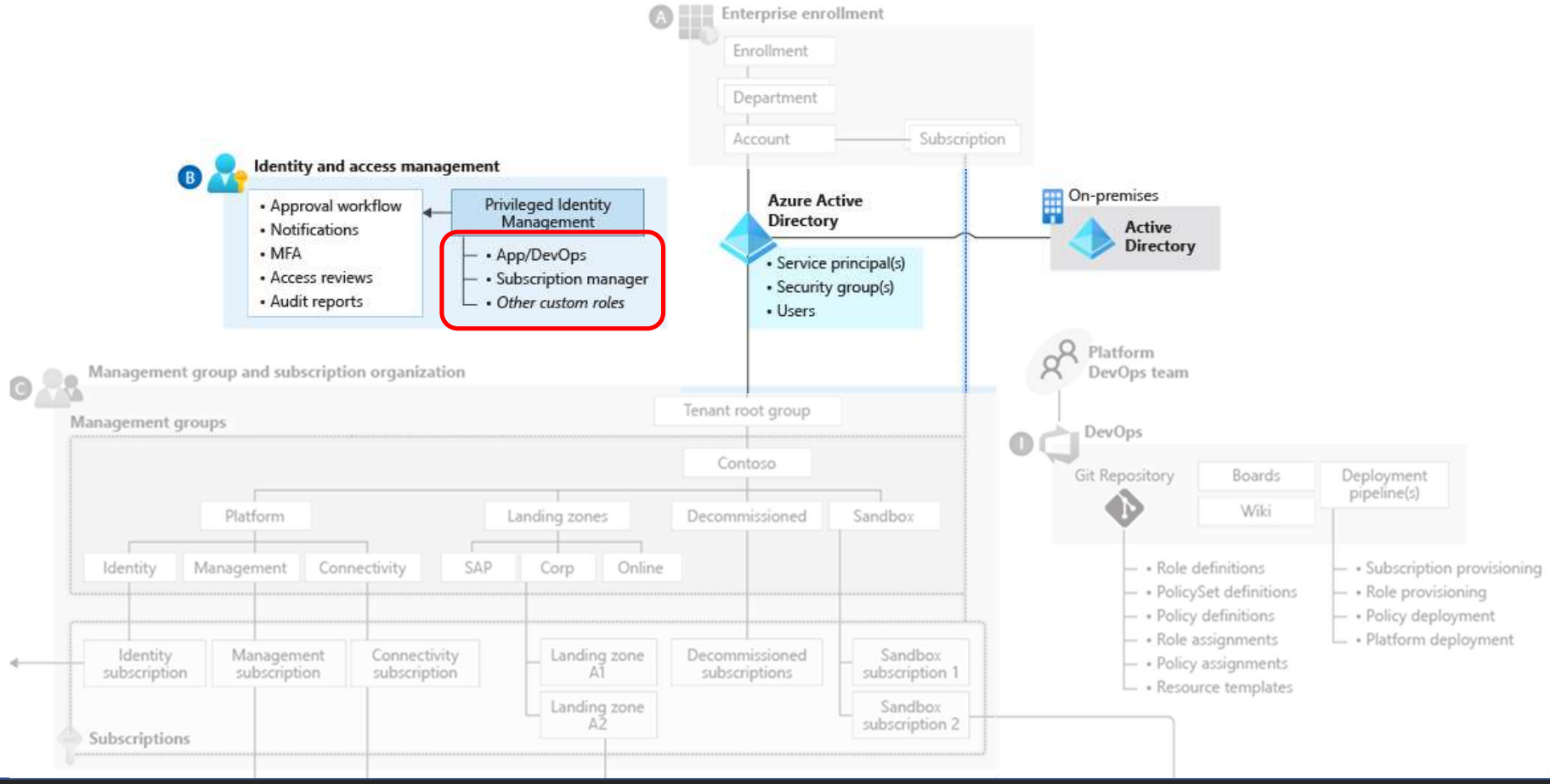



- Account Owner can manage subscription permissions
  Restrict and minimize the number of account owners within the enrollment
- No Auditing and PIM integration
  Periodically audit the EA portal to review and avoid "manual management"

→ Automation (as part of AzOps) and Account Owner as "Break Glass"

Source: Complete Enterprise Agreement tasks in your billing account for a Microsoft Customer Agreement

# **Critical Design Areas:** Identity and Access




Source: Start with Cloud Adoption Framework enterprise-scale landing zones

# **Critical Design Areas**: Identity and Access
# **Tiered Administration & Least Privilege**

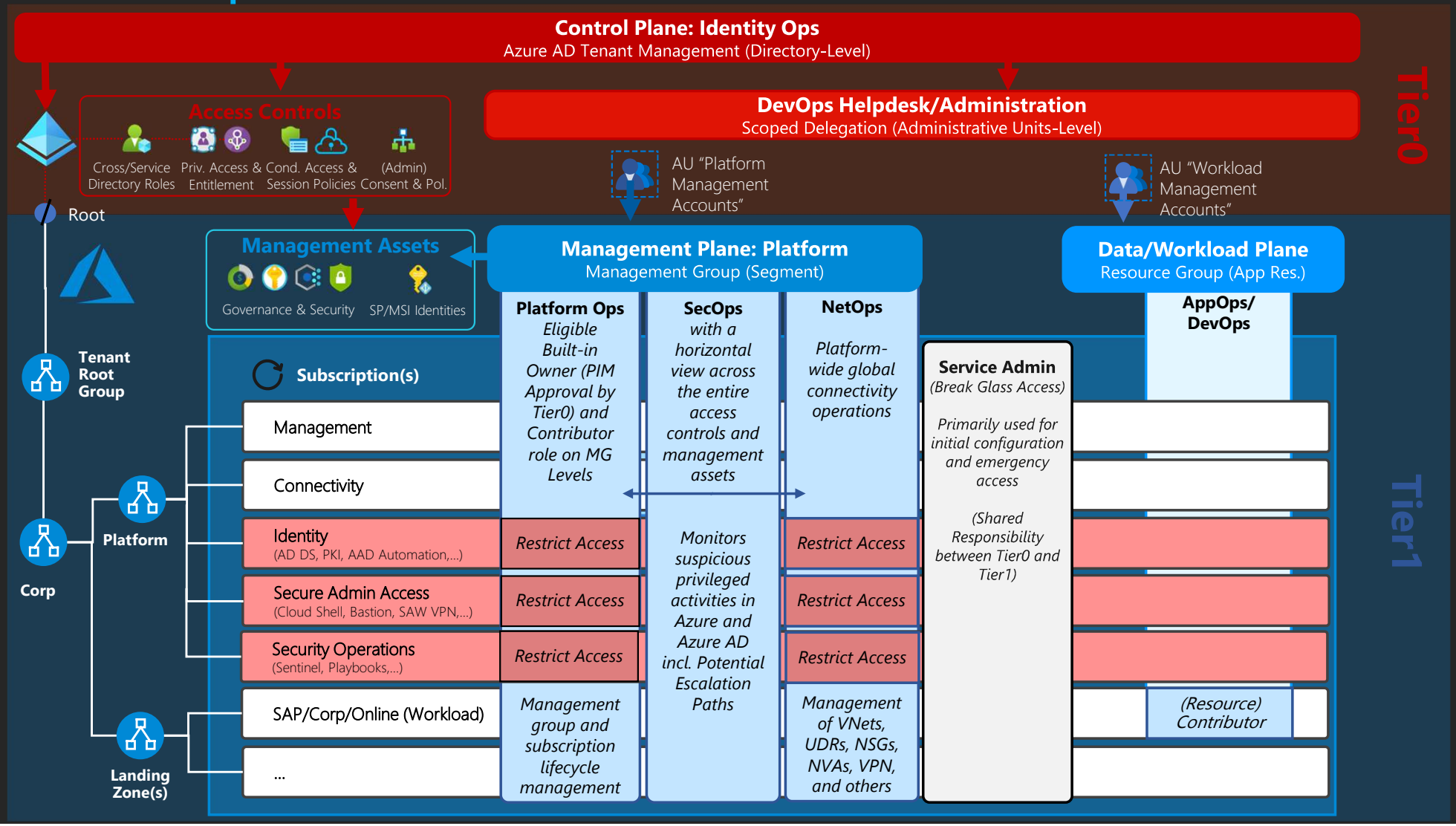
Azure Meetup BONN

„To mitigate risk of identity compromise, or bad actors, implement tiered administration and ensure that you follow principles of least privilege for Azure AD Administrator Roles."

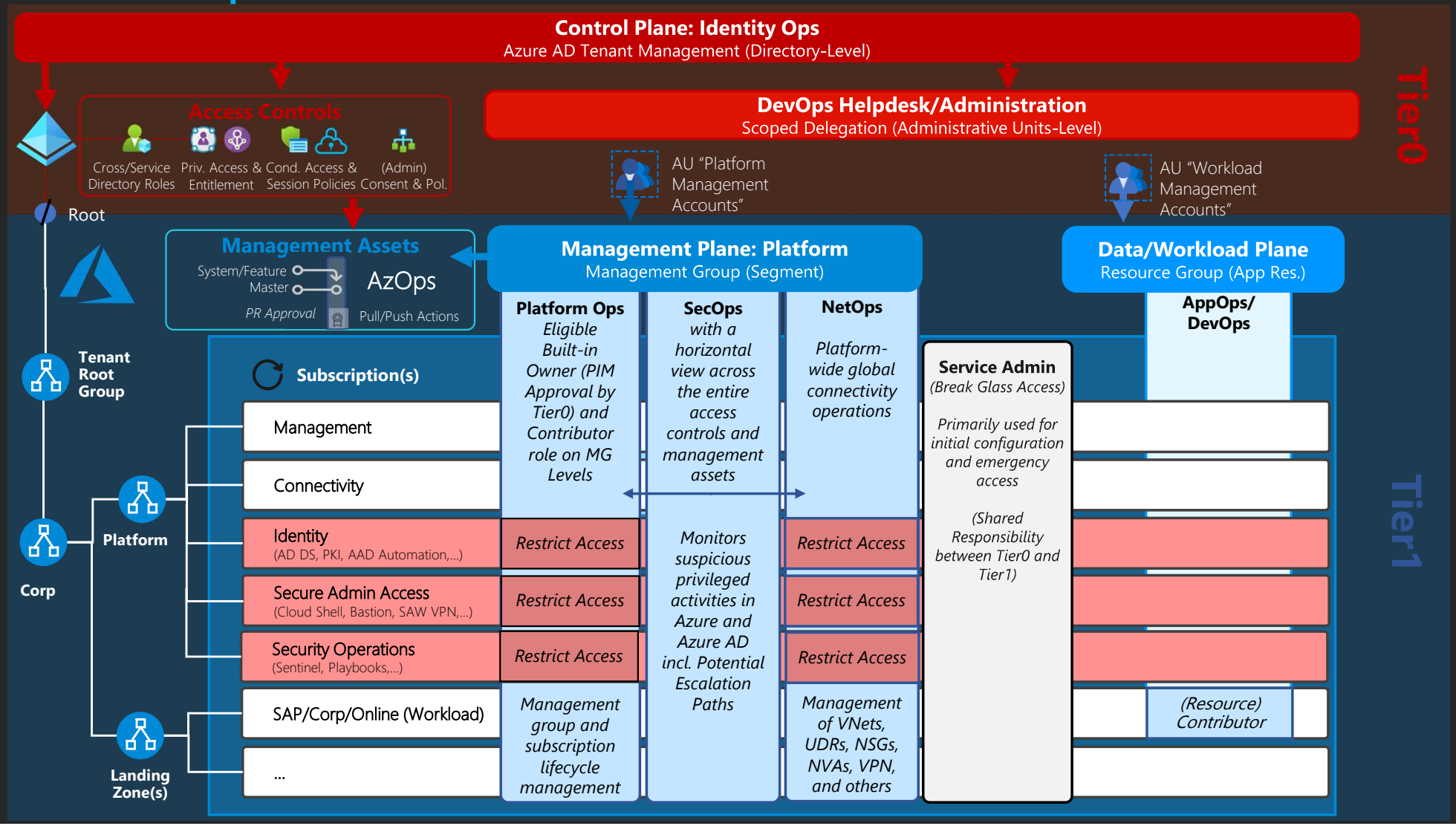
*Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)", Page 8*


Source: Securing Azure environments with Azure Active Directory

# Example of Tiered Administration Model

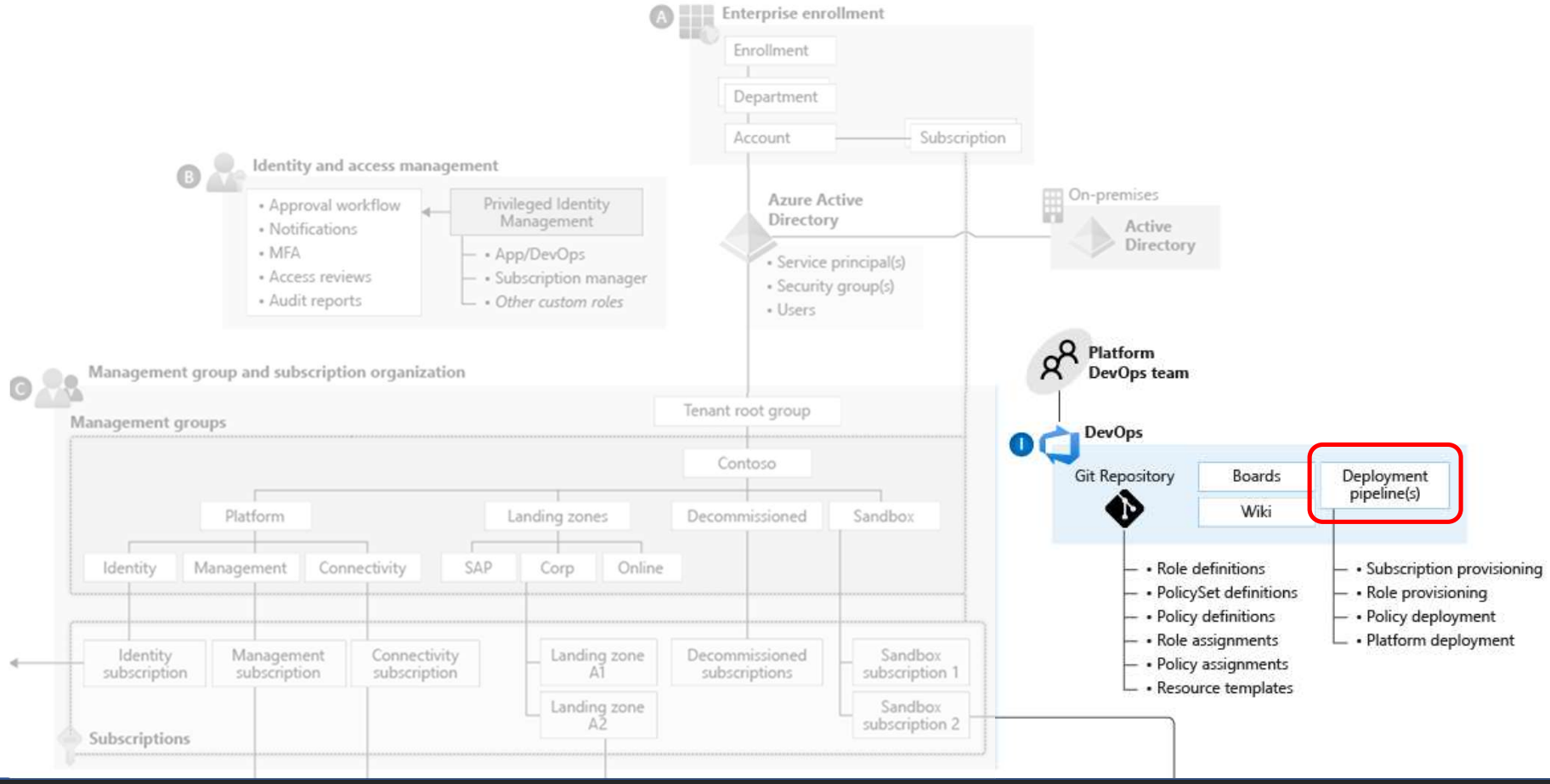


# Example of Tiered Administration Model



# **Managing access to AzOps**
## with RBAC, PIM and Entitlement Management

# **Critical Design Areas:** Identity and DevOps

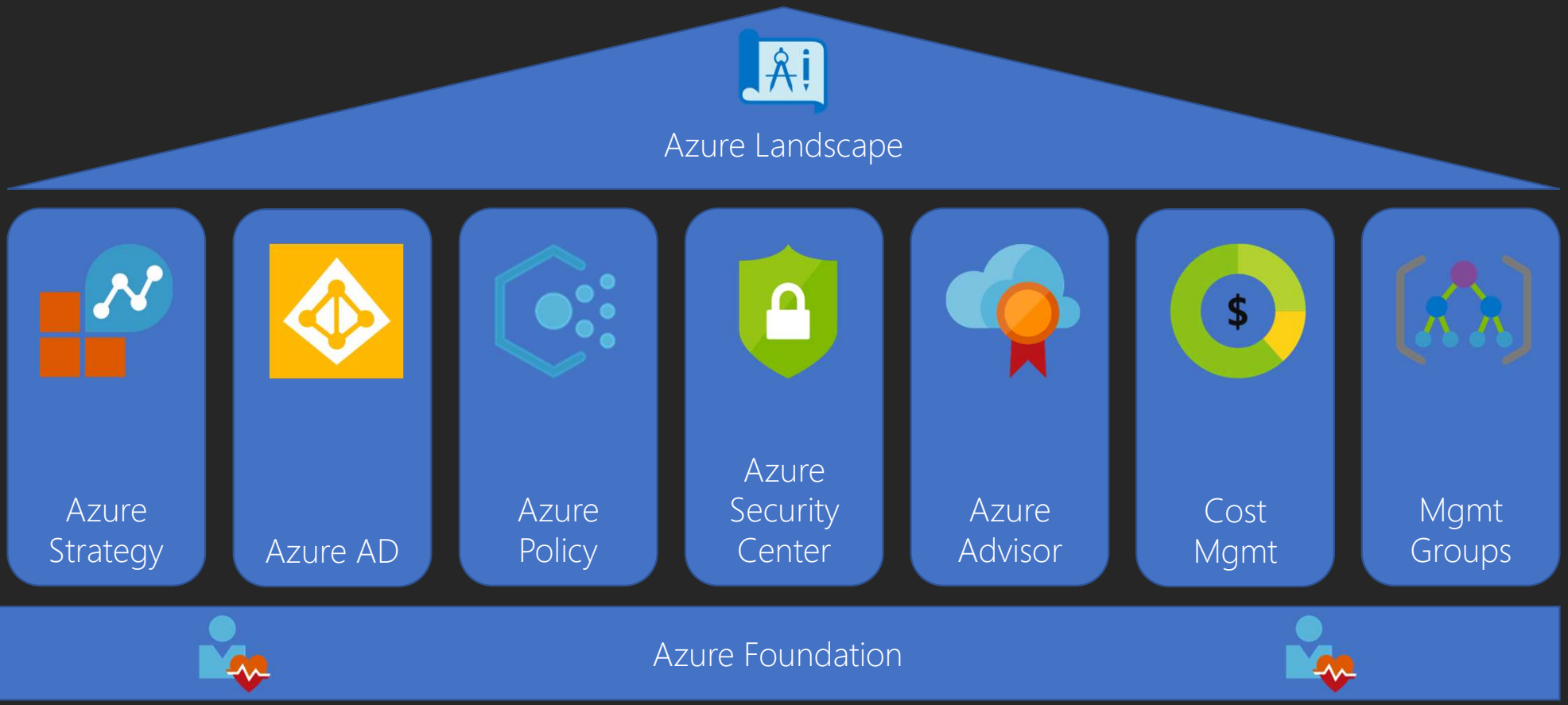



Source: Start with Cloud Adoption Framework enterprise-scale landing zones

# Links


- https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/
- https://docs.microsoft.com/en-us/azure/architecture/framework/
- https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-quickstart-center
- https://docs.microsoft.com/en-us/azure/advisor/
- https://docs.microsoft.com/en-us/azure/governance/policy
- https://www.reimling.eu/2019/03/azure-management-groups-und-blueprints-ueberblick-und-einrichtung-teil-1/
- https://aka.ms/SecurityCommunity
- https://blog.azureandbeyond.com/2020/04/24/mastering-azure-security-my-latest-adventure/

# How brings it to Azure?



# Our Recommendations


- Define a Cloud Strategy
  - Use the available Tools and Guidelines
  - Define the added value of the cloud
- Create a Team for Cloud Services of different people
- Evaluate guidelines and best practices
- Organize a regulary meeting/call for Cloud news
- Get in touch with Partners and Community for help and support


Session Slides

# Questions? ->
# Reach us via Twitter ☺


@Thomas_Live | @GregorReimling | @AzureBonn


www.cloud-architekt.net | www.reimling.eu | www.azurebonn.de