Microsoft

Enterprise-scale landing zones

Getting ready to deploy workloads on Azure

Agenda

- Azure landing zones
- What is Enterprise-scale?
- Enterprise-scale Design Principles
- Enterprise-scale Design Guidelines
- Enterprise-scale Implementation Guide
- Enterprise-scale Reference Implementation
- Resources & Next Steps

Azure landing zones

What are you going to build?

A house

A stadium

A bridge

All foundations are NOT created equal

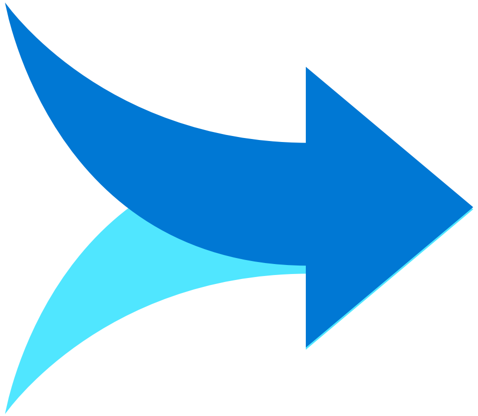
A house

A stadium

A bridge

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

Azure landing zones

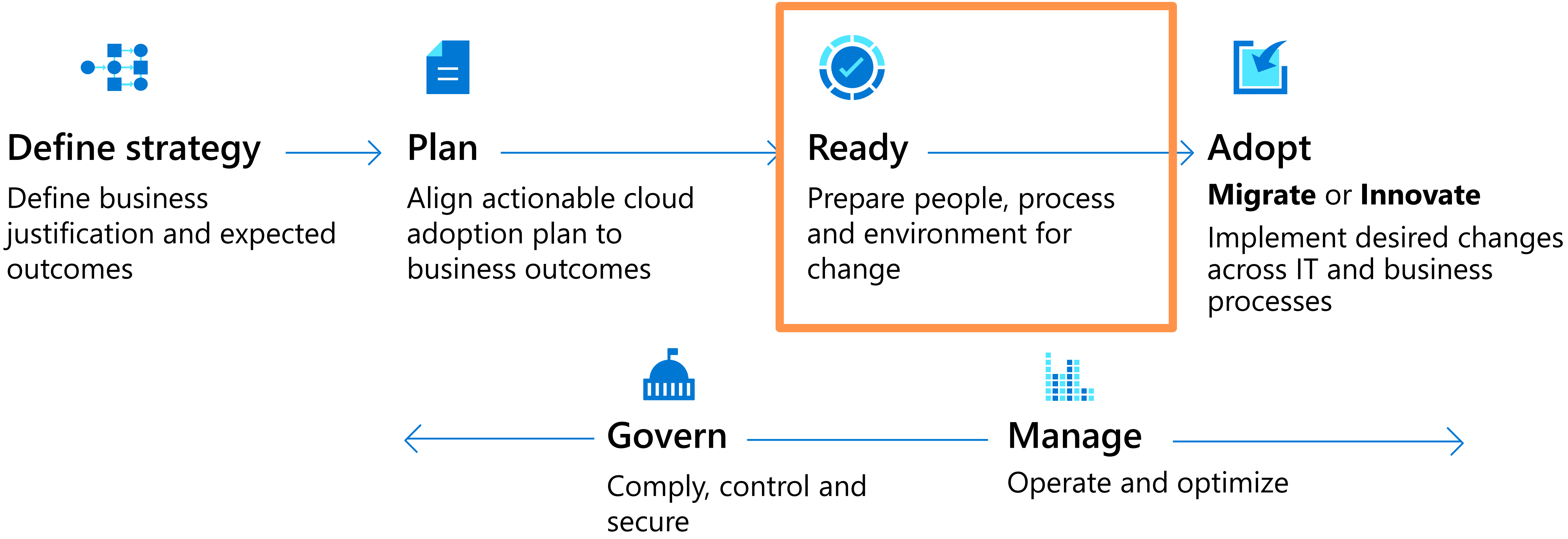
Azure landing zones help customers set up their Azure environment for scale, security, governance, networking, and identity.

Azure landing zones:

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

Microsoft Cloud Adoption Framework for Azure

Proven business and technical guidance to help customers create and implement the ***business and technology strategies*** *necessary to succeed in the cloud*



Define strategy

Define business justification and expected outcomes

Plan

Align actionable cloud adoption plan to business outcomes

Ready

Prepare people, process and environment for change

Adopt

Migrate or **Innovate**

Implement desired changes across IT and business processes

Govern

Comply, control and secure

Manage

Operate and optimize

Azure Landing Zones | Design Areas

Enterprise Enrollment

Identity

Resource Organization

Network Topology & Connectivity

Business Continuity & Disaster Recovery

Governance disciplines

Deployment options

Operations baseline

How do we get started?

Platform
Development
Velocity

Cloud
Operating
Model

How to get started?

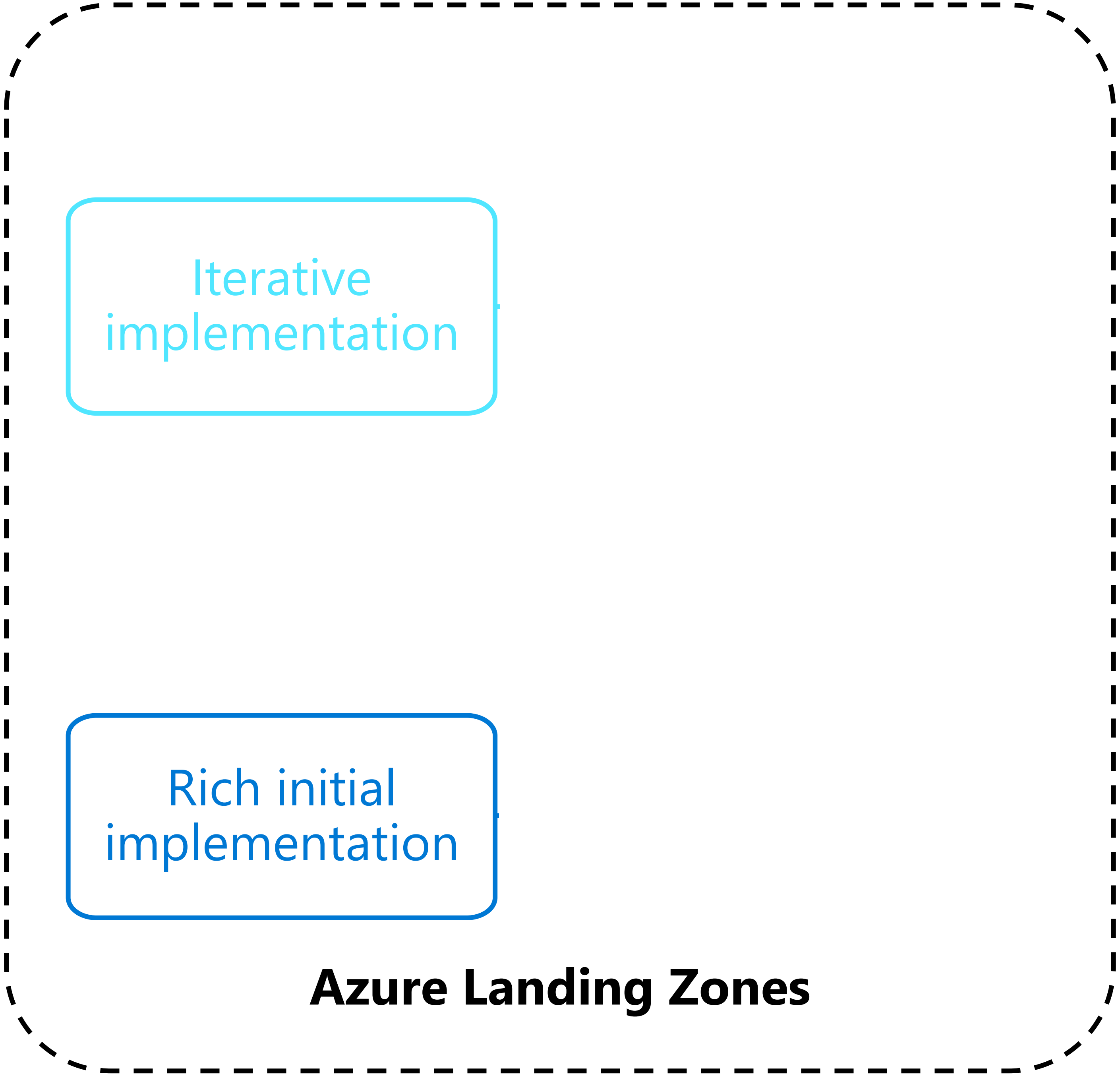
Platform Development Velocity

https://aka.ms/adopt/landingzone/cafmigrate

https://aka.ms/adopt/landingzone/caffoundation

https://aka.ms/adopt/landingzone/terraform

https://aka.ms/adopt/landingzone/enterprise-scale



Iterative implementation

Rich initial implementation

Azure Landing Zones

What is Enterprise-scale?

Key Challenges

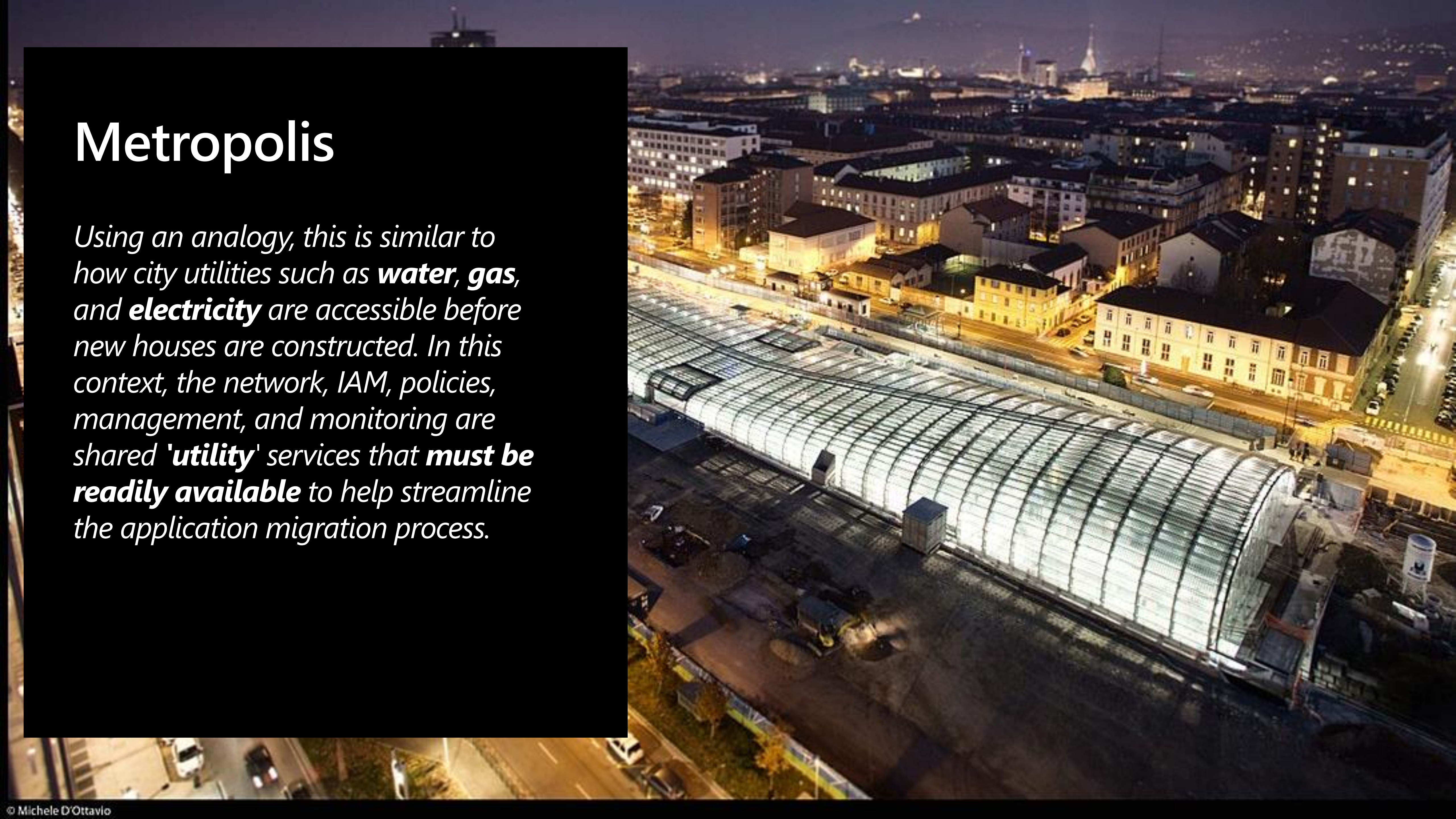
Architecture Complexity: Customers lack the required level of understanding and experience on Azure. The mismatch between on-premises infrastructure and cloud-design considerations creates dissonance and friction with respect to defining architectures and standards for their migration to the cloud. They are struggling with the translation of their requirements to Azure concepts, capabilities, constructs and security model.

Operating Compatibility: Existing approaches and functions for the traditional delivery and management of IT services are not compatible with the Azure platform and cloud operating models. When combined with a lack of skills and experience, customers are struggling to define and therefore transform their operating model to manage and support large-scale cloud infrastructure.

Lack of Trust and Desire for Control: The absence of a precise and detailed cloud architecture that is compliant with their requirements, and the lack of a well-defined operating model to support such a platform, leads IT not to trust Azure and instead strive to maintain full control. This often involves building ‘walls’ and complicated processes which ultimately get in the way of business lines adopting Azure.

Metropolis

*Using an analogy, this is similar to how city utilities such as **water**, **gas**, and **electricity** are accessible before new houses are constructed. In this context, the network, IAM, policies, management, and monitoring are shared **'utility**' services that **must be readily available** to help streamline the application migration process.*



© Michele D'Ottavio

Enterprise-scale?

Enterprise-scale is an **architecture approach and reference implementation** that enables effective **construction** and **operationalization** of landing zones on Azure, at scale and **aligned** with **Azure Roadmap** and **Microsoft Cloud Adoption Framework for Azure**.

Authoritative
Provides holistic design decision framework for Azure Platform.

Proven
Based on success of large-scale migration projects at-scale.

Prescriptive
Apply it on clearly plan and design your Azure environment.

Enterprise-scale Architecture:

- **Enterprise-scale design principles**: Principles to help/guide you customize the design.
- **Enterprise-scale design guidelines**: Guidelines (decisions and recommendations) for the 8 components of the enterprise-scale architecture
- **Enterprise-scale Implementation guide**: The way you create those things using reference implementation in GitHub and the deployment pipeline

Enterprise-scale Reference Implementation:

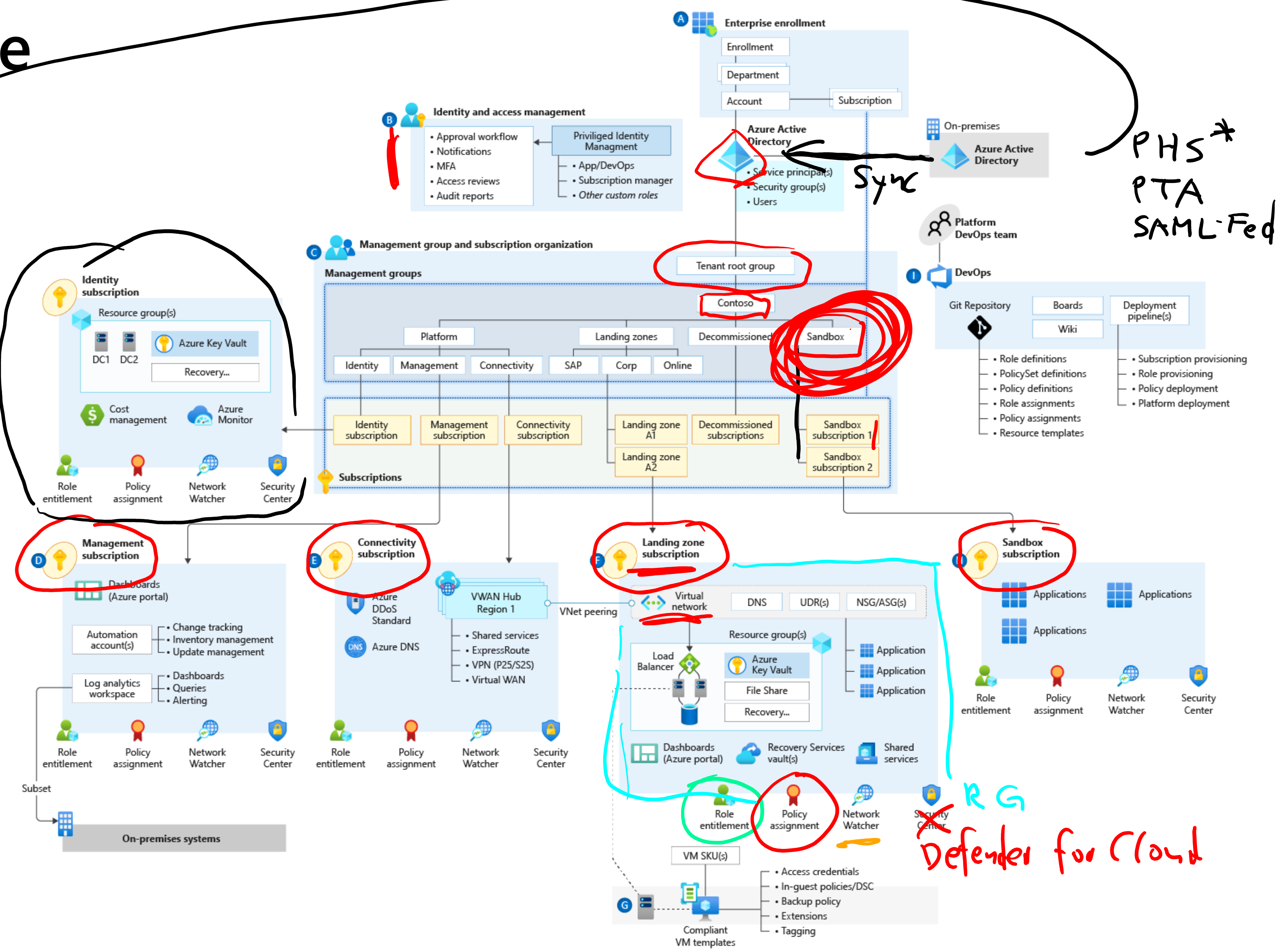
- **Enterprise-scale foundation:** A reference implementation of shared services containing network, security, identity, governance services required to construct and operationalize an enterprise-scale landing zone
- **Enterprise-scale landing zone(s):** A reference implementation of a workload environment conforming to the enterprise-scale architecture (opinionated way to implement, code)

Enterprise-scale

On Prem AD

AD-DS

Azure AD-DS



A Enterprise enrollment

Enrollment

Department

Account

Subscription

B Identity and access management

- Approval workflow
- Notifications
- MFA
- Access reviews
- Audit reports

Priviliged Identity Managment

- App/DevOps
- Subscription manager
- *Other custom roles*

Azure Active Directory

- Service principal(s)
- Security group(s)
- Users

On-premises

Azure Active Directory

Sync

PHS*

PTA

SAML-Fed

Platform DevOps team

I DevOps

Git Repository

Boards

Wiki

Deployment pipeline(s)

- Role definitions
- PolicySet definitions
- Policy definitions
- Role assignments
- Policy assignments
- Resource templates

- Subscription provisioning
- Role provisioning
- Policy deployment
- Platform deployment

C Management group and subscription organization

Management groups

Tenant root group

Contoso

Platform

Landing zones

Decommissioned

Sandbox

Identity

Management

Connectivity

SAP

Corp

Online

Subscriptions

Identity subscription

Management subscription

Connectivity subscription

Landing zone A1

Landing zone A2

Decommissioned subscriptions

Sandbox subscription 1

Sandbox subscription 2

Identity subscription

Resource group(s)

DC1

DC2

Azure Key Vault

Recovery...

Cost management

Azure Monitor

Role entitlement

Policy assignment

Network Watcher

Security Center

D Management subscription

Dashboards (Azure portal)

Automation account(s)

- Change tracking
- Inventory management
- Update management

Log analytics workspace

- Dashboards
- Queries
- Alerting

Role entitlement

Policy assignment

Network Watcher

Security Center

Subset

On-premises systems

E Connectivity subscription

Azure DDoS Standard

Azure DNS

VWAN Hub Region 1

- Shared services
- ExpressRoute
- VPN (P25/S2S)
- Virtual WAN

VNet peering

Role entitlement

Policy assignment

Network Watcher

Security Center

F Landing zone subscription

Virtual network

DNS

UDR(s)

NSG/ASG(s)

Resource group(s)

Load Balancer

Azure Key Vault

File Share

Recovery...

Application

Application

Application

Dashboards (Azure portal)

Recovery Services vault(s)

Shared services

Role entitlement

Policy assignment

Network Watcher

~~Security Center~~

RG

Defender for Cloud

VM SKU(s)

G Compliant VM templates

- Access credentials
- In-guest policies/DSC
- Backup policy
- Extensions
- Tagging

H Sandbox subscription

Applications

Applications

Applications

Role entitlement

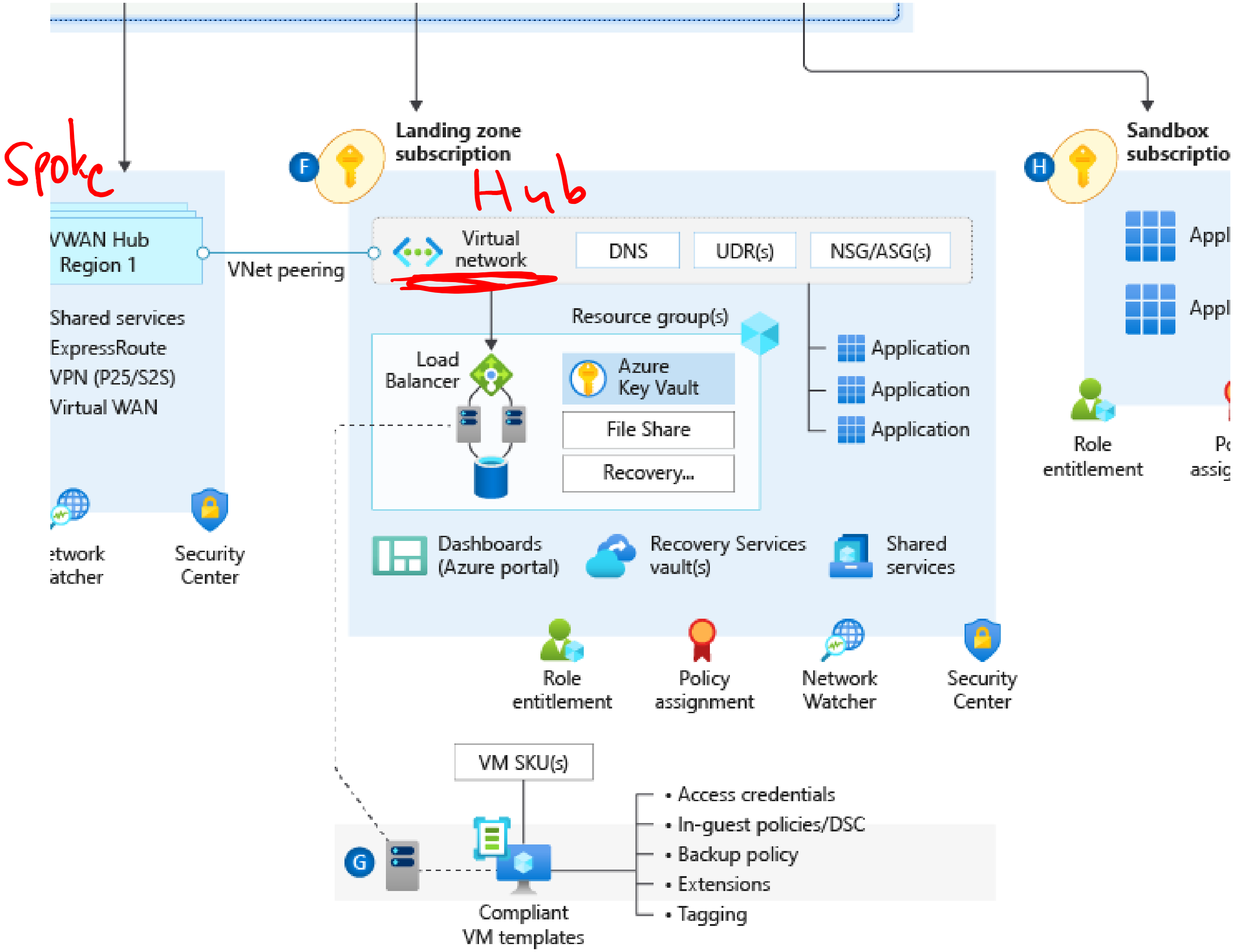
Policy assignment

Network Watcher

Security Center

Enterprise-scale landing zone(s)

The principle purpose of the “Landing Zone” is therefore to ensure that when an application or workload lands on Azure, the required “plumbing” is already in place, providing greater agility and compliance with enterprise security and governance requirements.



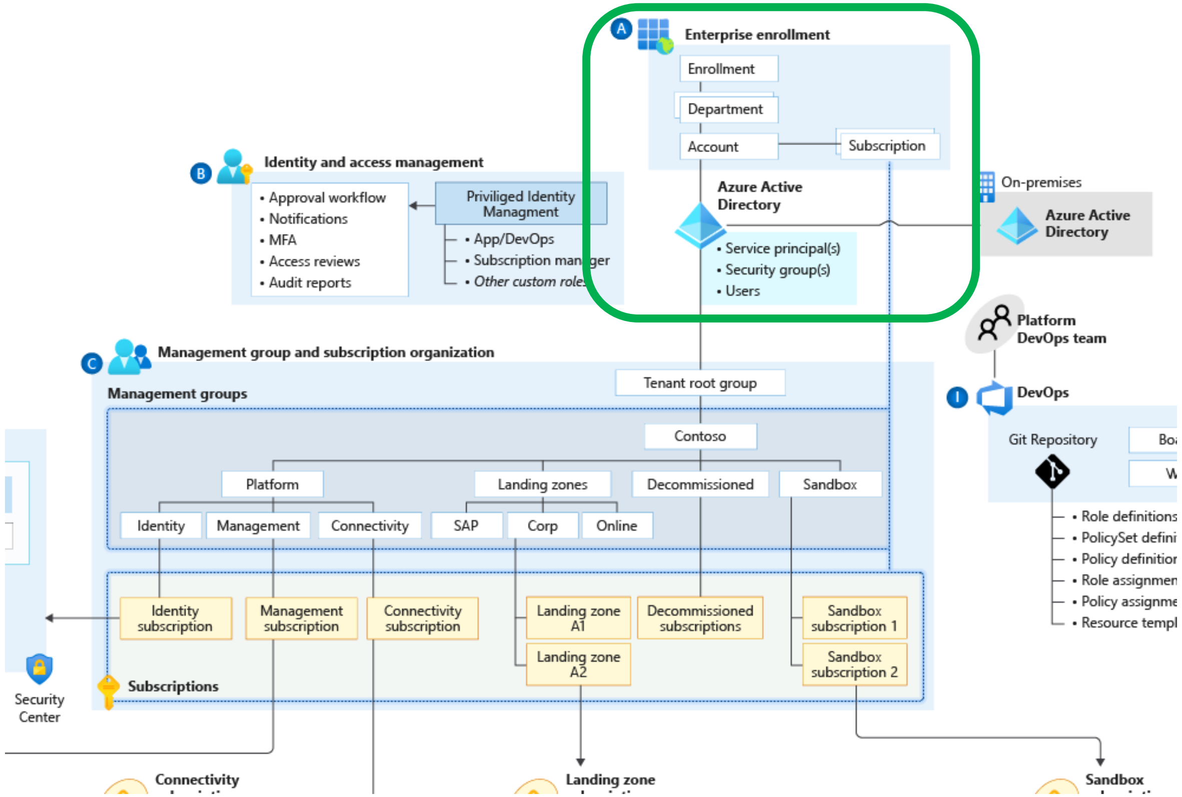
Enterprise-scale Design Guidelines

Enterprise-scale Design Guidelines

- Enterprise Enrolment & 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

Enterprise Enrolment & Azure AD Tenants

Define Azure AD Tenants



Enterprise enrolment roles links users with their **functional role** and consists of

□ Enterprise Administrator

□ Department Administrator

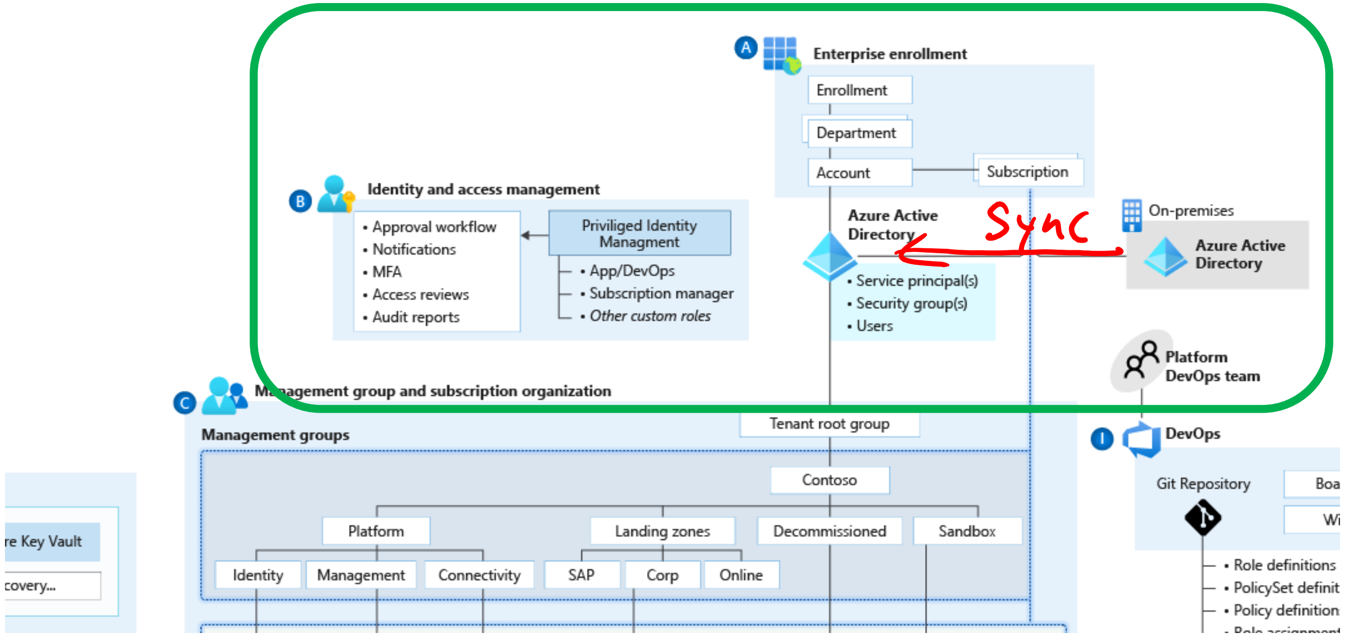
□ Account Owner

□ Service Administrator

□ Notification Contact

Identity & Access Management

Planning for Authentication Inside the Landing Zone



A critical design decision enterprise organization must make when adopting Azure is whether to:

❑ **extend** an existing on-premises identity domain into Azure

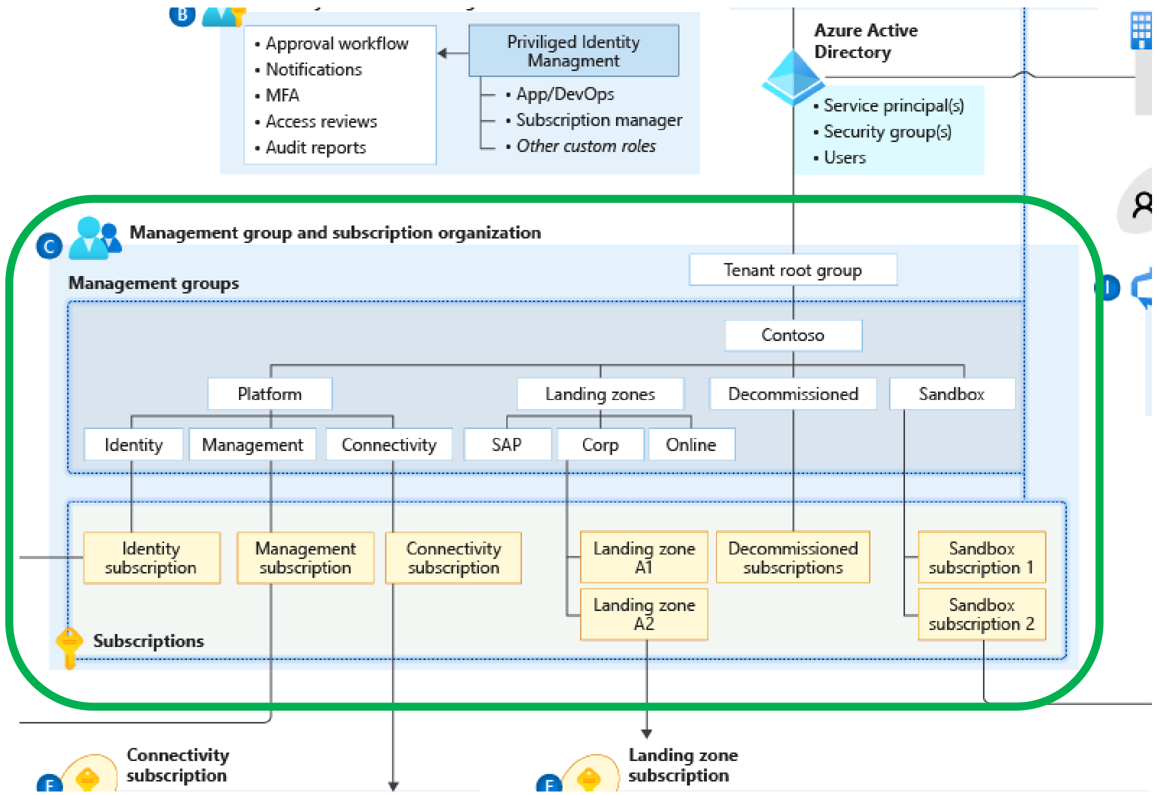
Azure AD Connect (MIM)

or

❑ **create** a brand new one △

Management Group & Subscription Organization

Define Hierarchy, Quota & Capacity, and Manage Cost



Subscription Organization and Governance

❑ Use Management Group structure, within an AAD tenant, to support org mapping

❑ Must be appropriately considered when planning Azure adoption at-scale

Configure Subscription Quota and Capacity

❑ Platform limits and quotas within the Azure platform for services

❑ Availability of required SKUs in chosen Azure regions

❑ Subscription quotas are not capacity guarantees and are per region

Establish Cost Management

❑ Potential need for chargeback models where shared PaaS services are concerned, such as ASE which may need to be shared to achieve higher density

❑ Shutdown schedule for non-prod workloads to optimise costs

UDR User Defined Route

NVA

Network Topology & Connectivity

BGP ✓

~~OSPF~~

~~RIP~~

.42 FW

next Hop

UDR

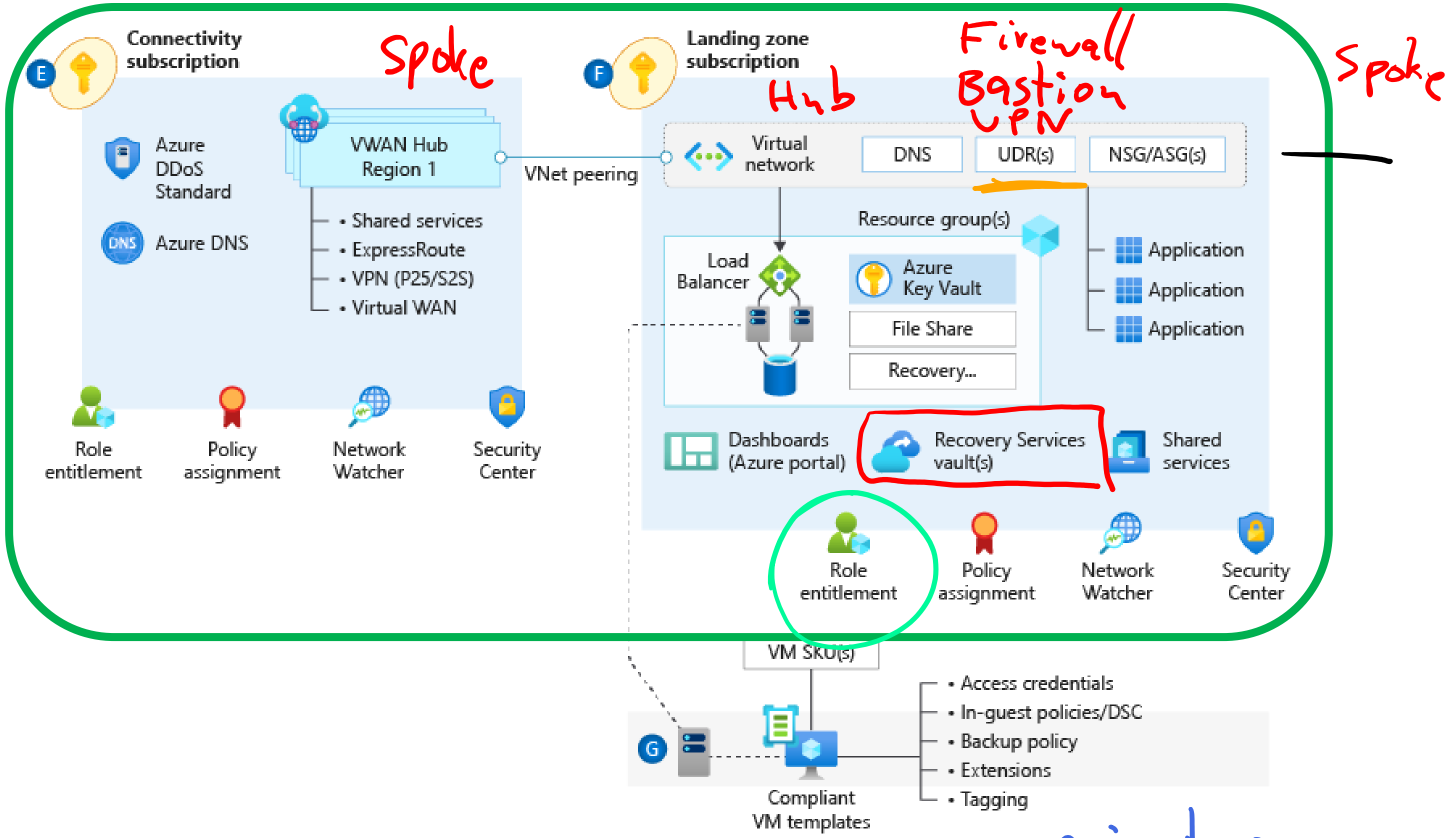
1 Default GW

.0

10.0.0.0/24

VNet

Sub IPv4 / IPv6



private DNS

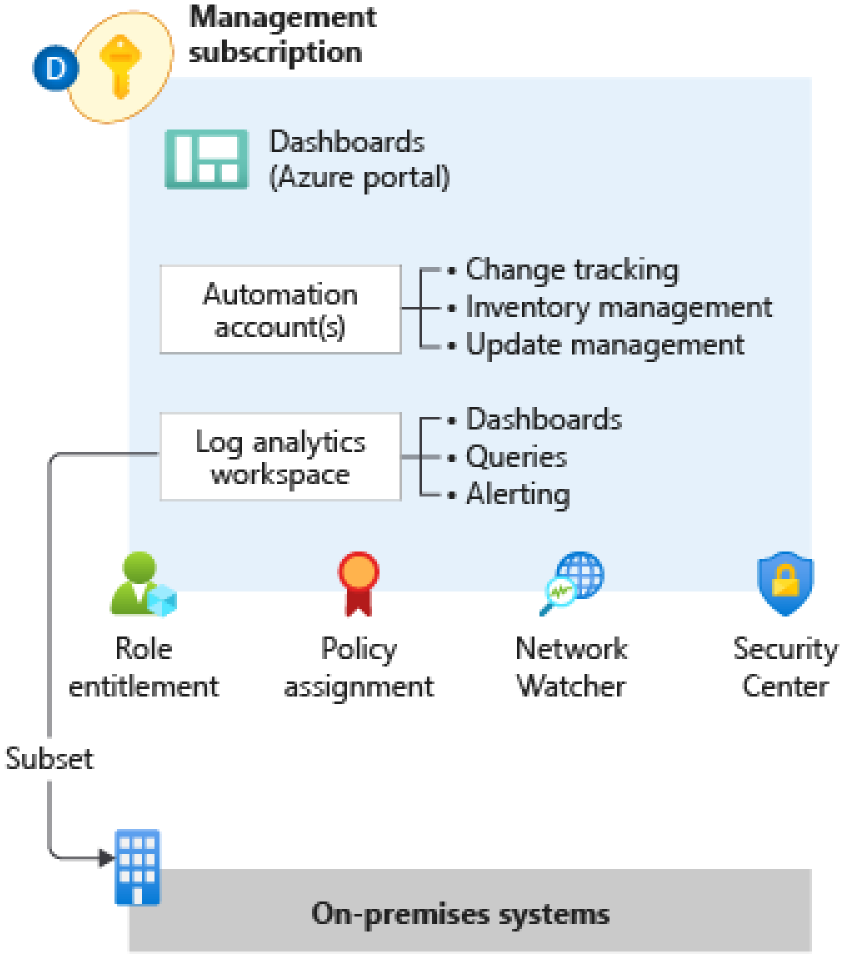
contoso.com

Consider the following design elements:

- ❑ Planning for IP Addressing
- ❑ Configure DNS
- ❑ Define an Azure Networking Topology
- ❑ Azure VWAN (Microsoft Managed)
- ❑ Traditional Azure networking (Customer Managed)
- ❑ Walkthrough – Enterprise-scale network topology (VWAN-based)
- ❑ Connectivity to Azure

Management & Monitoring

Planning for Platform & Application Management and Monitoring

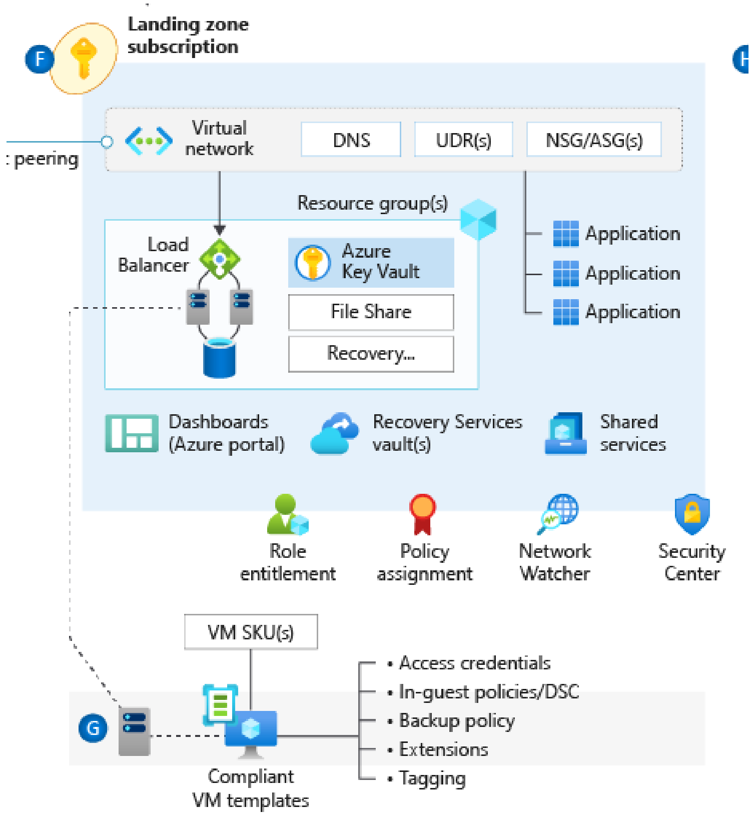


❑ **Log Analytics workspace** is an administrative boundary Security audit logging and achieving a horizontal security lens across the entire customer Azure estate

❑ **Azure data retention thresholds** and requirements for archiving

Business Continuity & Disaster Recovery

Planning for BCDR



Application and data availability requirements:

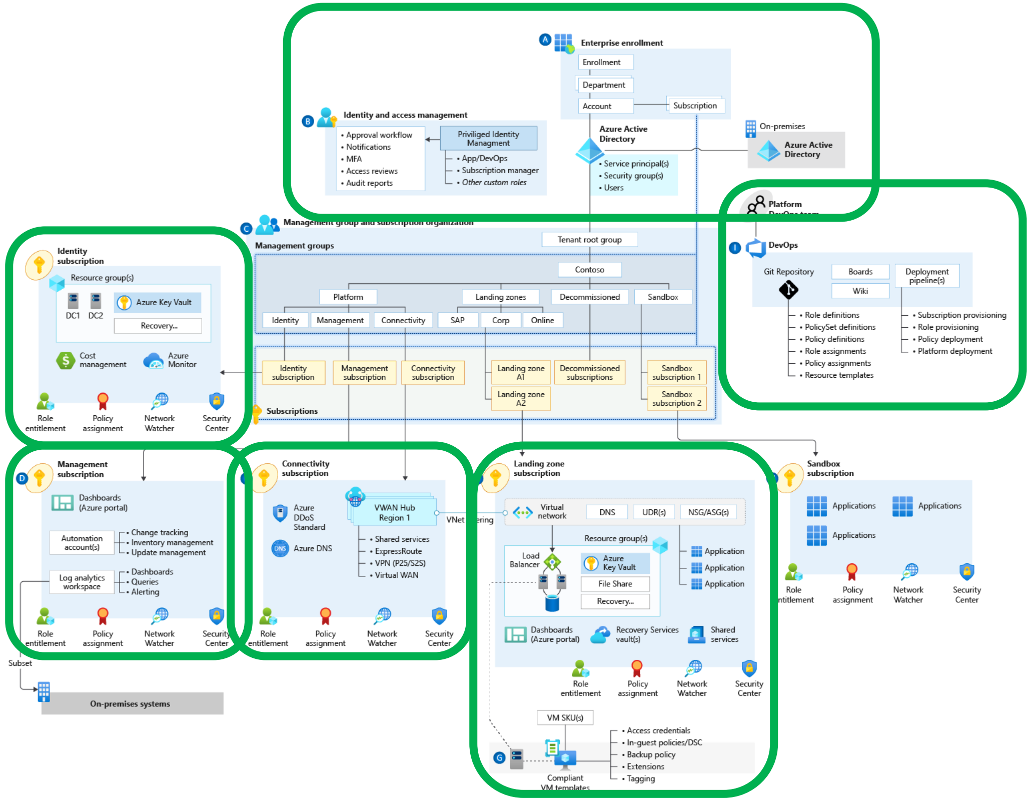
□ **BCDR for PaaS** services and the availability of native DR and HA features

□ Support for **multi-region deployments** for failover purposes

□ Application operations with **reduced functionality or degraded performance** in the presence of an outage

Security, Governance & Compliance

Define Encryption & Key Management



Subscription and scale limits as they apply to Key Vault

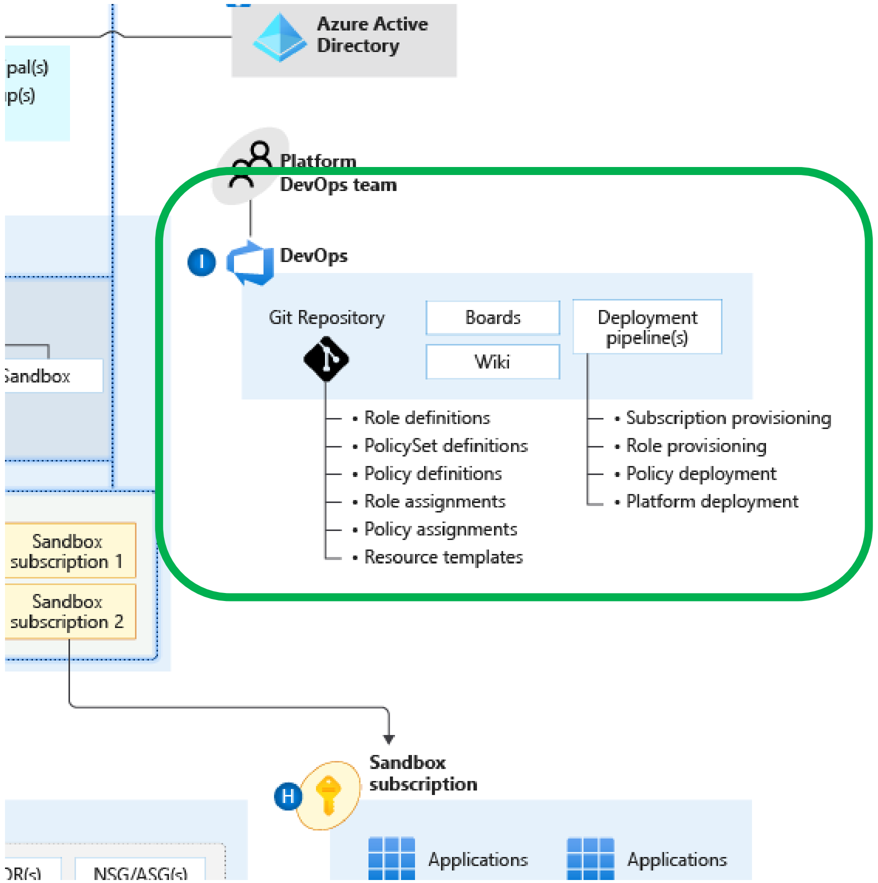
- ❑ Key Vault serves a security boundary since access permissions for keys, secrets and certificates are at the vault level
- ❑ Premium SKU can be leveraged where HSM protected keys are required

Key rotation and secret expiration

- ❑ Use a federated Key Vault model to avoid transaction scale limits
- ❑ Establish an automated process for key and certificate rotation

Platform Automation & DevOps

Planning for a DevOps Approach



❑ Where central teams are concerned, CI/CD pipelines should be used to manage policy definitions, role-definitions, policy assignments, and template galleries

The blanket application of a DevOps model will not miraculously establish capable DevOps teams.

❑ Establish a cross functional **DevOps Platform Team** to build, manage and maintain your Enterprise Scale architecture.

Thank you!