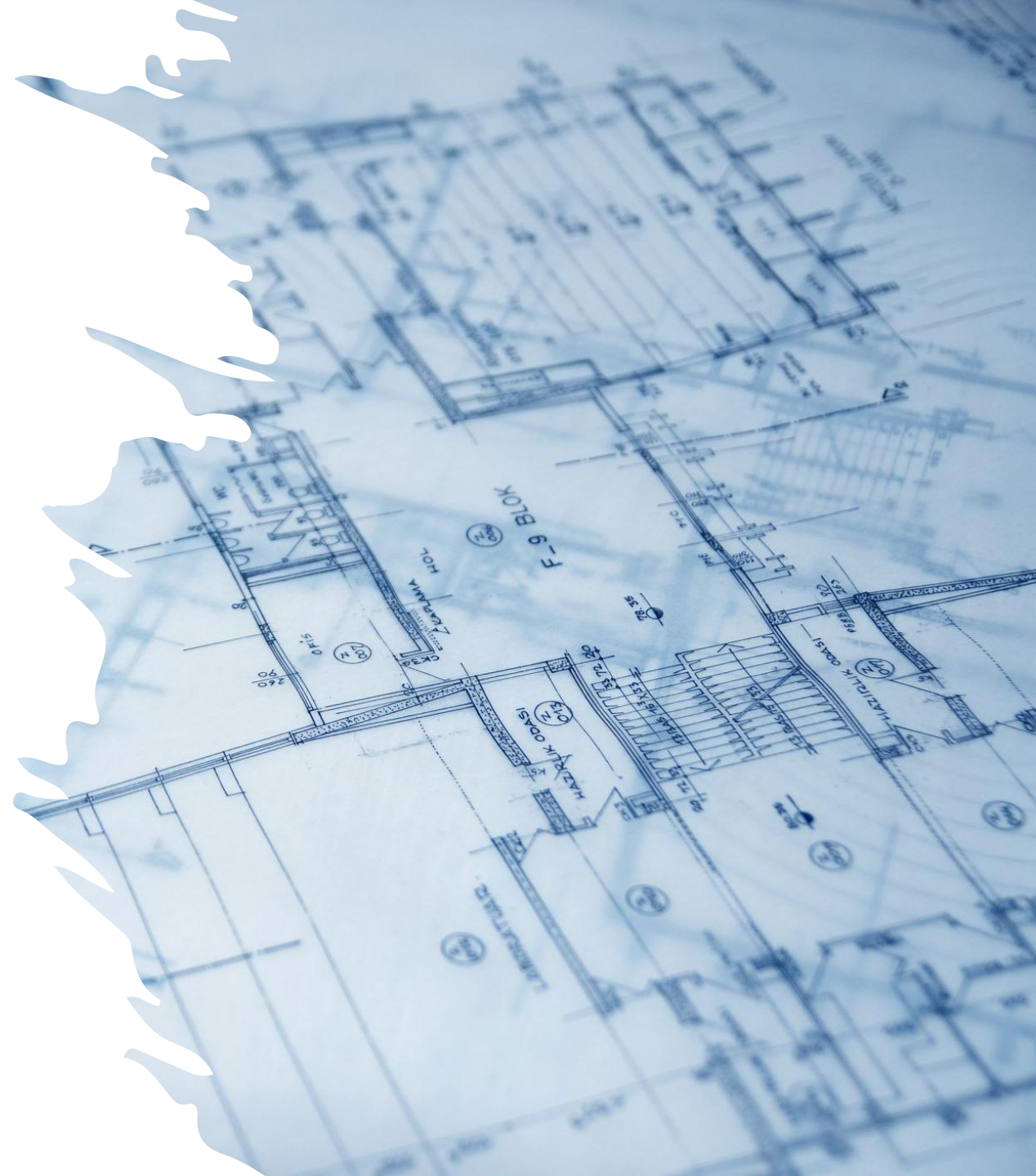# Azure AI
Landing Zone Architecture

Agenda

- (CAF) Cloud Adoption Framework
- (ALZ) Azure Landing Zone
- ALZ Key Components
- AI Landing Zone
- Implementation Steps
- Best Practices

Cloud Adoption Framework (CAF)
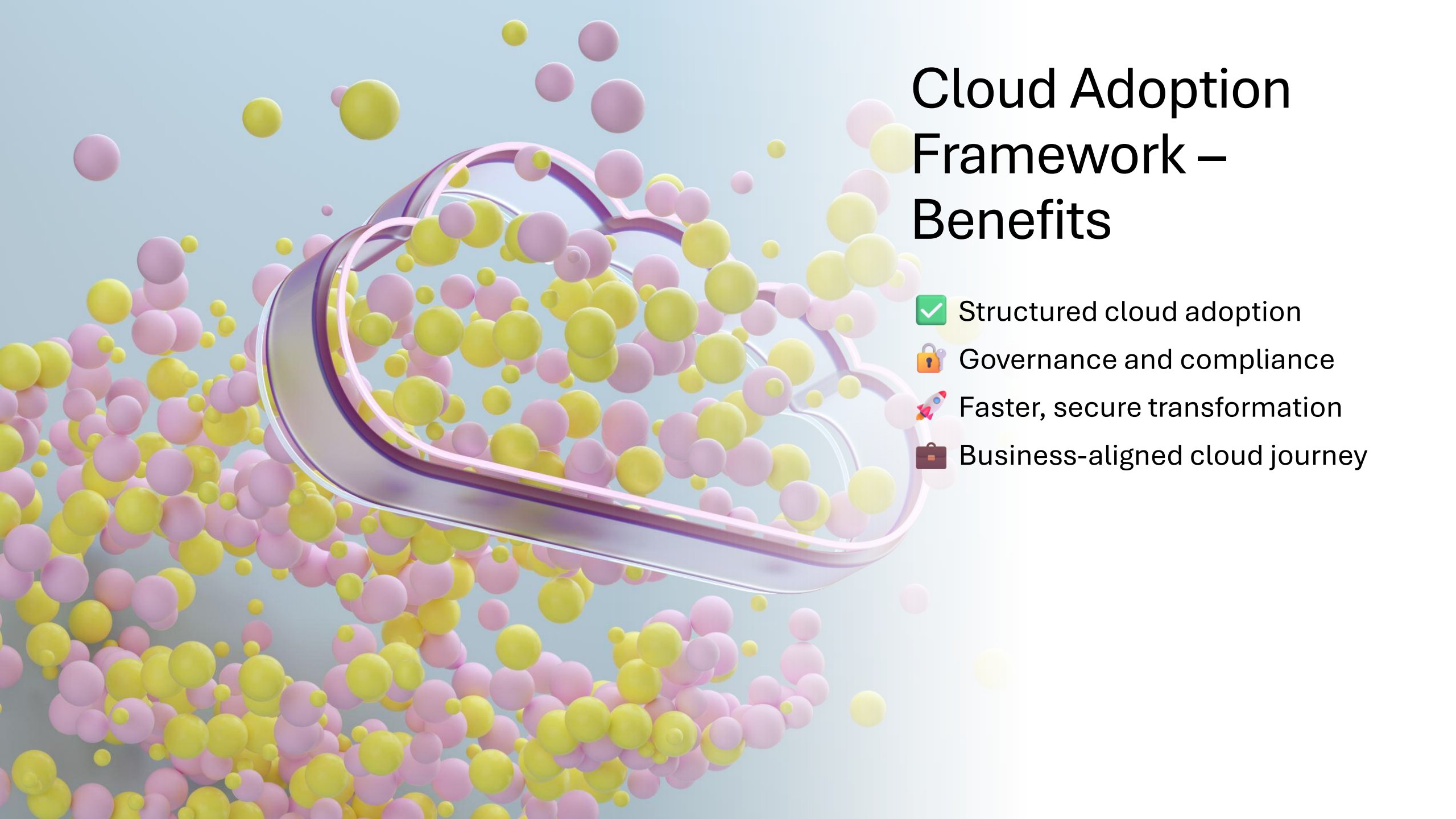
Comprehensive set of **guidance, best practices, tools, and templates** that help organizations plan and implement their cloud adoption strategy successfully.

Cloud Adoption Framework - Purpose

- Align business, people, and technology for successful cloud adoption

- Accelerate digital transformation while minimizing risk

- Provide structure across the entire cloud journey

Cloud Adoption Framework – Core Stages

CAF Methodology	Description
🚀 Strategy	Define business justification and expected outcomes
📝 Plan	Align cloud adoption plans with business goals
🛠️ Ready	Prepare your Azure environment and landing zones
🌐 Adopt	Migrate, modernize, and innovate in Azure
🛡️ Govern	Establish governance to manage risks
🔒 Secure	Protect your Azure environment
⚙️ Manage	Operate and optimize your cloud environment

Cloud Adoption Framework – Benefits

✅ Structured cloud adoption

🔒 Governance and compliance

🚀 Faster, secure transformation

💼 Business-aligned cloud journey

How ALZ fits into CAF

ALZ – Practical implementation of Ready Stage

Azure Landing Zone

Well-architected and governed foundation in Microsoft Azure that includes essential building blocks like networking, identity, and security policies to support your cloud adoption journey

A Enterprise Agreement/Microsoft Customer Agreement

- Enrollment/Billing account
- Department/Billing profile
- Account/Invoice section
- Subscription

Microsoft Entra ID
- Service principals
- Security groups
- Users

On-premises
Active Directory Domain Services

B Identity and access management
- Approval workflow
- Notifications
- Multifactor authentication
- Access reviews and packages
- Audit reports

Privileged identity management
- App/DevOps
- Subscription manager
- Other custom roles

D Management subscription

Dashboards (Azure portal)

Log Analytics workspace
For platform logs
- Dashboards
- Queries
- Alerting
- Change tracking
- Inventory management

C Management group and subscription organization

Management group
- Tenant root group
- Contoso
  - Platform
    - Management
    - Identity
    - Connectivity
  - Landing zones
    - Corp
    - Online
  - Decommissioned
  - Sandbox

Platform DevOps team

I DevOps
Git repository
- Boards
- Deployment pipelines
- Wiki

- Role definitions
- Policy set definitions
- Policy definitions
- Role assignments
- Policy assignments
- Resource templates

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

Subset

On-premises systems

AMBA-ALZ Action Groups / AMBA-ALZ Alerts / Cost Management / Role assignment / Policy assignment / Network Watcher / Defender for Cloud / Azure Update Manager

Subscriptions

- Management subscription
- Identity subscription
- Connectivity subscription
- Landing zone A1 subscription
- Landing zone P1 subscription
- Landing zone A2 subscription
- Decommissioned subscription
- Sandbox subscription 1
- Sandbox subscription 2

Identity subscription

Virtual network region 1 — DNS — UDRs — NSGs/ASGs

Resource groups

DC1 DC2 DC3 **OR** Microsoft Entra ID Domain Services

Recovery Services vault

Virtual network peering

E Connectivity subscription

Azure DDoS Protection
Azure DNS

Azure DNS Private Resolver
VPN/ExpressRoute gateways
Azure Firewall

Hub virtual network region 1

Virtual network peering

F Landing zone A2 subscription

Virtual network region 1 — DNS — UDRs — NSGs/ASGs
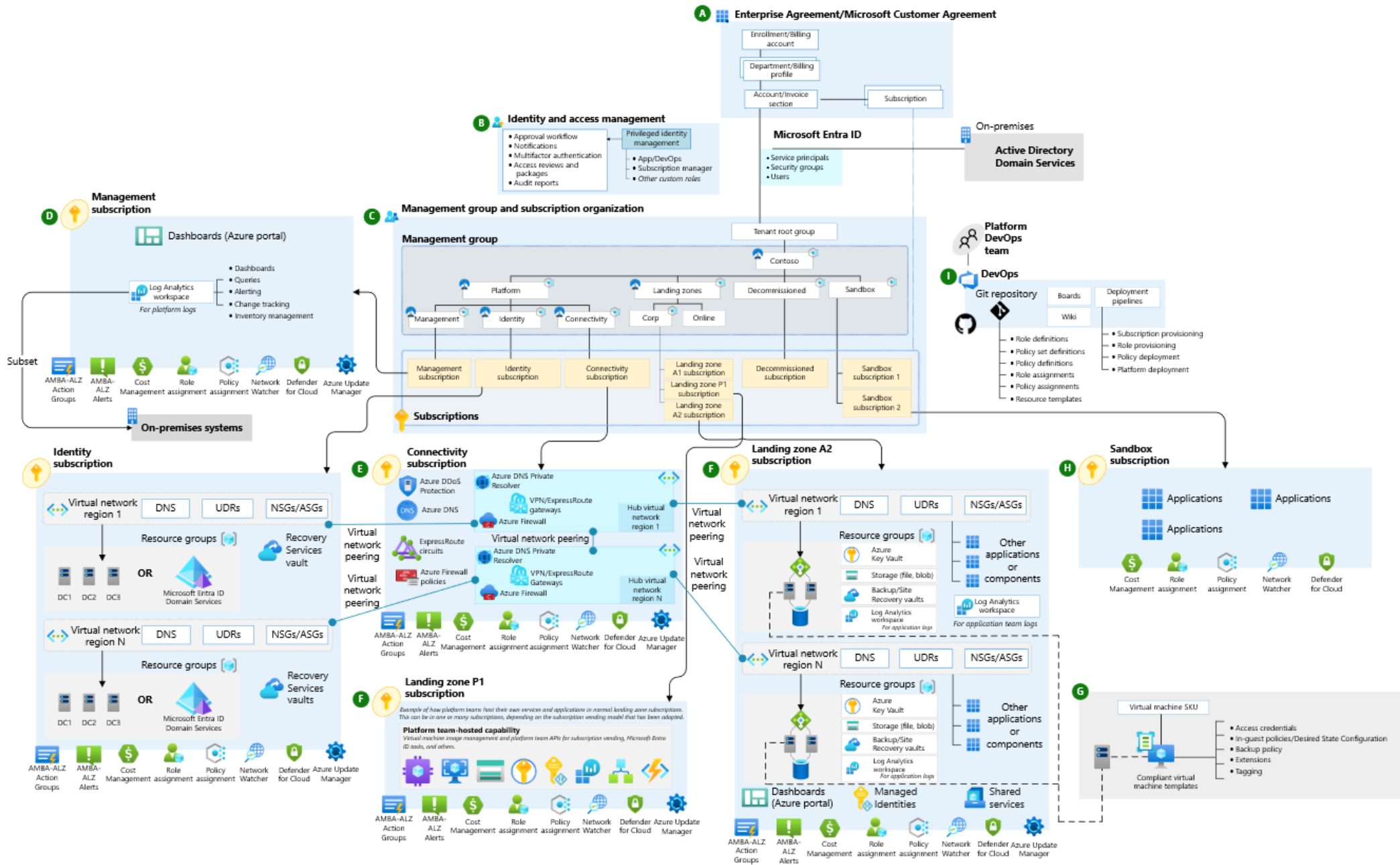
Resource groups
- Azure Key Vault
- Storage (file, blob)
- Backup/Site Recovery vaults
- Log Analytics workspace *For application logs*

Other applications or components

H Sandbox subscription

Applications   Applications
Applications

Cost Management / Role assignment / Policy assignment / Network Watcher / Defender for Cloud

Virtual network region N — DNS — UDRs — NSGs/ASGs

Resource groups

DC1 DC2 DC3 **OR** Microsoft Entra ID Domain Services

Recovery Services vaults

ExpressRoute circuits

Virtual network peering

Azure Firewall policies

Virtual network peering

Azure DNS Private Resolver
VPN/ExpressRoute Gateways
Azure Firewall

Hub virtual network region N

Virtual network peering

Virtual network region N — DNS — UDRs — NSGs/ASGs

Resource groups
- Azure Key Vault
- Storage (file, blob)
- Backup/Site Recovery vaults
- Log Analytics workspace *For application logs*

Other applications or components

G Virtual machine SKU

Compliant virtual machine templates
- Access credentials
- In-guest policies/Desired State Configuration
- Backup policy
- Extensions
- Tagging

AMBA-ALZ Action Groups / AMBA-ALZ Alerts / Cost Management / Role assignment / Policy assignment / Network Watcher / Defender for Cloud / Azure Update Manager

F Landing zone P1 subscription

Example of how platform teams host their own services and application in normal landing zone subscriptions. This can be one or many subscriptions, depending on the subscription vending model that has been adopted.

Platform team-hosted capability
Virtual machine image management and platform team APIs for subscription vending, Microsoft Entra ID tools, and others.

AMBA-ALZ Action Groups / AMBA-ALZ Alerts / Cost Management / Role assignment / Policy assignment / Network Watcher / Defender for Cloud / Azure Update Manager

Dashboards (Azure portal)   Managed Identities   Shared services

AMBA-ALZ Action Groups / AMBA-ALZ Alerts / Cost Management / Role assignment / Policy assignment / Network Watcher / Defender for Cloud / Azure Update Manager

Microsoft Azure

Version: 2025-02-19

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

Azure Landing Zone

Pre-configured, secure, and scalable Azure environment that serves as the foundation for deploying and operating workloads in the cloud. It incorporates governance, security, networking, identity, and management best practices.

Azure Landing Zone

- Environment that follows key design principles across certain design areas

- Accommodate all application portfolios and enable application migration, modernization, and innovation at scale

- Uses subscriptions to isolate and scale application resources and platform resources

Azure Landing Zone - Purpose

- Provide a ready-to-use cloud environment aligned with organizational policies

- Accelerate workload deployment with built-in controls

- Establish a foundation for scalability, compliance, and operations

Azure Landing Zone - Benefits

✅ Accelerated and consistent deployment

🔄 Repeatable infrastructure patterns

📏 Built-in compliance and policy enforcement

🧊 Integration with DevOps and CI/CD pipelines

Azure Landing Zone – Types of Landing Zones

- Start Small and Expand – Minimal viable zone for early adoption

- Enterprise-Scale – Comprehensive, scalable, modular architecture

- Custom – Tailored to specific organizational or industry needs
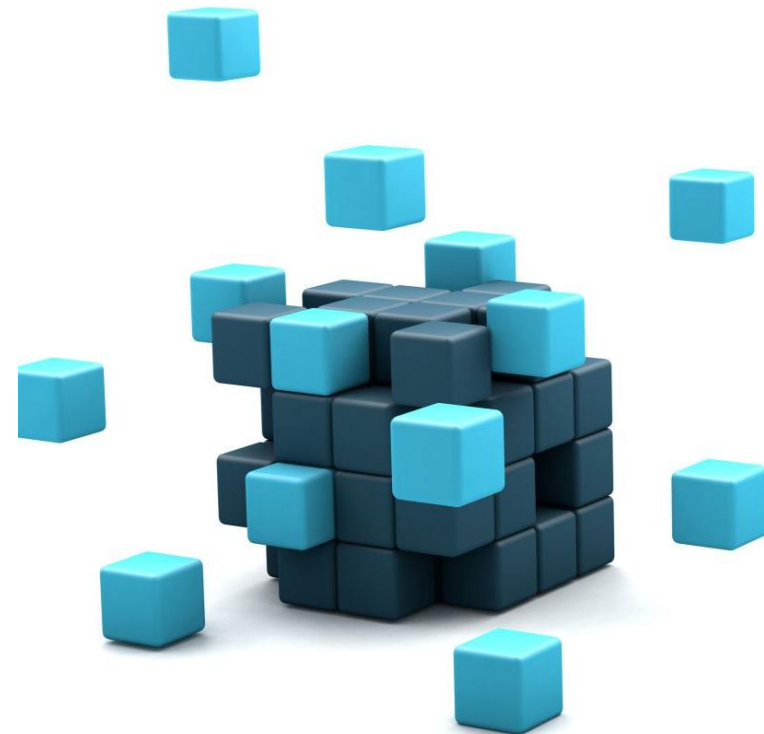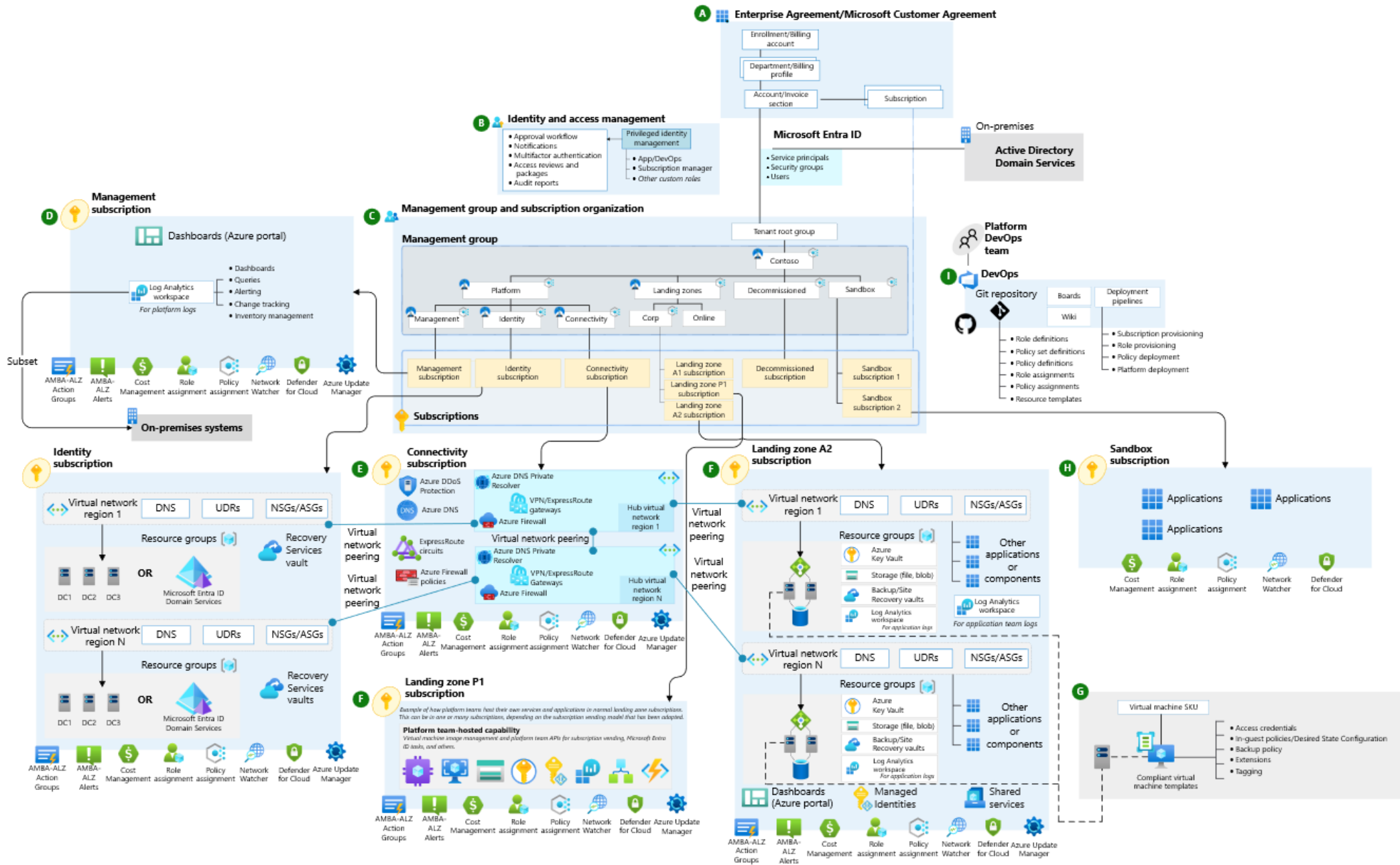
Key Components of an Azure AI Landing Zone

- Identity and Access Management (IAM)

- Networking

- Security

- Monitoring and Logging

- Resource Management

- Cost Management

Identity and Access Management (IAM)

- Azure Active Directory integration
- Role-Based Access Control (RBAC)
- Managed identities and service principals
- Identity protection strategies

A Enterprise Agreement/Microsoft Customer Agreement

Enrollment/Billing account → Department/Billing profile → Account/Invoice section → Subscription

Microsoft Entra ID
- Service principals
- Security groups
- Users

On-premises
Active Directory Domain Services

B Identity and access management
- Approval workflow
- Notifications
- Multifactor authentication
- Access reviews and packages
- Audit reports

Privileged identity management
- App/DevOps
- Subscription manager
- Other custom roles

D Management subscription

Dashboards (Azure portal)

Log Analytics workspace
For platform logs
- Dashboards
- Queries
- Alerting
- Change tracking
- Inventory management

Subset

AMBA-ALZ Action Groups | AMBA-ALZ Alerts | Cost Management | Role assignment | Policy assignment | Network Watcher | Defender for Cloud | Azure Update Manager

On-premises systems

C Management group and subscription organization

Management group

Tenant root group → Contoso
- Platform
  - Management
  - Identity
  - Connectivity
- Landing zones
  - Corp
  - Online
- Decommissioned
- Sandbox

Platform DevOps team

I DevOps

Git repository | Boards | Deployment pipelines | Wiki
- Role definitions
- Policy set definitions
- Policy definitions
- Role assignments
- Policy assignments
- Resource templates
- Subscription provisioning
- Role provisioning
- Policy deployment
- Platform deployment

Subscriptions
- Management subscription
- Identity subscription
- Connectivity subscription
- Landing zone A1 subscription
- Landing zone P1 subscription
- Landing zone A2 subscription
- Decommissioned subscription
- Sandbox subscription 1
- Sandbox subscription 2

Identity subscription

Virtual network region 1 | DNS | UDRs | NSGs/ASGs
Resource groups
DC1 DC2 DC3 **OR** Microsoft Entra ID Domain Services
Recovery Services vault

Virtual network region N | DNS | UDRs | NSGs/ASGs
Resource groups
DC1 DC2 DC3 **OR** Microsoft Entra ID Domain Services
Recovery Services vaults

Virtual network peering

AMBA-ALZ Action Groups | AMBA-ALZ Alerts | Cost Management | Role assignment | Policy assignment | Network Watcher | Defender for Cloud | Azure Update Manager

E Connectivity subscription
- Azure DDoS Protection
- Azure DNS
- Azure DNS Private Resolver
- VPN/ExpressRoute gateways
- Azure Firewall
Hub virtual network region 1

- ExpressRoute circuits
- Azure Firewall policies
- Azure DNS Private Resolver
- VPN/ExpressRoute Gateways
- Azure Firewall
Hub virtual network region N

Virtual network peering
Virtual network peering

AMBA-ALZ Action Groups | AMBA-ALZ Alerts | Cost Management | Role assignment | Policy assignment | Network Watcher | Defender for Cloud | Azure Update Manager

F Landing zone P1 subscription
Example of how platform teams host their own services and application in normal landing zone subscriptions. This can be one or many subscriptions, depending on the subscription vending model that has been adopted.

Platform team-hosted capability
Virtual machine image management and platform team APIs for subscription vending, Microsoft Entra ID tools, and others.

AMBA-ALZ Action Groups | AMBA-ALZ Alerts | Cost Management | Role assignment | Policy assignment | Network Watcher | Defender for Cloud | Azure Update Manager

F Landing zone A2 subscription

Virtual network region 1 | DNS | UDRs | NSGs/ASGs
Resource groups
- Azure Key Vault
- Storage (file, blob)
- Backup/Site Recovery vaults
- Log Analytics workspace *For application logs*
Other applications or components

Virtual network peering
Virtual network peering

Virtual network region N | DNS | UDRs | NSGs/ASGs
Resource groups
- Azure Key Vault
- Storage (file, blob)
- Backup/Site Recovery vaults
- Log Analytics workspace *For application logs*
Other applications or components

Dashboards (Azure portal) | Managed Identities | Shared services

AMBA-ALZ Action Groups | AMBA-ALZ Alerts | Cost Management | Role assignment | Policy assignment | Network Watcher | Defender for Cloud | Azure Update Manager

H Sandbox subscription
Applications | Applications | Applications

Cost Management | Role assignment | Policy assignment | Network Watcher | Defender for Cloud

G
Virtual machine SKU
Compliant virtual machine templates
- Access credentials
- In-guest policies/Desired State Configuration
- Backup policy
- Extensions
- Tagging

For application team logs

Microsoft Azure

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/
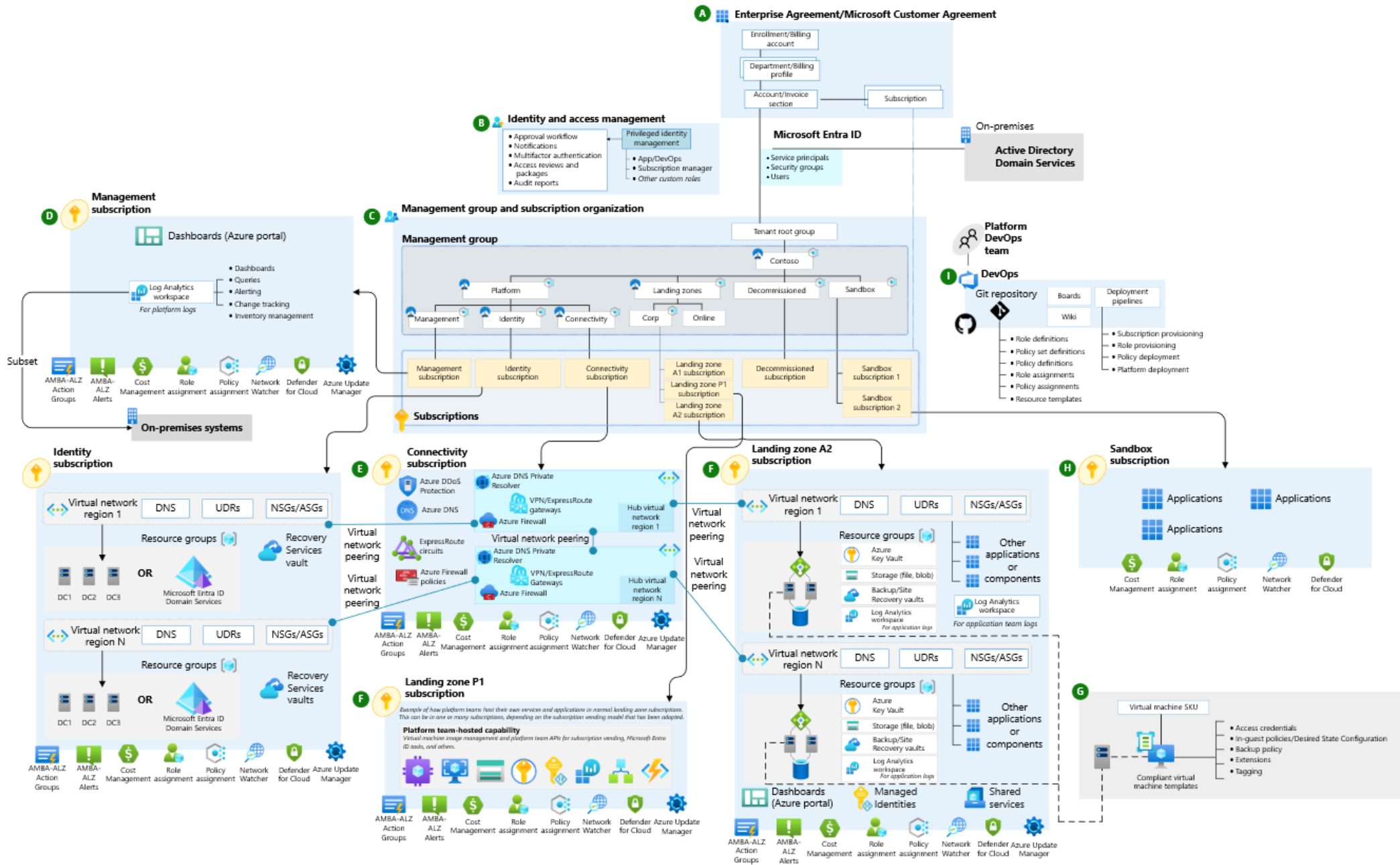
Networking Architecture

- Azure Virtual Networks (VNet)
- Private Endpoints and Link Services
- Azure Firewall and NSGs
- Hybrid connectivity scenarios (VPN, ExpressRoute)

Security Considerations

- Azure Security Center
- Threat detection and prevention
- Data encryption (at rest, in transit)
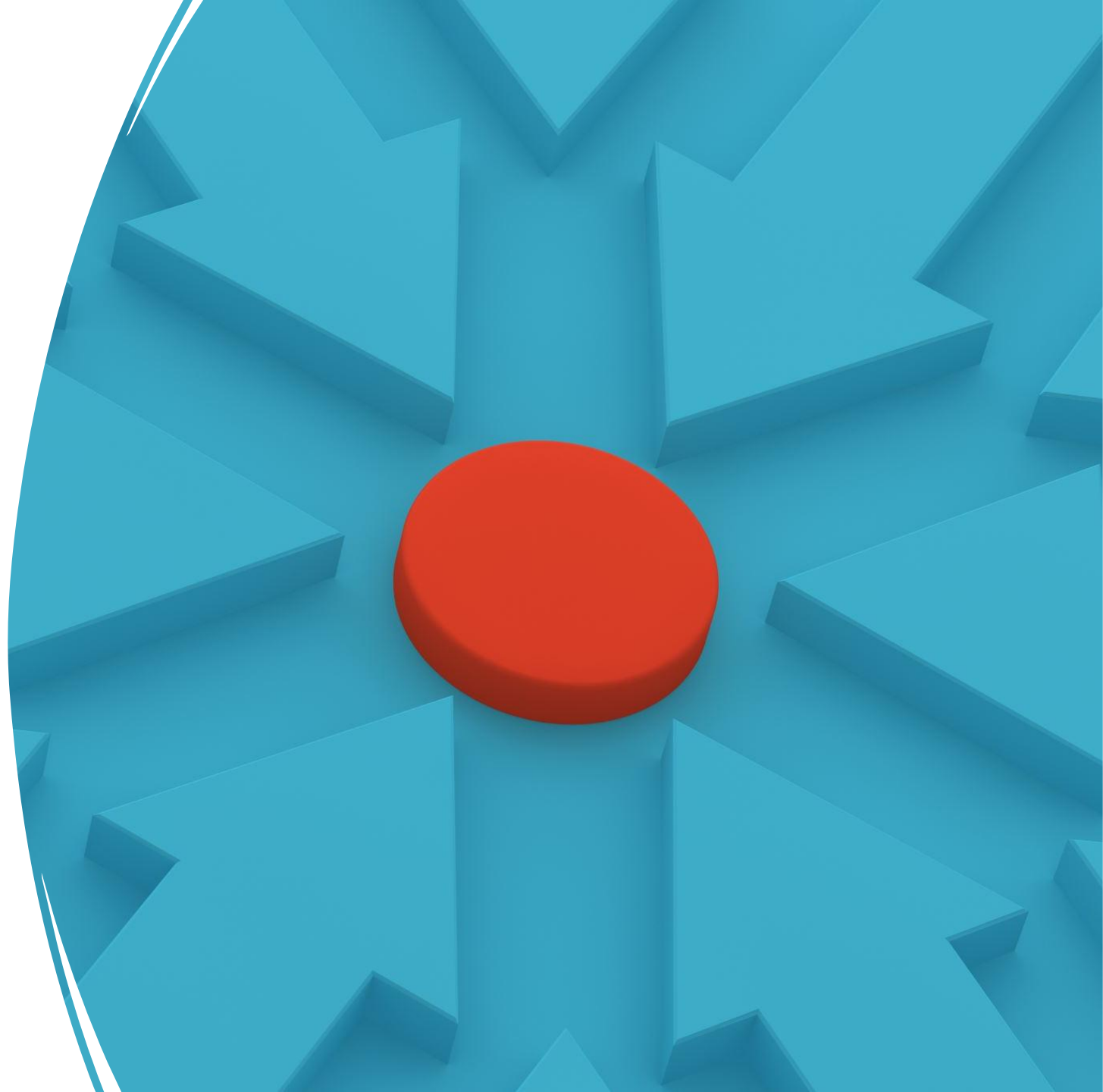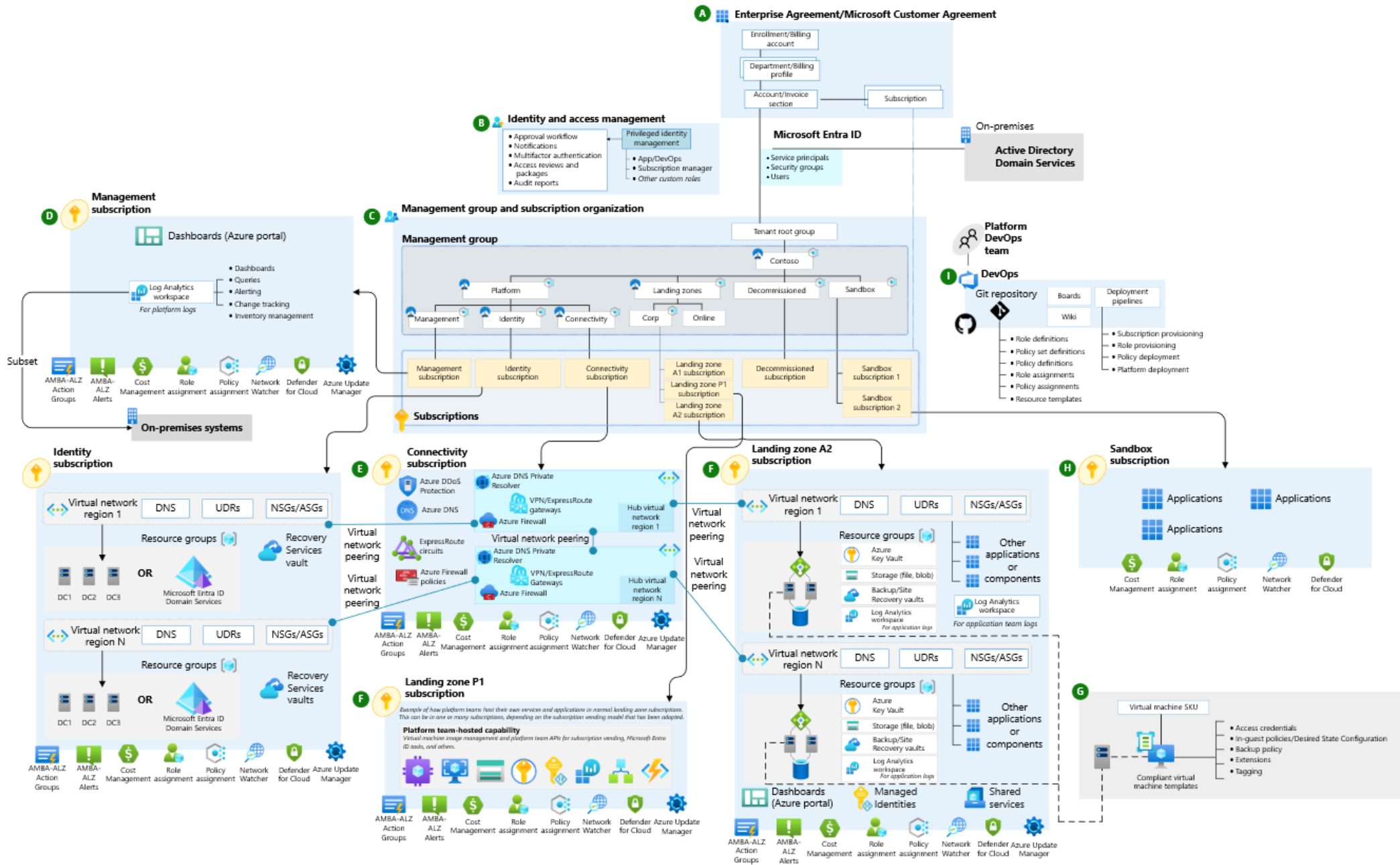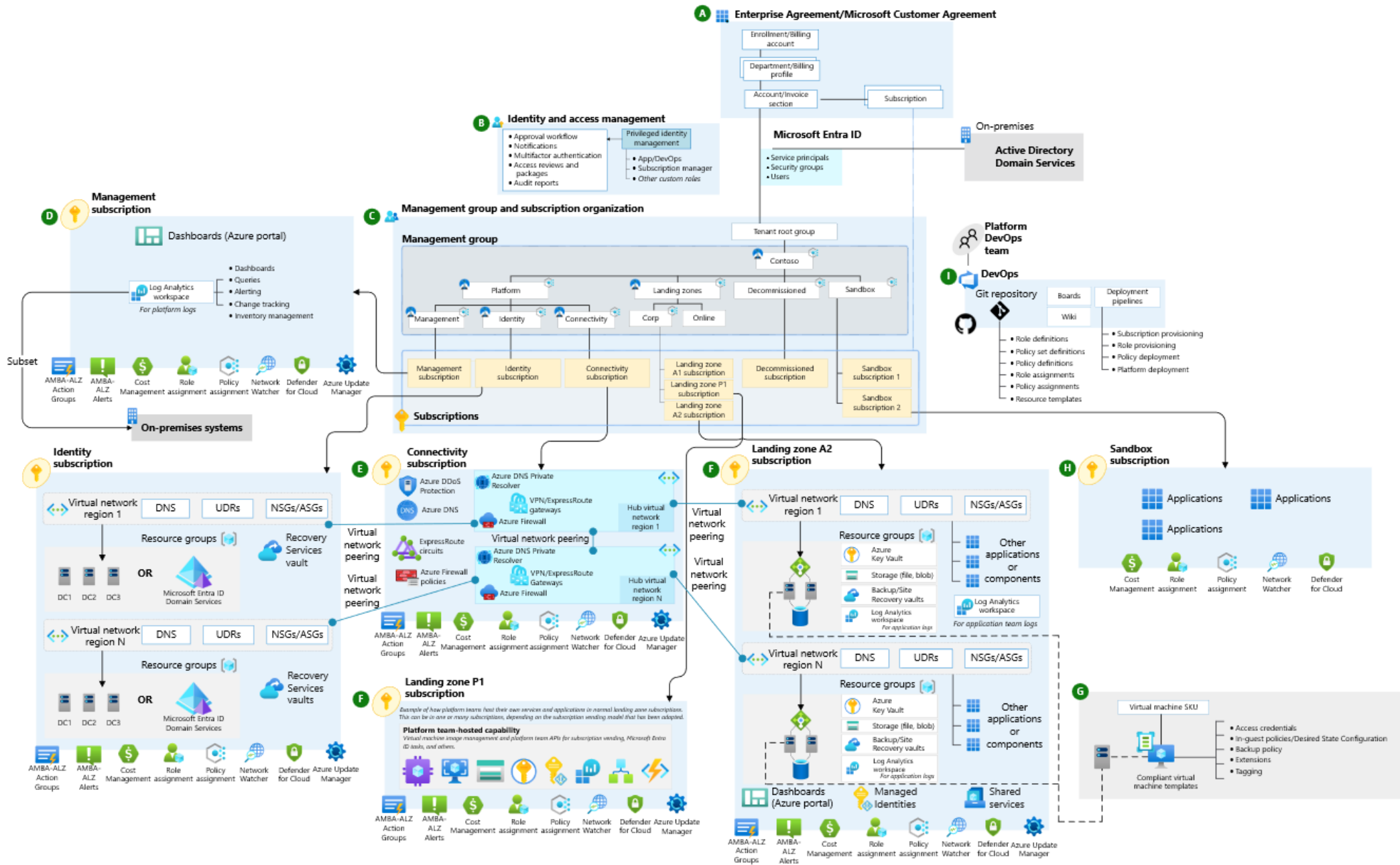- Compliance (GDPR, HIPAA, etc.)

Version: 2025-02-19

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

Monitoring and Logging

- Azure Monitor
- Log Analytics
- Application Insights
- Azure Sentinel integration

Azure Landing Zone conceptual architecture diagram

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

Resource Management and Governance

- Azure Resource Groups
- Azure Policy enforcement
- Management groups and subscriptions
- Resource tagging strategies

A Enterprise Agreement/Microsoft Customer Agreement

- Enrollment/Billing account
- Department/Billing profile
- Account/Invoice section
- Subscription

B Identity and access management

- Approval workflow
- Notifications
- Multifactor authentication
- Access reviews and packages
- Audit reports

Privileged identity management
- App/DevOps
- Subscription manager
- Other custom roles

Microsoft Entra ID
- Service principals
- Security groups
- Users

On-premises
Active Directory Domain Services

D Management subscription

Dashboards (Azure portal)
- Dashboards
- Queries
- Alerting
- Change tracking
- Inventory management

Log Analytics workspace
For platform logs

C Management group and subscription organization

Management group

Tenant root group → Contoso
- Platform
  - Management
  - Identity
  - Connectivity
- Landing zones
  - Corp
  - Online
- Decommissioned
- Sandbox

Subset → On-premises systems

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

Subscriptions
- Management subscription
- Identity subscription
- Connectivity subscription
- Landing zone A1 subscription
- Landing zone P1 subscription
- Landing zone A2 subscription
- Decommissioned subscription
- Sandbox subscription 1
- Sandbox subscription 2

Platform DevOps team

I DevOps

Git repository
- Boards
- Deployment pipelines
- Wiki

- Role definitions
- Policy set definitions
- Policy definitions
- Role assignments
- Policy assignments
- Resource templates

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

Identity subscription

Virtual network region 1 · DNS · UDRs · NSGs/ASGs

Resource groups
DC1 DC2 DC3 **OR** Microsoft Entra ID Domain Services
Recovery Services vault

Virtual network region N · DNS · UDRs · NSGs/ASGs

Resource groups
DC1 DC2 DC3 **OR** Microsoft Entra ID Domain Services
Recovery Services vaults

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

E Connectivity subscription

- Azure DDoS Protection
- Azure DNS
- Azure DNS Private Resolver
- VPN/ExpressRoute gateways
- Azure Firewall
Hub virtual network region 1

- ExpressRoute circuits
- Azure Firewall policies
- Azure DNS Private Resolver
- VPN/ExpressRoute Gateways
- Azure Firewall
Hub virtual network region N

Virtual network peering

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

F Landing zone P1 subscription

Example of how platform teams host their own services and application in normal landing zone subscriptions. This can be one or many subscriptions, depending on the subscription vending model that has been adopted.

Platform team-hosted capability
Virtual machine image management and platform team APIs for subscription vending, Microsoft Entra ID tools, and others.

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

F Landing zone A2 subscription

Virtual network region 1 · DNS · UDRs · NSGs/ASGs

Resource groups
- Azure Key Vault
- Storage (file, blob)
- Backup/Site Recovery vaults
- Log Analytics workspace *For application logs*

Other applications or components

Virtual network region N · DNS · UDRs · NSGs/ASGs

Resource groups
- Azure Key Vault
- Storage (file, blob)
- Backup/Site Recovery vaults
- Log Analytics workspace *For application logs*

Other applications or components

Dashboards (Azure portal) · Managed Identities · Shared services

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

H Sandbox subscription

Applications · Applications · Applications

Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud

G Virtual machine SKU

Compliant virtual machine templates
- Access credentials
- In-guest policies/Desired State Configuration
- Backup policy
- Extensions
- Tagging

Virtual network peering

Version: 2025-02-19

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

Cost Management

- Cost allocation and budgeting
- Azure Cost Management tools
- Cost optimization techniques

Azure Cloud Adoption Framework – Ready: Landing Zone architecture diagram

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

Version: 2025-02-19

Platform vs Application Landing Zones

- **Platform landing zone:** A subscription that provides shared services (identity, connectivity, management) to applications in application landing zones.

- **Application landing zone:** A subscription for hosting an application.

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

Azure AI Landing Zone

- Extends the standard Azure Landing Zone with AI-specific components
- Provides a secure, governed, and scalable environment for AI workloads
- Includes integration with Azure AI services (Machine Learning, Cognitive Services, OpenAI, etc.)
- Ensures compliance with Responsible AI principles (fairness, privacy, transparency)
- Enables rapid experimentation while maintaining enterprise controls
- Supports MLOps and data governance for production-ready AI solutions

Azure AI Landing Zones
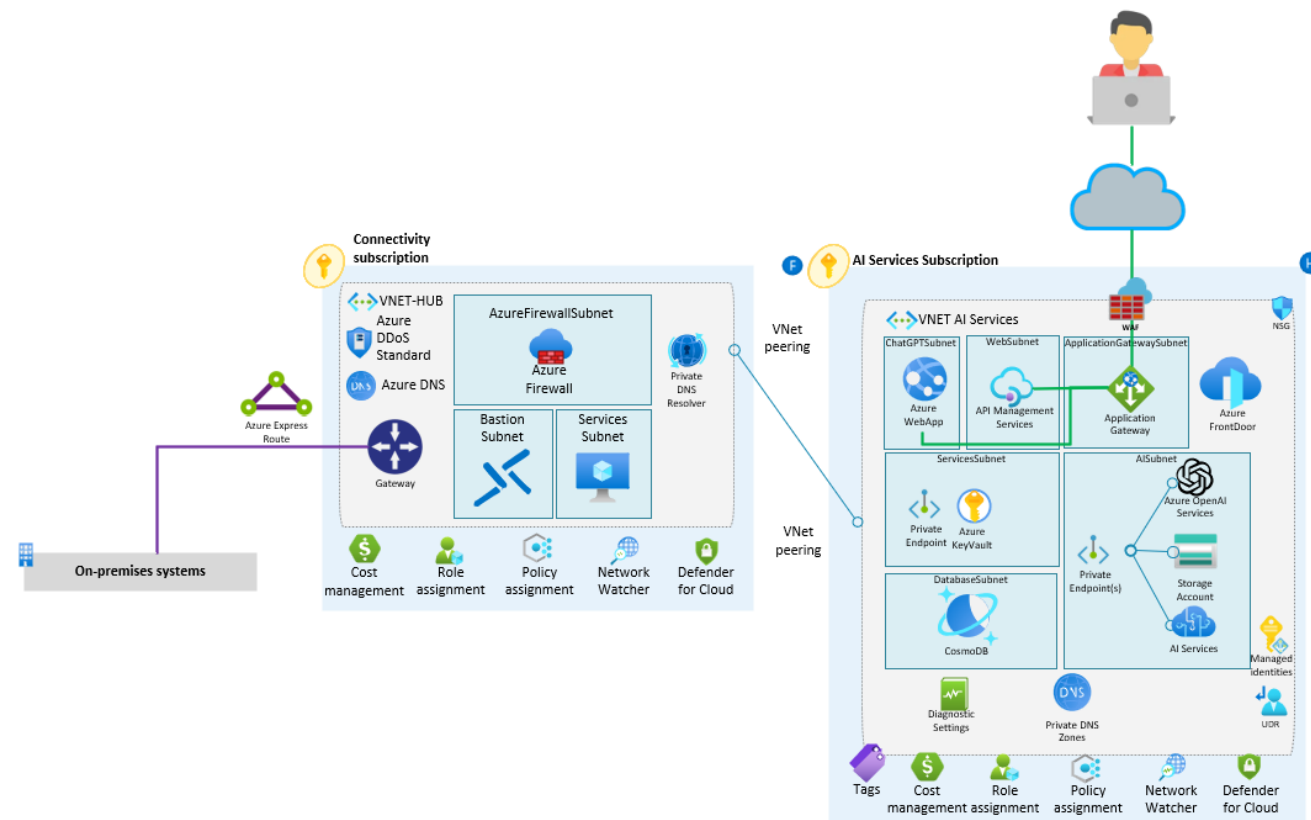
Empowering AI: Building and Deploying Azure AI Landing Zones with Terraform
Author: Freddy Ayala
https://techcommunity.microsoft.com/blog/azurearchitectureblog/empowering-ai-building-and-deploying-azure-ai-landing-zones-with-terraform/3891249

Responsible AI Principles

- Fairness.

    Treat everyone equally and provide the same recommendations to all individuals.

- Reliability and safety

    Operate reliably, safely, and consistently under various conditions to help build trust.

- Privacy and security

    Ensure strong data protection, secure design, and privacy safeguards

- Inclusiveness

    Understand and address potential exclusion barriers in a product or service

- Transparency

    Provide understanding on how the system makes decisions

- Accountability

    People must be accountable for AI system outcomes

Implementation Steps

- Initial Planning and Design

- Infrastructure Deployment

- AI Service Integration

- Continuous Management and Optimization

Best Practices

- Automation and Infrastructure as Code (IaC)
  - ARM Templates
  - Bicep
  - Terraform
- Scalability and flexibility
- Regular security reviews and audits

Azure Verified Modules (AVM)

Pre-approved, reusable infrastructure-as-code (IaC) building blocks developed and validated by Microsoft and the Azure community to accelerate and standardize Azure deployments.
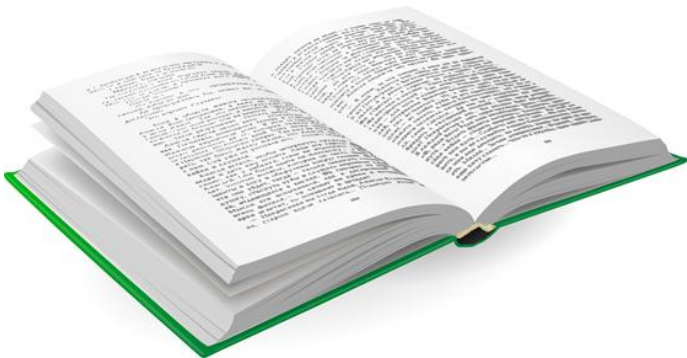
Azure Verified Modules – Benefits

🚀 Faster time to deploy

🧱 Infrastructure consistency

✅ Reduced risk of misconfiguration

🧩 Integration with landing zones and CI/CD pipelines
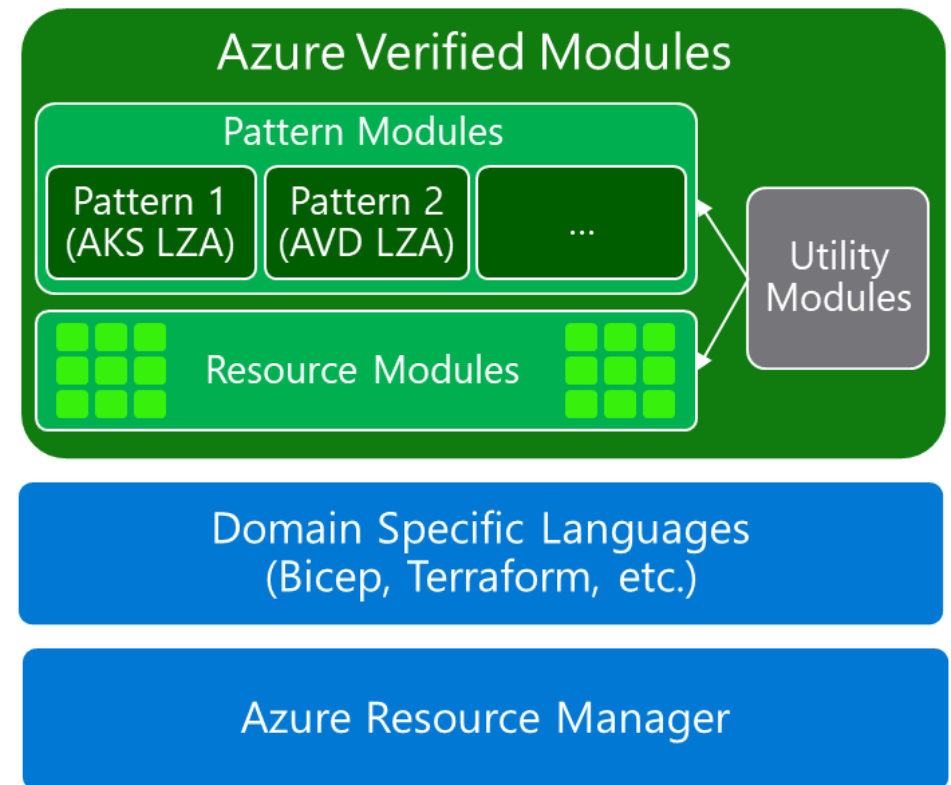
Azure Verified Modules – Key Features

📦 Pre-Built Modules
Virtual Networks, Key Vaults, AKS, etc.

🔐 Validated for Security & Compliance

🔄 Reusable & Composable

☁️ Supports Terraform & Bicep

Azure Verified Modules - Purpose

- Simplify and standardize deployment of Azure resources
- Ensure compliance with Microsoft best practices
- Enable secure, modular, and scalable infrastructure provisioning

Resources

- Azure Landing Zones

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

- AI Adoption

  https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/ai/

- Azure Verified Modules Repository

  https://github.com/Azure/Azure-Verified-Modules

Additional Resources

Why Landing Zones Matter
(What are they and How to Build One) - Simone Bennett

https://www.youtube.com/watch?v=huEzpDoLrqQ&t=1s

Thank you