Azure Landing Zones with Bicep: The ultimate workout for your cloud infrastructure

Mark Scholman

Founder CA8 – Azure MVP

Once upon a time…

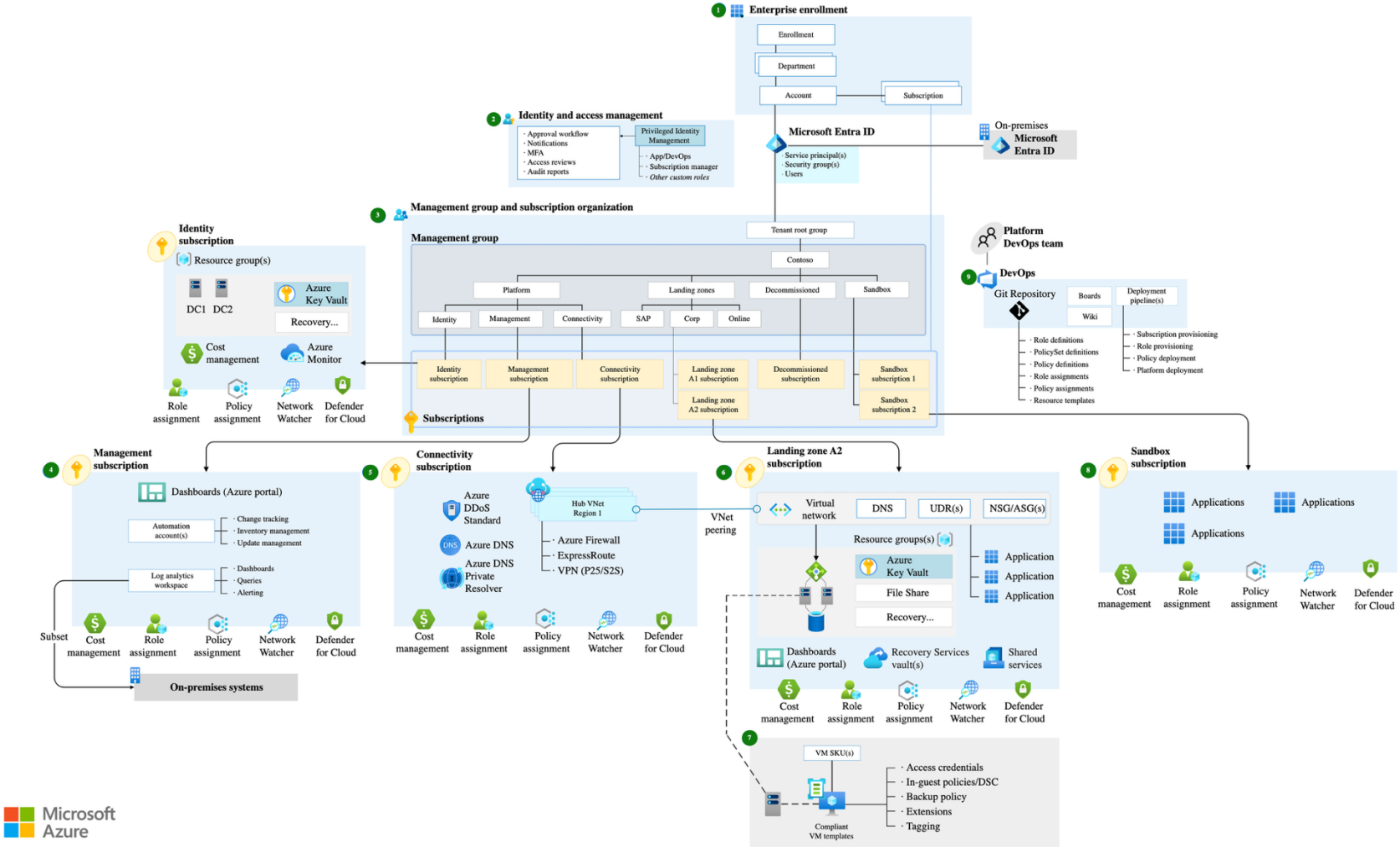
We did manage Azure in a proper way – at least we thought

- No hierarchy (or self invented)
  - Management groups
  - RBAC
  - Policies
  - Cost controls
- No automation
  - Maybe a bit of ARM templates or imperative PowerShell…

And we evolved to…

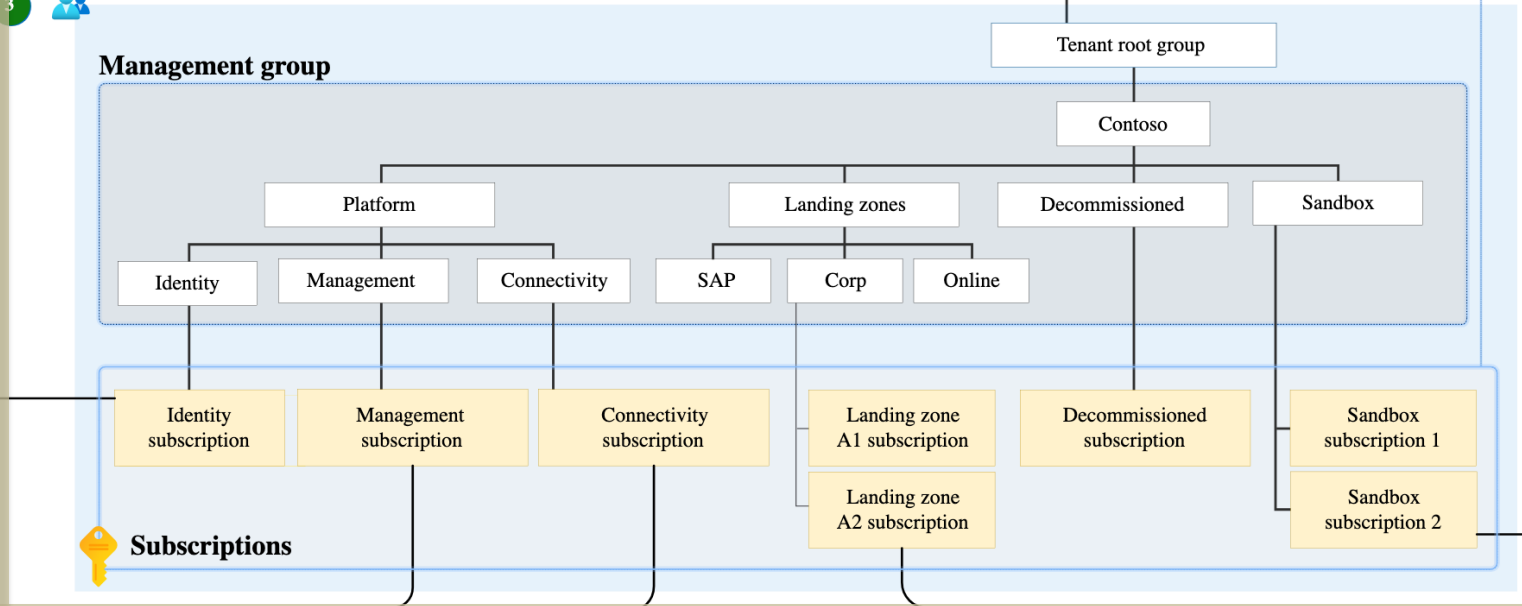
- Multiple deployment tooling (ARM, Bicep, Terraform & Pulumi)
- Enterprise scale landing zone
- Cost management
- Governance hierarchy

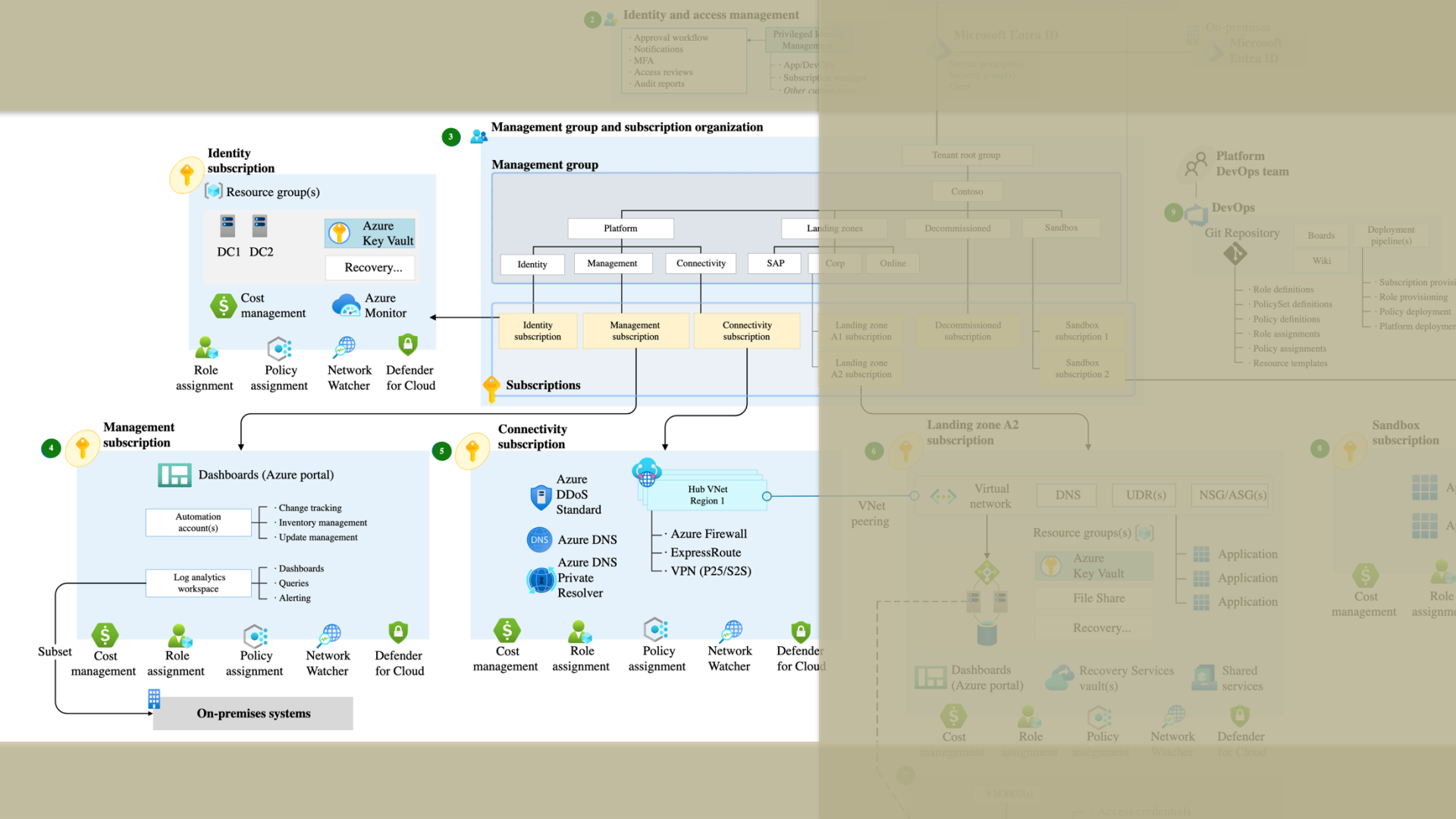
With eventually the new kid on the block…

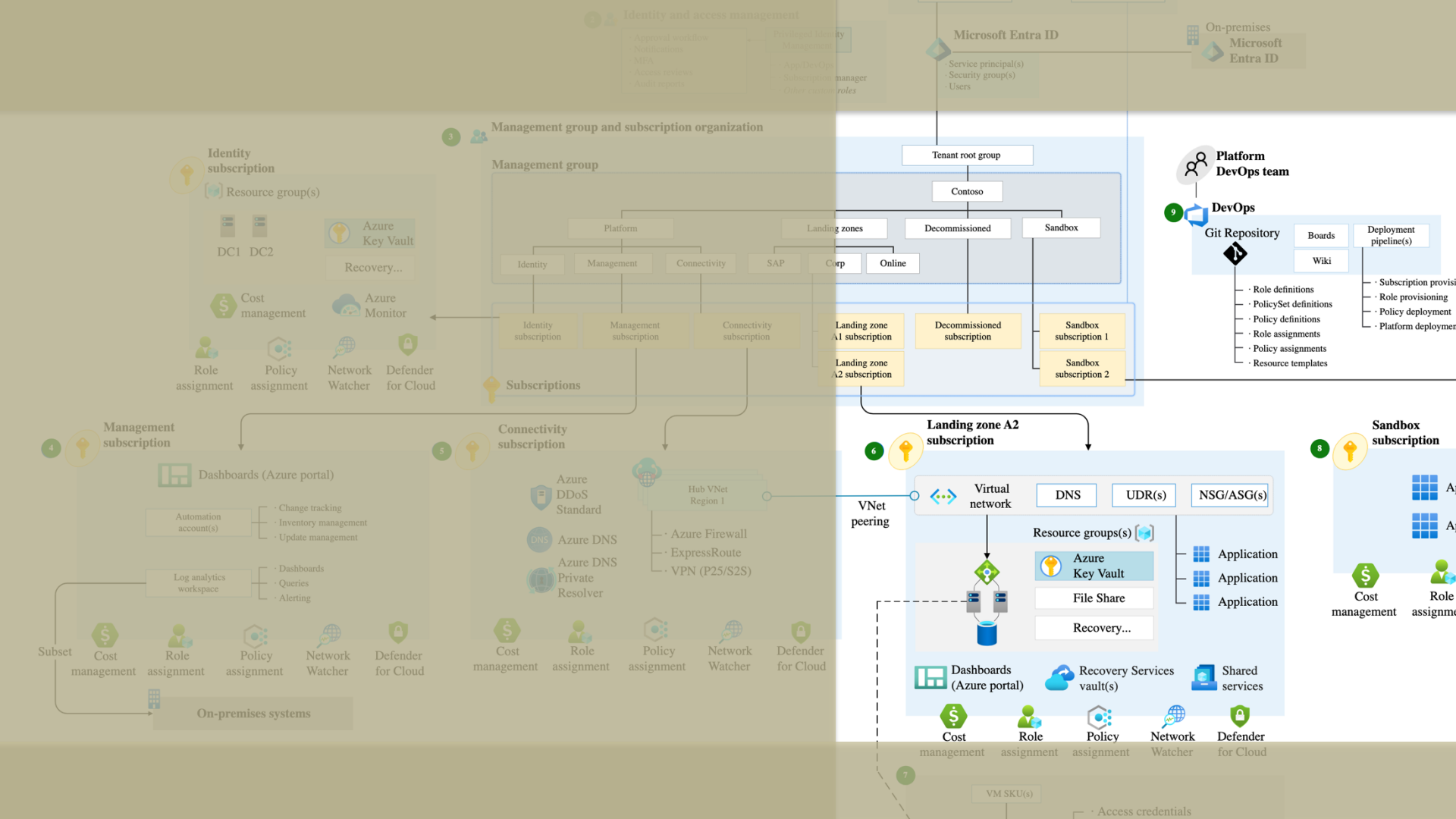


Microsoft Azure

Management group and subscription organization




Identity and access management
Approval workflow
Notifications
MFA
Access reviews
Audit reports
Microsoft Entra ID
On-premises Microsoft Entra ID
Management group and subscription organization
Identity subscription
Resource group(s)
DC1
DC2
Azure Key Vault
Recovery...
Cost management
Azure Monitor
Role assignment
Policy assignment
Network Watcher
Defender for Cloud
Management group
Tenant root group
Contoso
Platform
Landing zones
Decommissioned
Sandbox
Identity
Management
Connectivity
SAP
Corp
Online
Identity subscription
Management subscription
Connectivity subscription
Landing zone A1 subscription
Landing zone A2 subscription
Decommissioned subscription
Sandbox subscription 1
Sandbox subscription 2
Subscriptions
Platform DevOps team
DevOps
Git Repository
Boards
Wiki
Deployment pipeline(s)
Role definitions
PolicySet definitions
Policy definitions
Role assignments
Policy assignments
Resource templates
Subscription provisi
Role provisioning
Policy deployment
Platform deployment
Management subscription
Dashboards (Azure portal)
Automation account(s)
Change tracking
Inventory management
Update management
Log analytics workspace
Dashboards
Queries
Alerting
Subset
Cost management
Role assignment
Policy assignment
Network Watcher
Defender for Cloud
On-premises systems
Connectivity subscription
Azure DDoS Standard
Azure DNS
Azure DNS Private Resolver
Hub VNet Region 1
Azure Firewall
ExpressRoute
VPN (P25/S2S)
Landing zone A2 subscription
VNet peering
Virtual network
DNS
UDR(s)
NSG/ASG(s)
Resource groups(s)
Azure Key Vault
File Share
Recovery...
Application
Application
Application
Dashboards (Azure portal)
Recovery Services vault(s)
Shared services
Sandbox subscription


Identity and access management
Microsoft Entra ID
On-premises
Microsoft Entra ID
Service principal(s)
Security group(s)
Users
Management group and subscription organization
Identity subscription
Resource group(s)
DC1
DC2
Azure Key Vault
Recovery...
Cost management
Azure Monitor
Role assignment
Policy assignment
Network Watcher
Defender for Cloud
Management group
Tenant root group
Contoso
Platform
Landing zones
Decommissioned
Sandbox
Identity
Management
Connectivity
SAP
Corp
Online
Identity subscription
Management subscription
Connectivity subscription
Landing zone A1 subscription
Landing zone A2 subscription
Decommissioned subscription
Sandbox subscription 1
Sandbox subscription 2
Subscriptions
Platform DevOps team
DevOps
Git Repository
Boards
Wiki
Deployment pipeline(s)
Role definitions
PolicySet definitions
Policy definitions
Role assignments
Policy assignments
Resource templates
Subscription provisi
Role provisioning
Policy deployment
Platform deployment
Management subscription
Dashboards (Azure portal)
Automation account(s)
Change tracking
Inventory management
Update management
Log analytics workspace
Dashboards
Queries
Alerting
Subset
Cost management
Role assignment
Policy assignment
Network Watcher
Defender for Cloud
On-premises systems
Connectivity subscription
Azure DDoS Standard
Hub VNet Region 1
Azure Firewall
ExpressRoute
VPN (P25/S2S)
Azure DNS
Azure DNS Private Resolver
Cost management
Role assignment
Policy assignment
Network Watcher
Defender for Cloud
Landing zone A2 subscription
VNet peering
Virtual network
DNS
UDR(s)
NSG/ASG(s)
Resource groups(s)
Azure Key Vault
File Share
Recovery...
Application
Application
Application
Dashboards (Azure portal)
Recovery Services vault(s)
Shared services
Cost management
Role assignment
Policy assignment
Network Watcher
Defender for Cloud
Sandbox subscription
Cost management
Role assignme
VM SKU(s)
Access credentials

Example ALZ Customer Journey

Bootstrap your environment

Whether you are a Brownfield or Greenfield customer, if you are looking to implement a new ALZ environment based upon best practice then you will require multiple subscriptions created. The below articles will refer you to manual and programmatic creation methods.

Deploy Azure Landing Zone Platform components

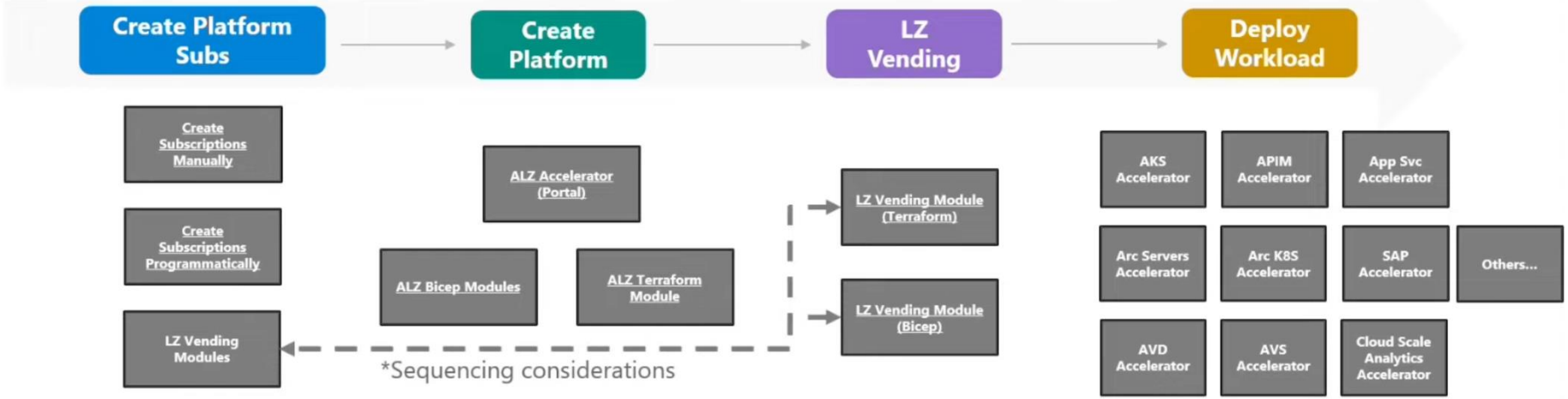
Accelerate the deployment of platform resources based upon ALZ conceptual architecture. Deployment options available via Portal, Terraform and Bicep to assist with the deployment of management group hierarchy, governance baseline, connectivity, management and security components.

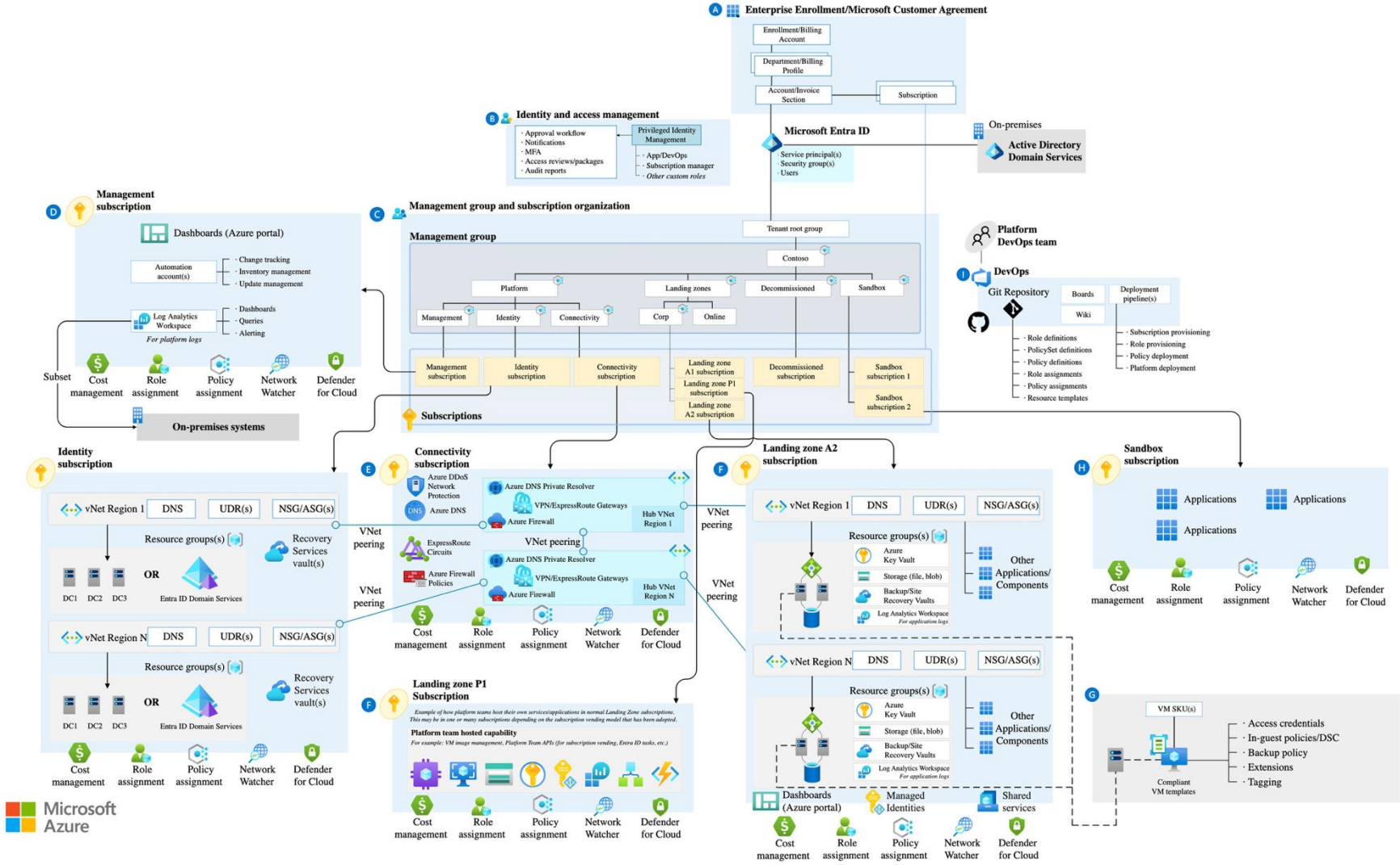
Subscription (LZ) Vending Process

To accelerate the deployment of individual landing zones within an Azure tenant, a subscription vending solution is recommended to help deploy a subscription and the core resources, e.g., networking. Subscription vending is available using both Terraform and Bicep.

Landing Zone Accelerators

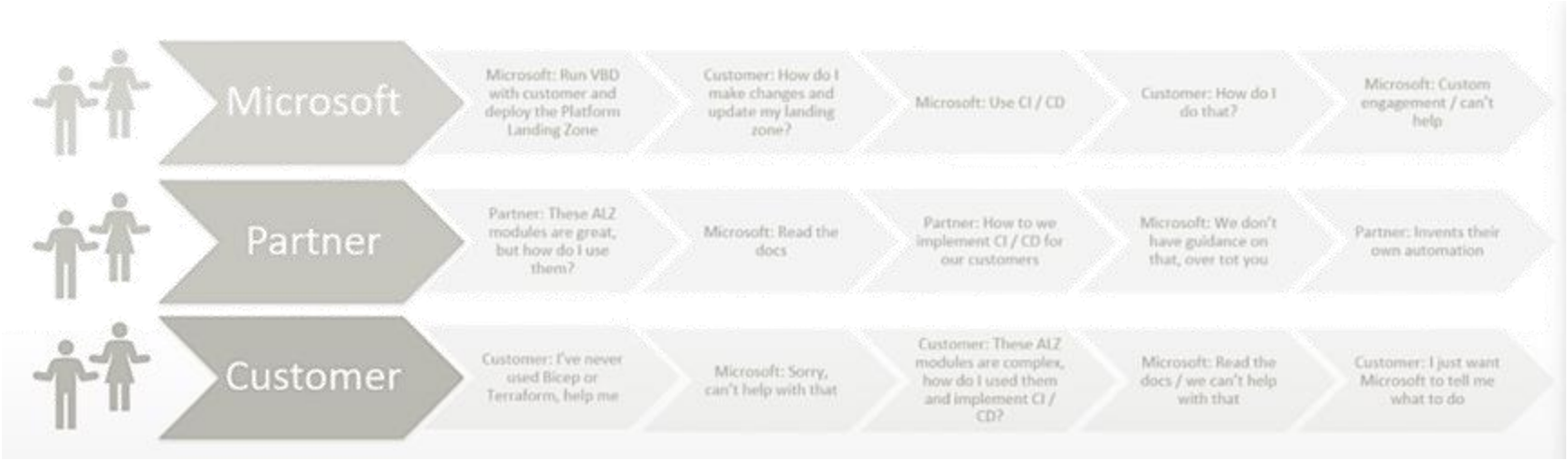
There are multiple Landing Zone Accelerators that provide a specific architectural approach and reference implementation for preparing landing zone subscriptions for an enterprise deployment, e.g. Azure Virtual Desktop, SAP, AKS etc.. These Accelerators are available in a wide range of deployment options.




A Enterprise Enrollment/Microsoft Customer Agreement
Enrollment/Billing Account
Department/Billing Profile
Account/Invoice Section
Subscription
B Identity and access management
· Approval workflow
· Notifications
· MFA
· Access reviews/packages
· Audit reports
Privileged Identity Management
· App/DevOps
· Subscription manager
· Other custom roles
Microsoft Entra ID
· Service principal(s)
· Security group(s)
· Users
On-premises
Active Directory Domain Services
D Management subscription
Dashboards (Azure portal)
Automation account(s)
· Change tracking
· Inventory management
· Update management
Log Analytics Workspace
For platform logs
· Dashboards
· Queries
· Alerting
Subset
Cost management
Role assignment
Policy assignment
Network Watcher
Defender for Cloud
On-premises systems
C Management group and subscription organization
Management group
Tenant root group
Contoso
Platform
Landing zones
Decommissioned
Sandbox
Management
Identity
Connectivity
Corp
Online
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
Subscriptions
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
Identity subscription
vNet Region 1
DNS
UDR(s)
NSG/ASG(s)
Resource groups(s)
Recovery Services vault(s)
DC1
DC2
DC3
OR
Entra ID Domain Services
vNet Region N
E Connectivity subscription
Azure DDoS Network Protection
Azure DNS
ExpressRoute Circuits
Azure Firewall Policies
Azure DNS Private Resolver
VPN/ExpressRoute Gateways
Azure Firewall
Hub VNet Region 1
Hub VNet Region N
VNet peering
F Landing zone A2 subscription
Azure Key Vault
Storage (file, blob)
Backup/Site Recovery Vaults
Log Analytics Workspace
For application logs
Other Applications/ Components
F Landing zone P1 Subscription
Example of how platform teams host their own services/applications in normal Landing Zone subscriptions. This may be in one or many subscriptions depending on the subscription vending model that has been adopted.
Platform team hosted capability
For example: VM image management, Platform Team API's (for subscription vending, Entra ID tasks, etc.)
Dashboards (Azure portal)
Managed Identities
Shared services
H Sandbox subscription
Applications
G
VM SKU(s)
Compliant VM templates
· Access credentials
· In-guest policies/DSC
· Backup policy
· Extensions
· Tagging
Microsoft Azure

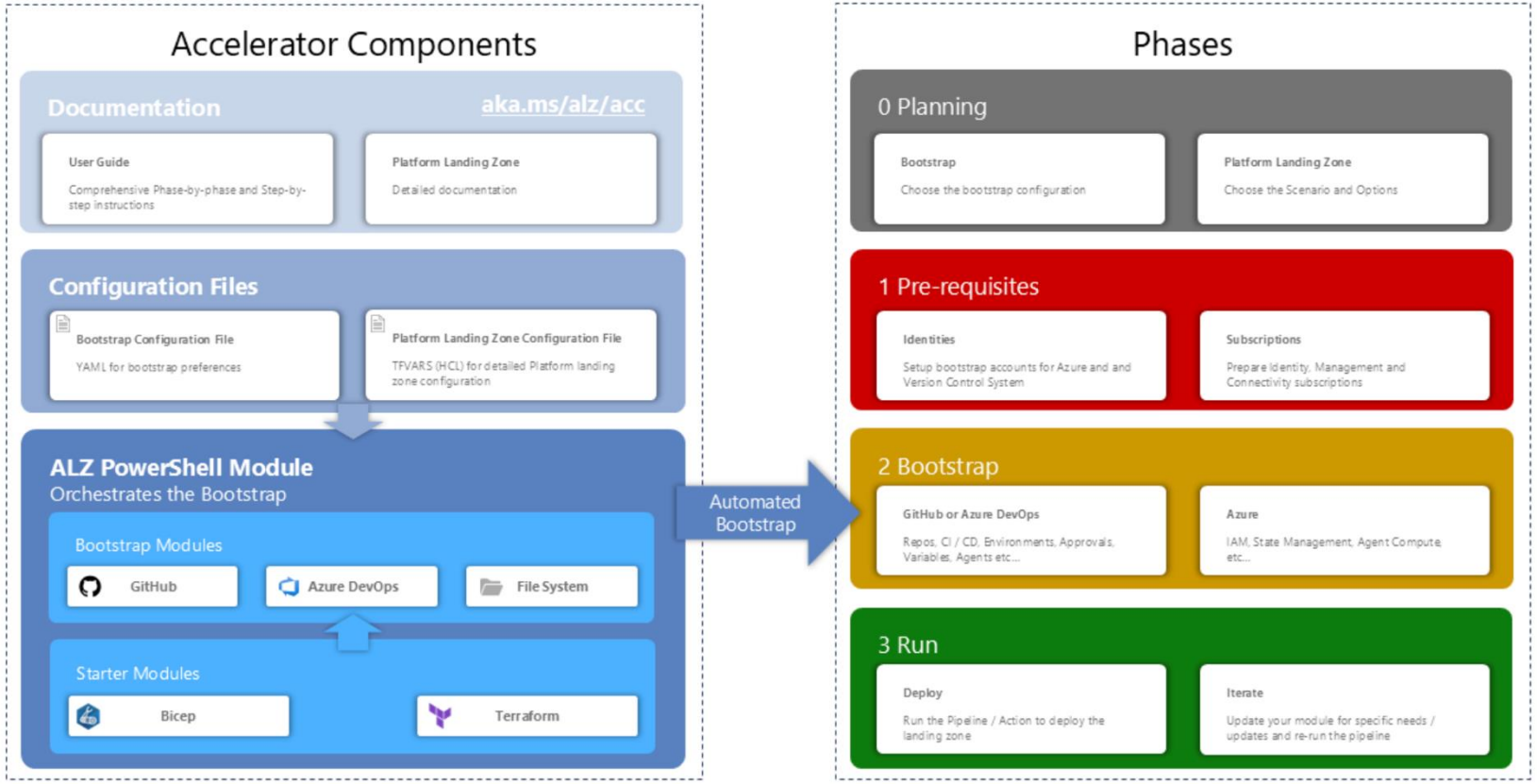
Deployment options

- Portal accelerator
- Bicep accelerator
- Terraform accelerator



ALZ Accelerator

ALZ Bicep Accelerator



Overview

Bicep – Azure Verified Modules

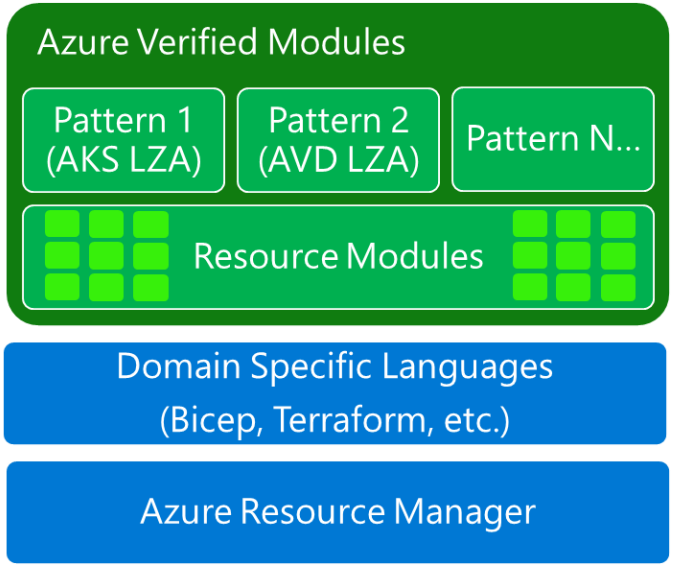
Modules are composable building blocks that encapsulate groups of resources dedicated to one task.

•Flexible, generalized, multi-purpose
•Integrates child resources
•Integrates extension resources

AVM improves code quality and provides a unified customer experience.

There are 2 main types of AVM modules*
- Resource modules
- Pattern Modules

* And utility modules



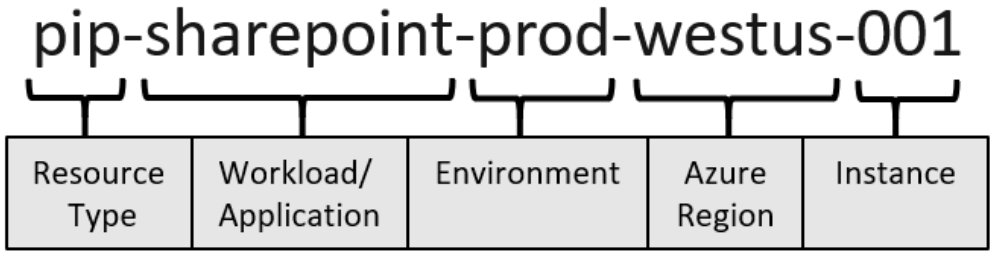
ALZ Do It Yourself (DIY)

But what if you want to do it yourself?

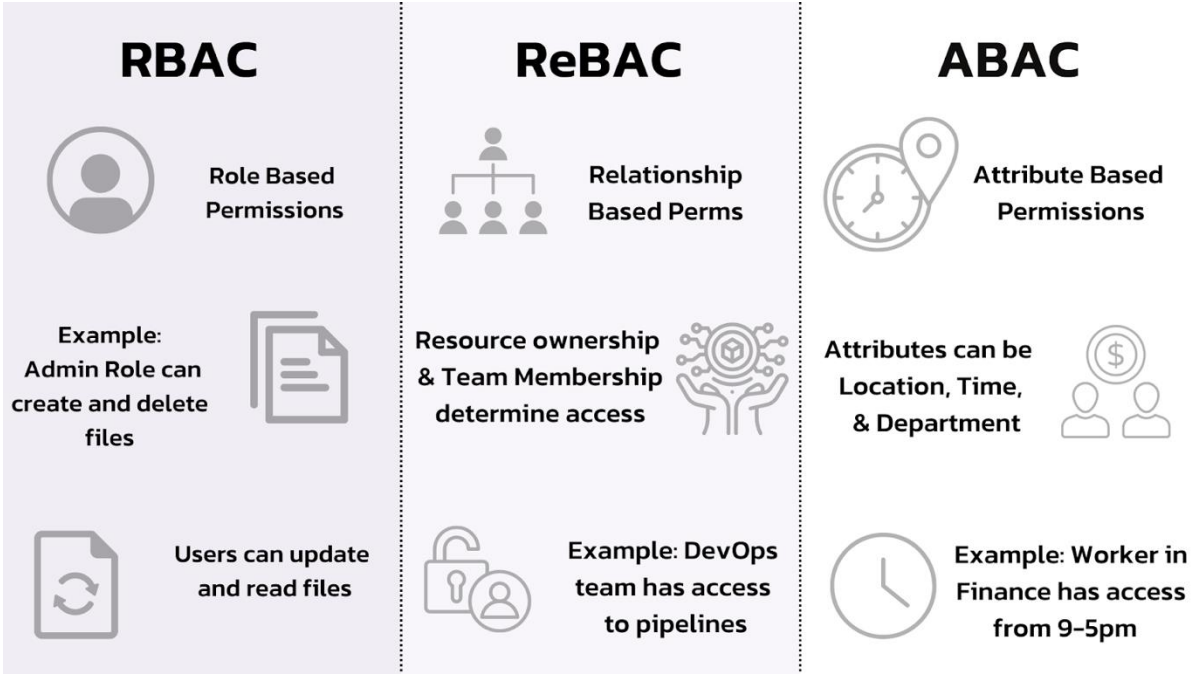
What would be the best approach & should I really do it?

Governance

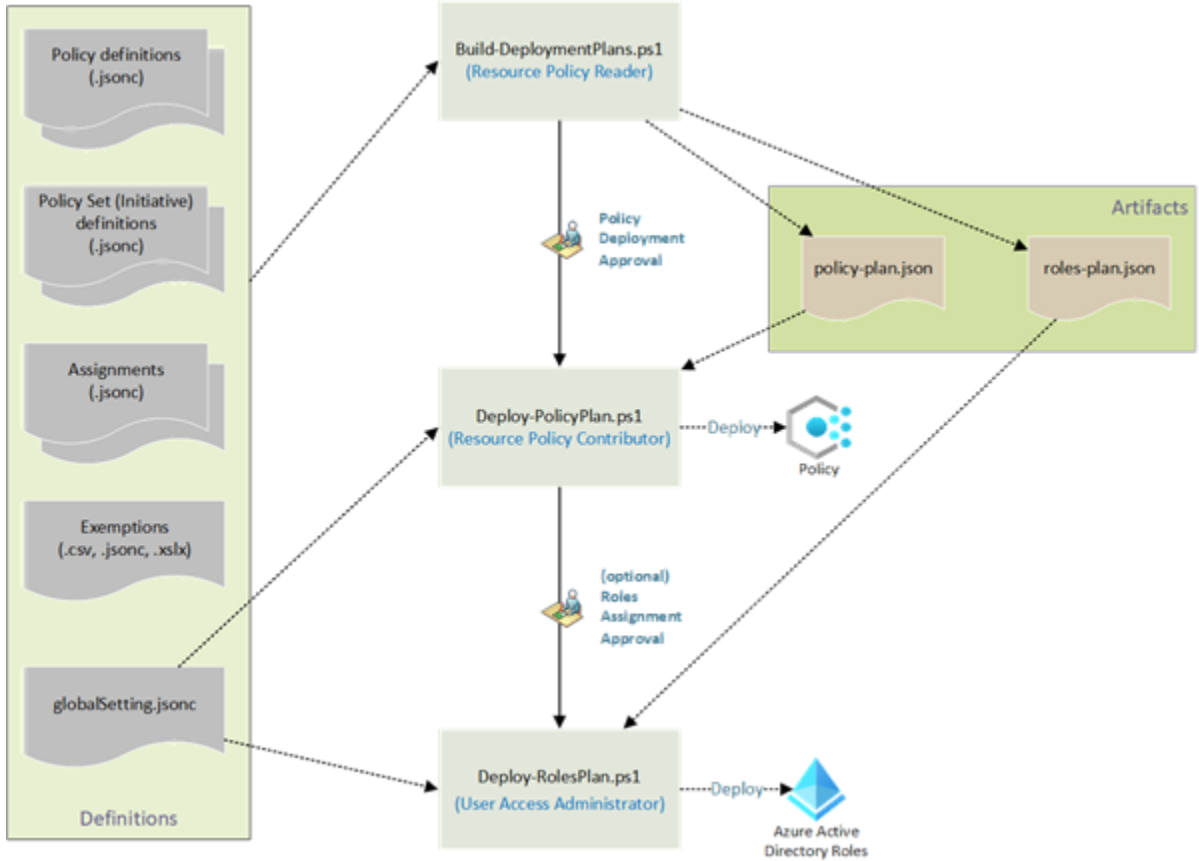
- Naming convention



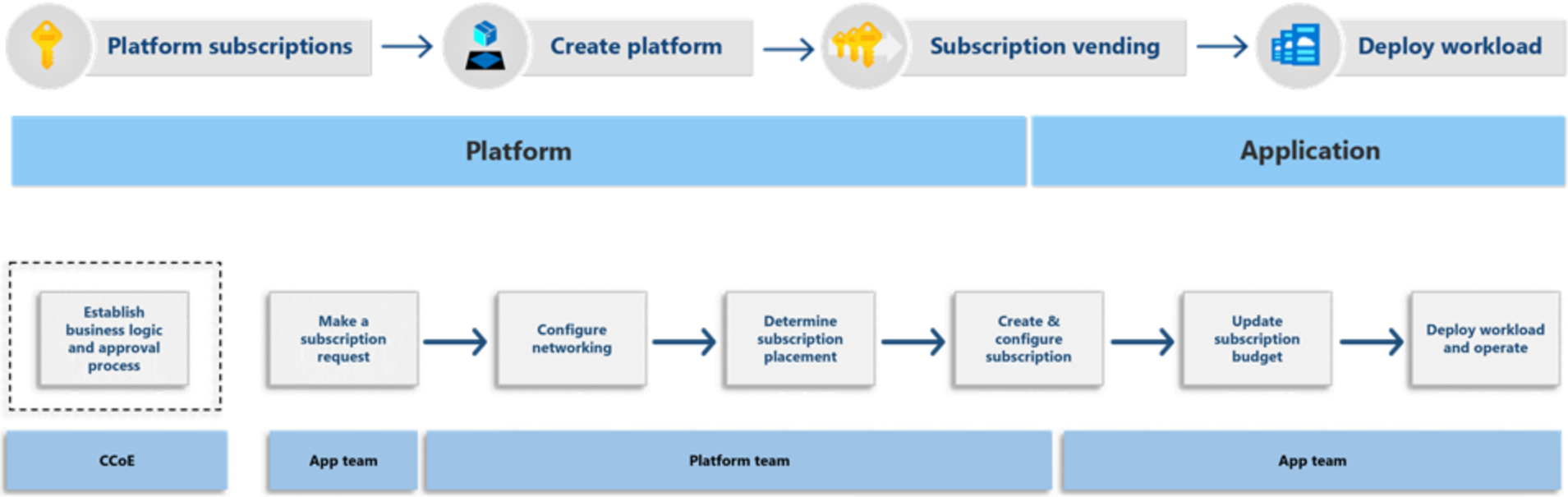
Governance


RBAC
Role Based Permissions
Example: Admin Role can create and delete files
Users can update and read files
ReBAC
Relationship Based Perms
Resource ownership & Team Membership determine access
Example: DevOps team has access to pipelines
ABAC
Attribute Based Permissions
Attributes can be Location, Time, & Department
Example: Worker in Finance has access from 9-5pm

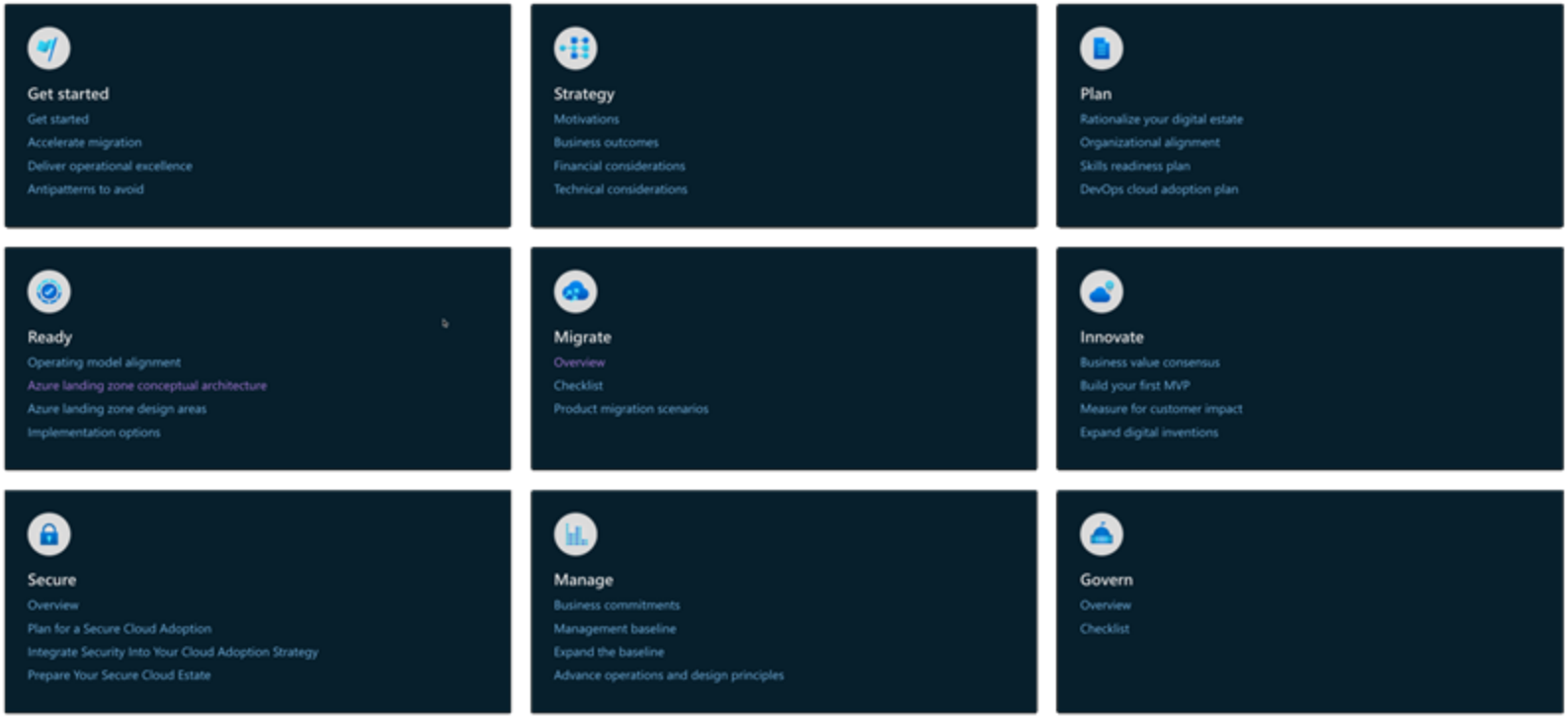
Enterprise Policy as Code (EPAC)



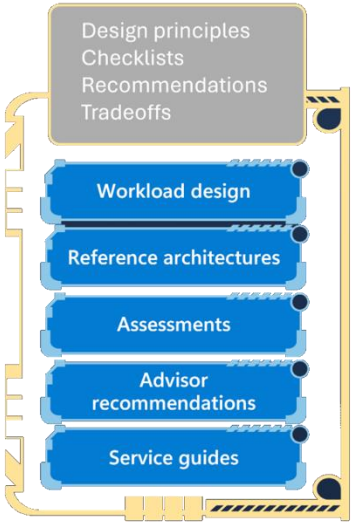
Subscription Vending



Cloud Adoption Framework



Well Architected Framework

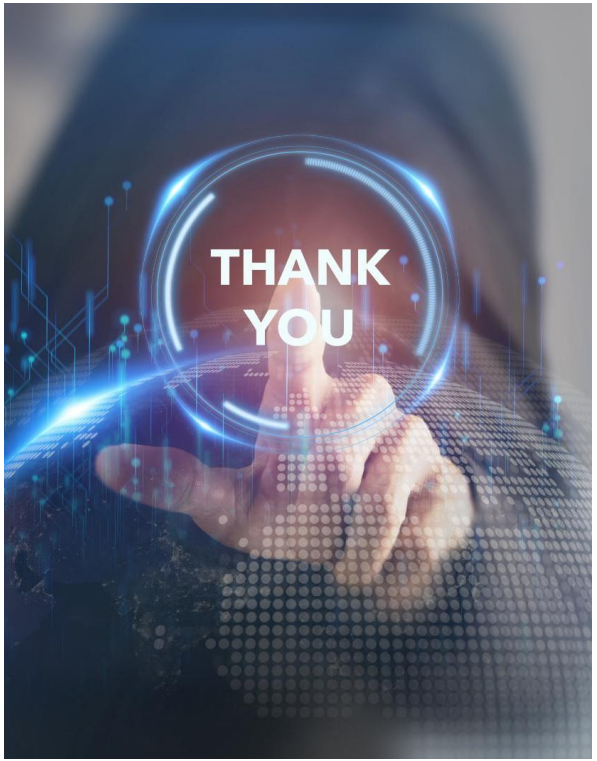


DEMO TIME

But… before

First a quiz!

What are the 3 AVM flavors that you can consume?



Are there any questions?