Azure Deployment Partitions and Naming Standards
- Based around a DevOps app deployment model

T0
(bootstrap tenant)

Azure
Active Directory

Deployment Service Principal - / **Owner**

Azure Tenant

Access & Identity across organization

Service Principals
Create Subscriptions
Create initial MG

M0

Deployment Service Principal -MG **Owner**

Azure Management Groups

Control and Policy enforcement across organization

Policies
RBAC [IAM]
Create MG's
Create Subscriptions's
Custom RBAC Roles

G0

Owners
Readers

Deployment Service Principal -Subscription **Owner**

Azure Subscriptions

Isolation of Cost and Business units

Policies
RBAC [IAM]
Create RG's
Custom RBAC Roles

G1

DNS Zones - External
Storage Accounts GRS
- Staging
Traffic Manager

Deployment Service Principal -RG **Contributor**

Azure Global Resources - RG

Global Dependencies - Shared Services

RBAC [IAM]

AZE2
P0

AZC1
P0

ER Gateways
Keyvault
Azure Firewall
Vnet Peerings to Spokes
Vnet Peerings to Regional Hubs
Automation/Recovery Services
DNS Zones - Private

Deployment Service Principal -RG **Contributor**

Azure Regional Hubs (VNet) - RG

Regional Dependencies - Shared Services

RBAC [IAM]

AZE2
S1,D2,T3,
U4,Q5,P6

AZC1
S1,D2,T3,
U4,Q5,P6

Most resources
Virtual Machines
Application Keyvault
Application Gateways
Load balancers
Automation/Monitoring
Recovery Services
Managed Service Identities

Deployment Service Principal -RG **Contributor**

Azure Regional Spokes (VNet) - RG

Isolate Application Environment -Stamp

RBAC [IAM]