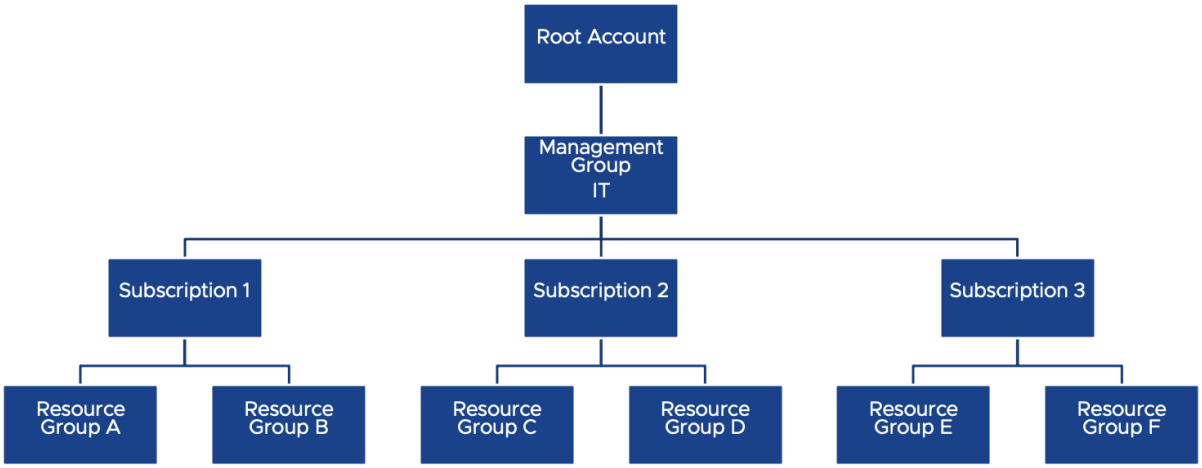
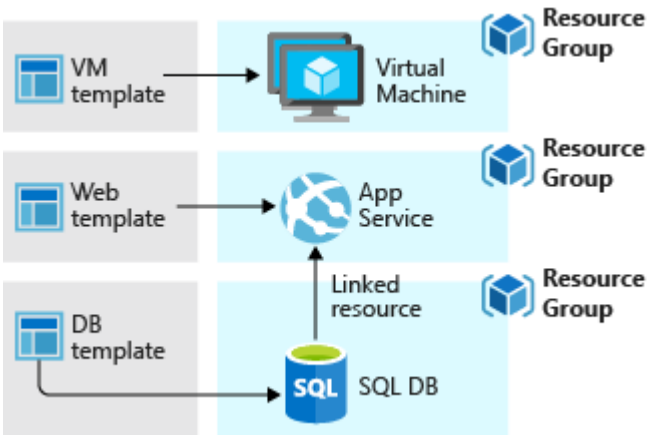
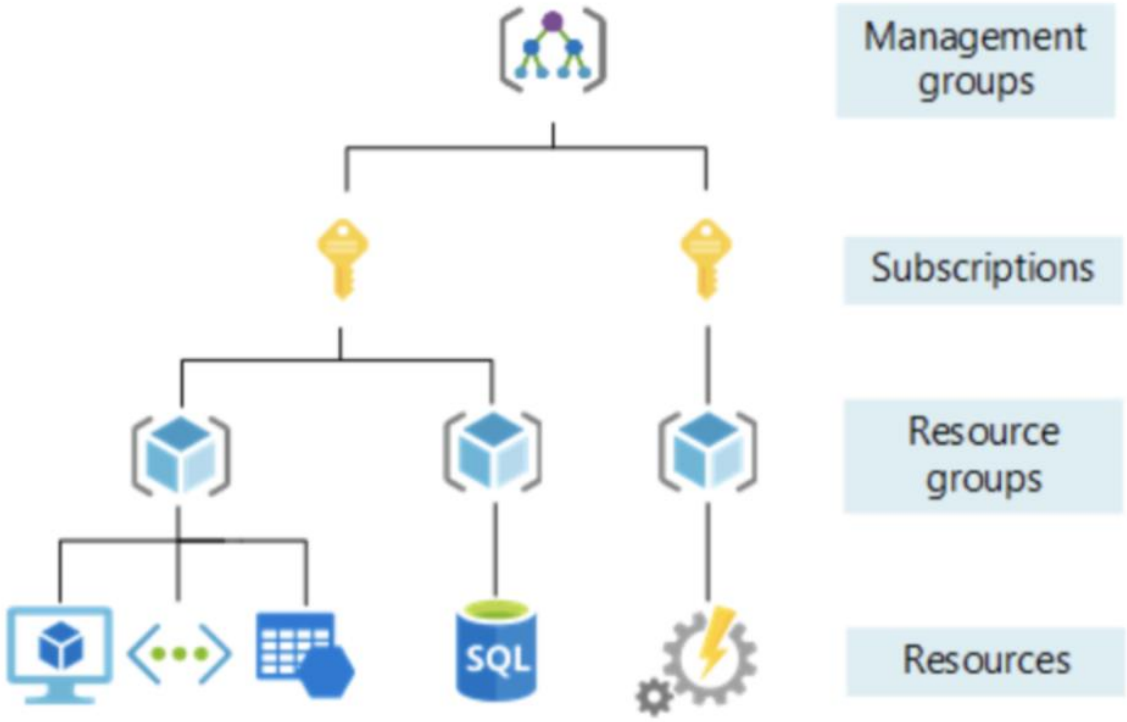
# Azure Resource Groups






Microsoft Azure lets you manage 4 specific areas of management for your resources which include the following:

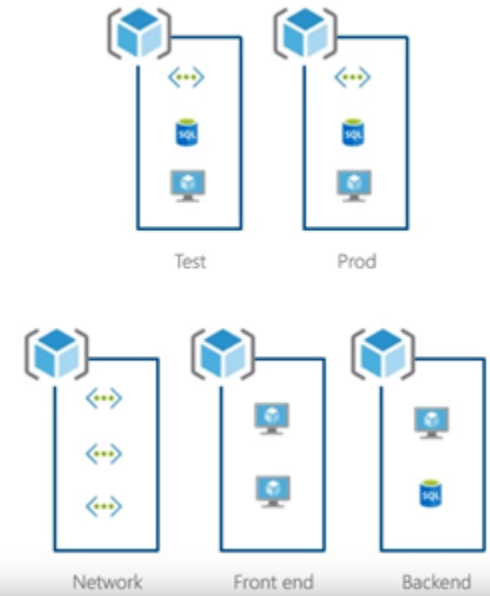
- Management Groups
- Subscriptions
- Resource Groups
- Resources

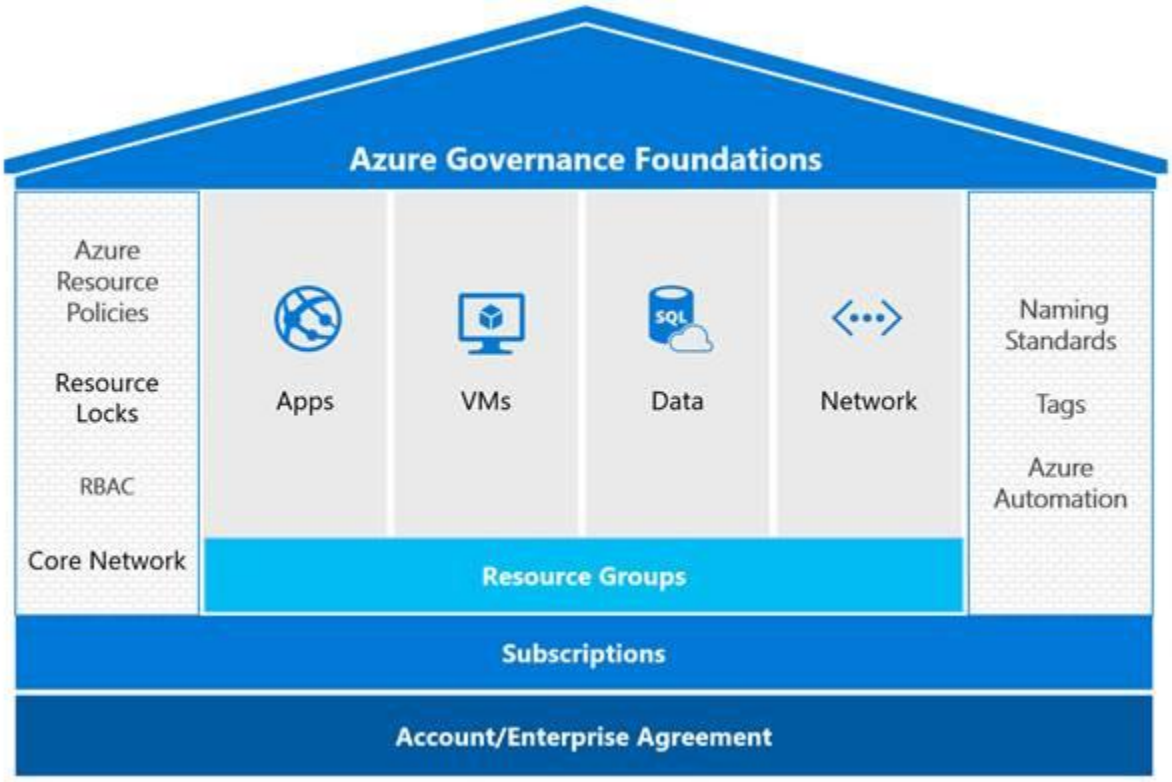




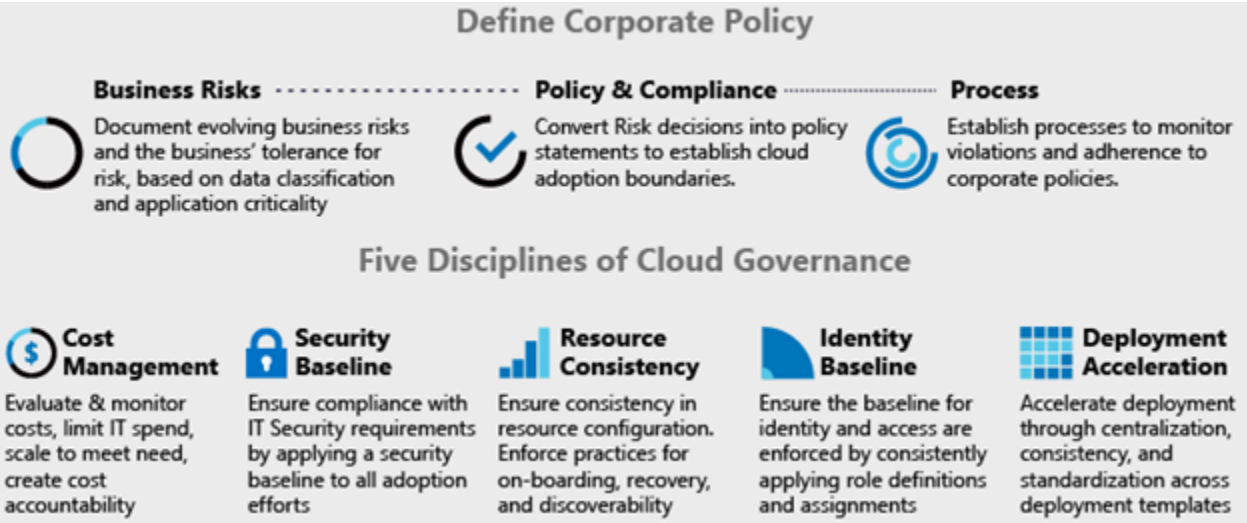

# Resource Group Strategy

- Resource groups give you an opportunity to add a governance control to a set of resources
- Some organizations break up by environment type (prod, pre-prod)
- Recommended to break resource groups apart by component or workload
  - i.e. networking resources live together






**Five Disciplines of Cloud Governance**




# Governance basics

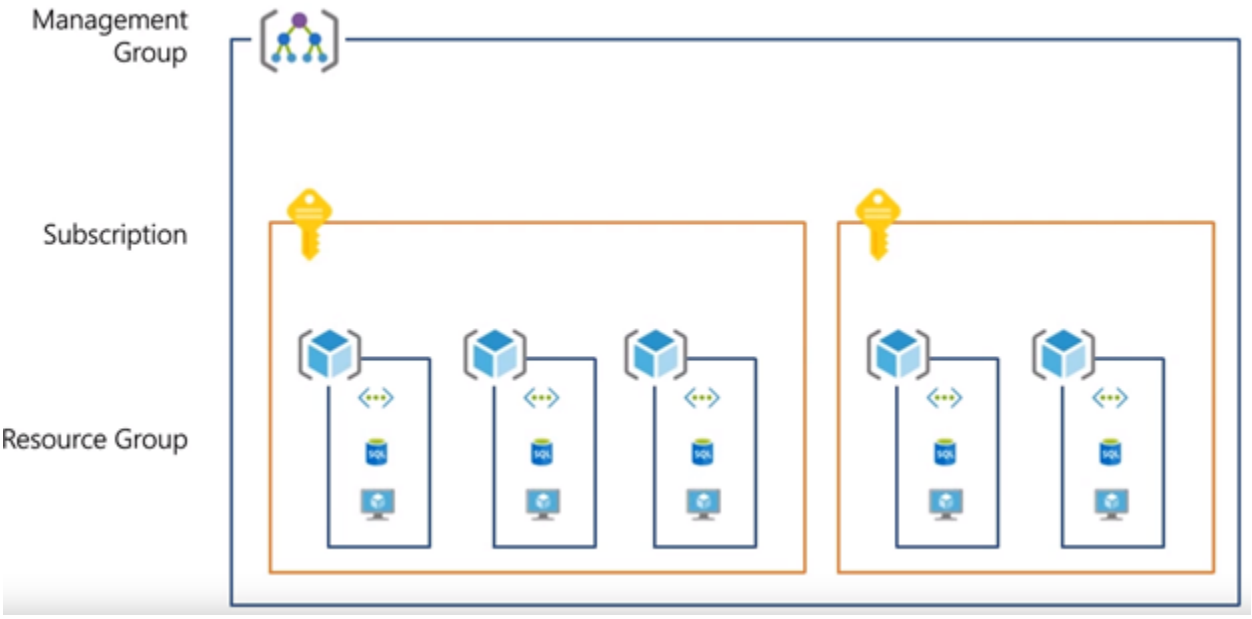
Following are the key components of the Governance for an Enterprise,

- Scope & Hierarchy

- RBAC
- Policy
- Azure Resource Manager Templates

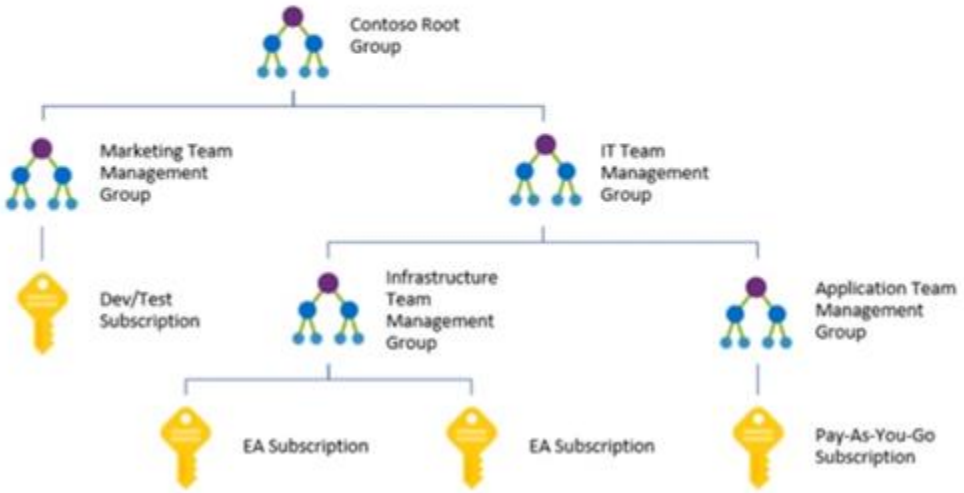
**Scope & Hierarchy**

Resource group stay in a subscription; a subscription is container for the logically similar resources. Management group is additional level of hierarchy which help to administer subscriptions.




As per business need Management group hierarchy up to Six level (deep) can be created.

# Management group hierarchy




**Role-based access control**

Access management for resources is a critical function for any organization. Role-based access control (RBAC) helps you to manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Following actions with RBAC,

- Allow one user to manage VM in a subscription and another user to manage virtual networks
- Allow a DBA group to manage SQL databases in a subscription
- Allow a user to manage all resources in a resource group, such as VM's, websites, and subnets
- Allow an application to access all resources in a resource group

**RBAC Recommended Practice**

Using RBAC, you can isolate duties within your team and grant only the amount of access to users that they need to perform their jobs.

Instead of giving everybody open permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope.

When planning your access control strategy, it's a best practice to grant users the least privilege to get their work done. The following diagram shows a suggested pattern for using RBAC.

# RBAC key info

- Restrict who can perform what operations on which resources
- Inherited to all children of the assigned scope
- Can be applied to all levels of your hierarchy, all scope types
- Custom roles allow you to change the operations that a role can perform