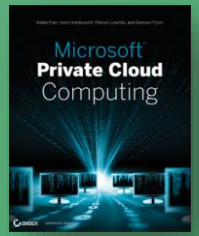
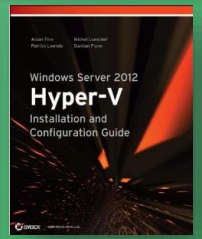
Damian Flynn

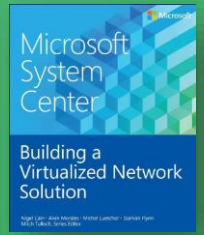
Microsoft Azure MVP
Cisco Champion
www.DamianFlynn.com
@damian_flynn

INNOFACTOR

- Cloud Governance + DevOps Evangelist
- Azure Management Elite + Advisor
- IoT & Embedded Microcontroller's
- KNX, CBus, Iridium Certified

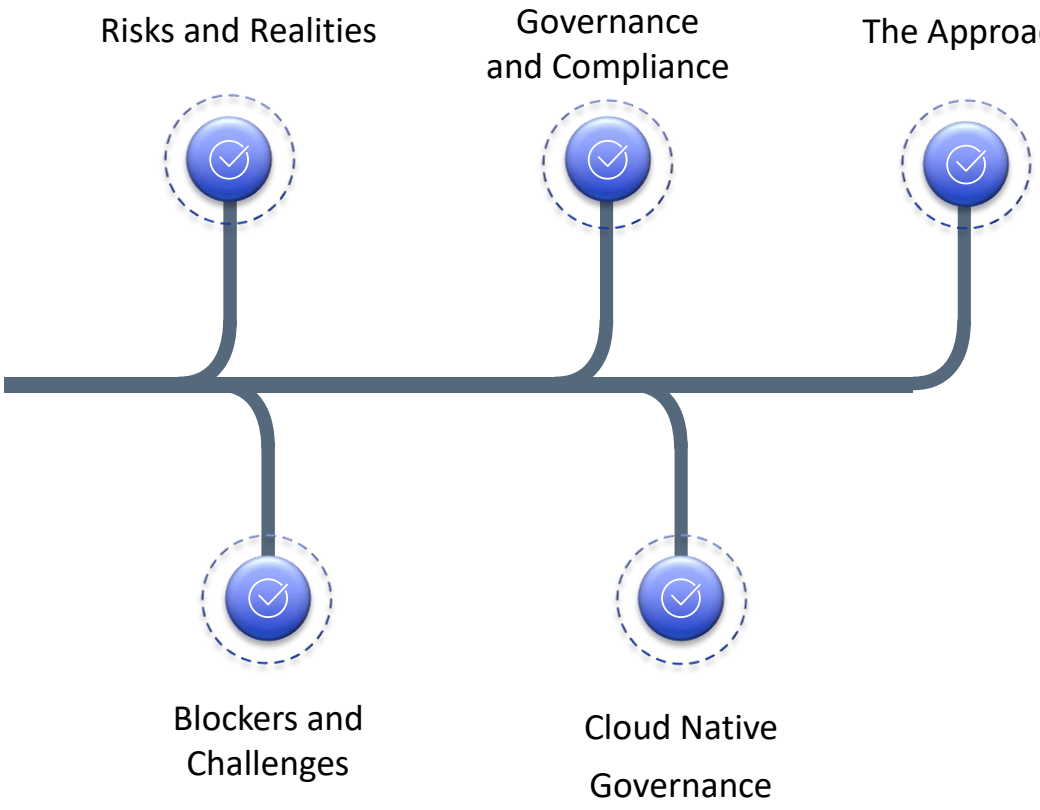




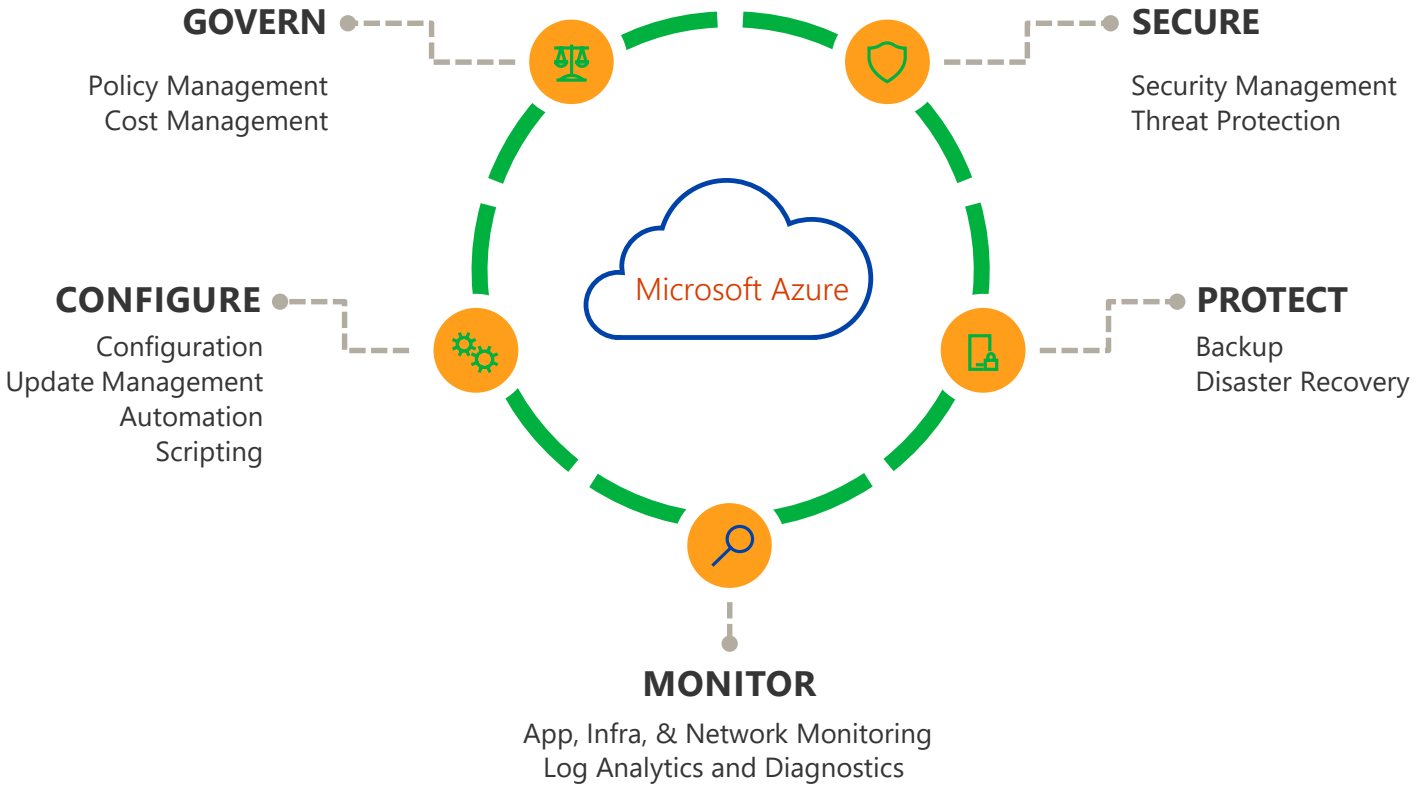


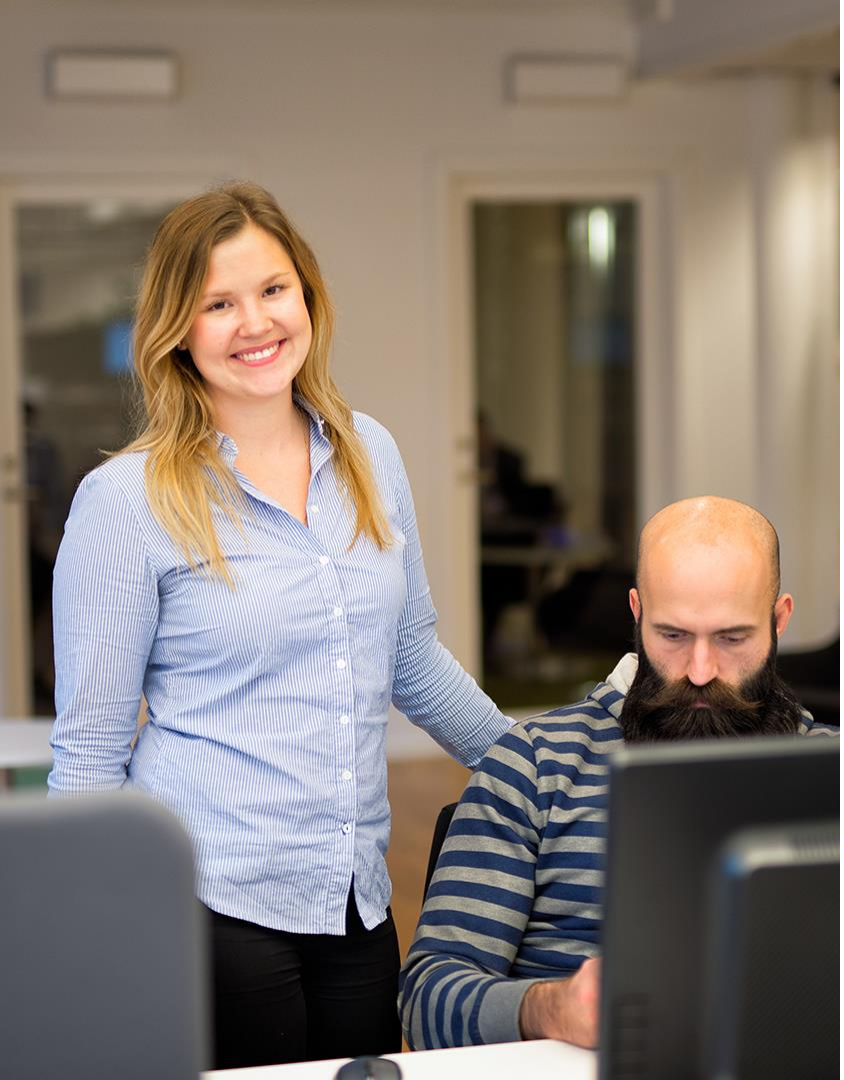
Agenda

Re-Scaffolding Cloud Fabrics
with Trust



Governance is essentially the activity of defining, continuously monitoring, and auditing the rules, guidelines, policies, and processes that allocate, coordinate and control a given operation’s resources and actions. In short, establishing and auditing the application of existing ruling.


GOVERN
Policy Management
Cost Management
SECURE
Security Management
Threat Protection
Microsoft Azure
CONFIGURE
Configuration
Update Management
Automation
Scripting
PROTECT
Backup
Disaster Recovery
MONITOR
App, Infra, & Network Monitoring
Log Analytics and Diagnostics



Realities

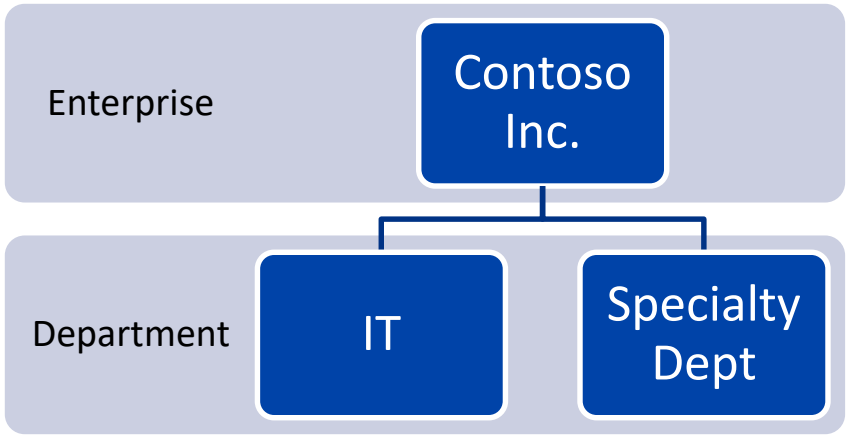
- Central Cloud Engineering
  - Cloud Custodians
  - Cloud Asset Managers
  - Effectively the **Central IT** for the Cloud era
- Cloud Sprawl
  - Cloud resources rapidly created by team without proper configuration and clear business alignment
  - Reminiscent of early 2000’s VM Sprawl

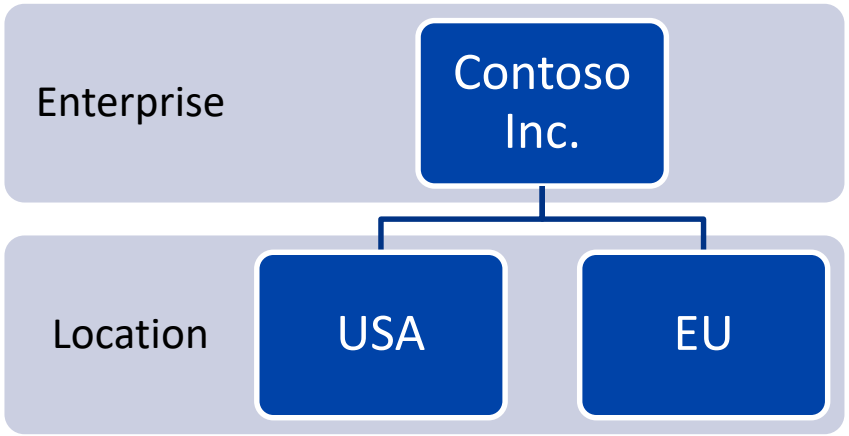
Challenges

- Cost Control
- Risk Mitigation
- Account Structures
- Complicated
- Business Disruption
- Service Availability
- Scale
- Security

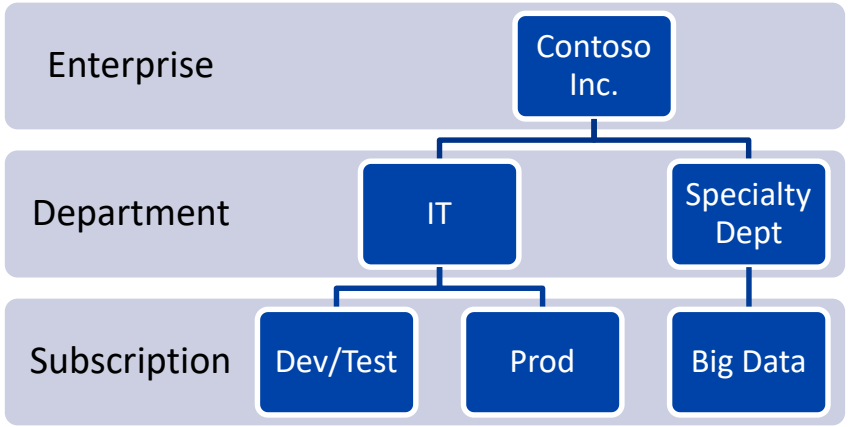
Structure Planning

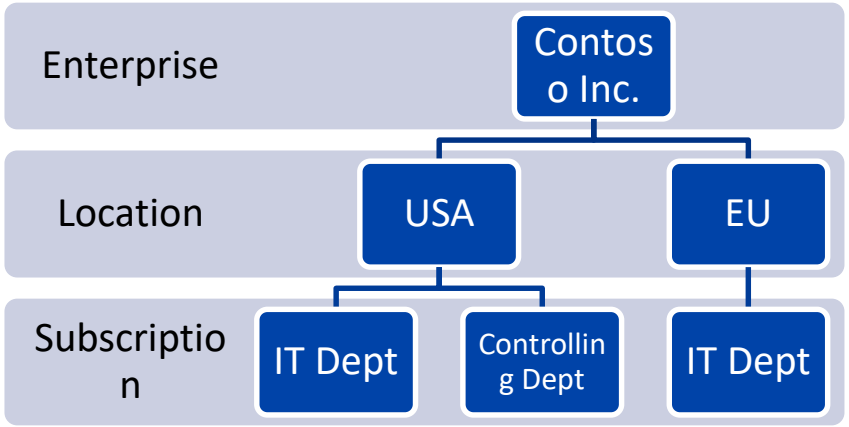
Structure Planning



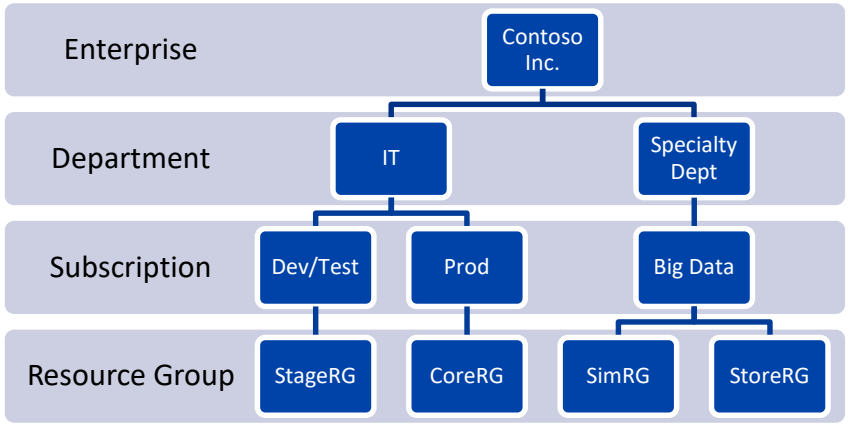


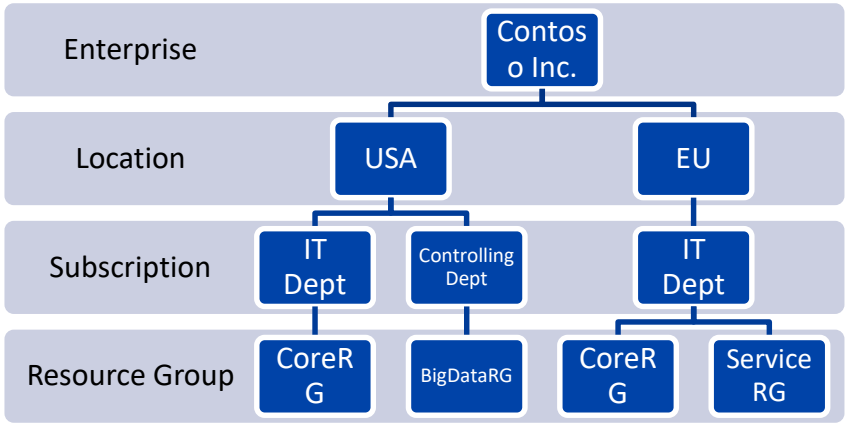
Structure Planning



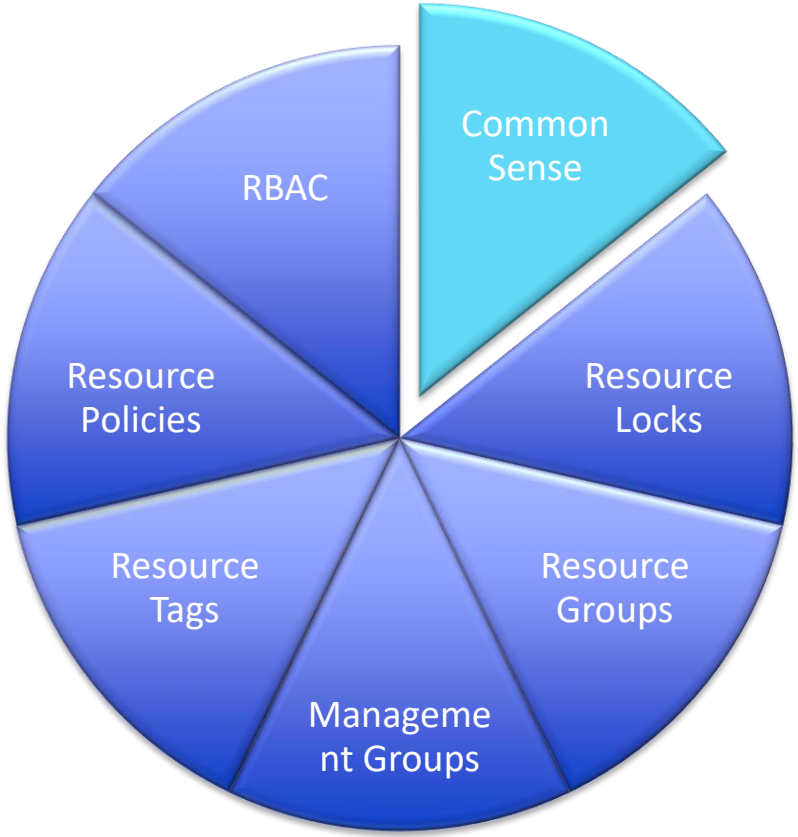


Structure Planning





Governance


Common Sense
RBAC
Resource Locks
Resource Policies
Resource Groups
Resource Tags
Management Groups

Common sense…

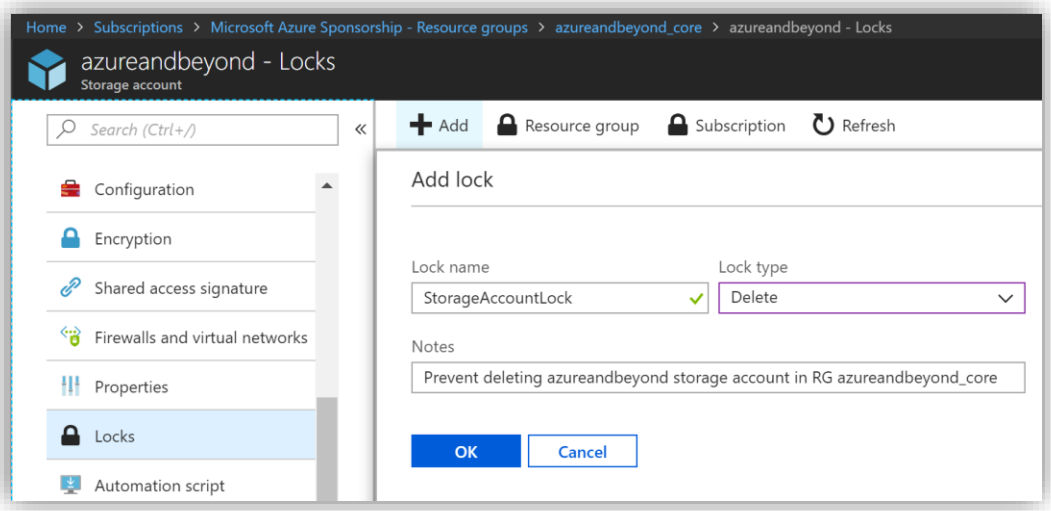
…is not so common.

- Voltaire

Governance: Resource Locks

Governance: Resource Locks

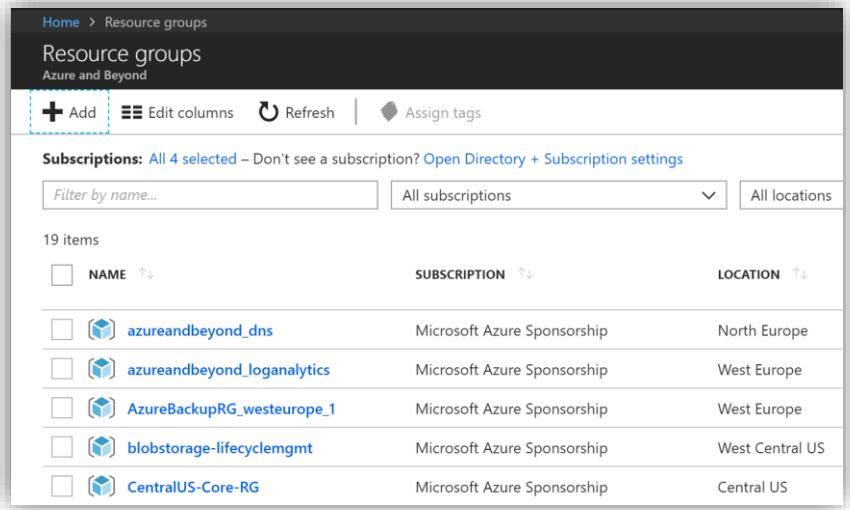
- Locks protect resources
  - Delete locks
  - ReadOnly locks
- Define locks in advance
- Use them in combination with common sense (e.g. read only means read only!)



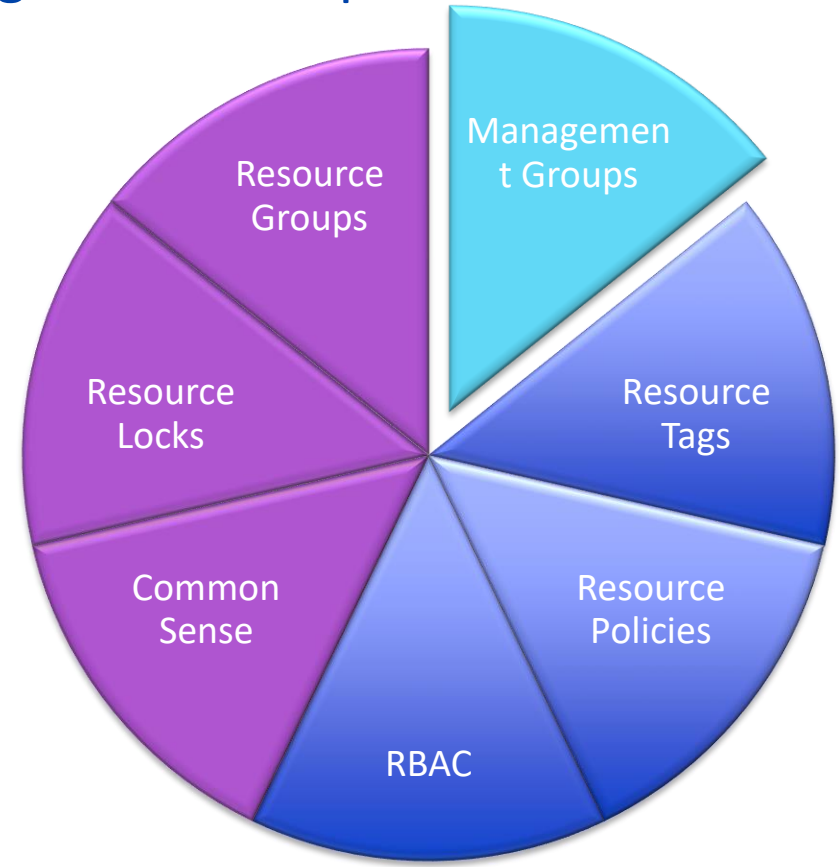
Governance: Resource Groups

Governane: Resource Groups

- Management
- Host resources in the same deployment lifecycle
- Assigned to a region but can contain resources that reside in different regions
- Every resource can only exist in one Resource Group
- Resources can be moved between Resource Groups



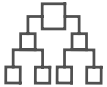
Governance: Management Groups



Introducing Azure Management Groups

Make environment management easier by grouping subscriptions together

- Grouping subscriptions into logical groups allow for new organization models
- Inheritance allows for single assignment of controls that apply to all subscriptions
- Aggregated views above the subscription level



Create a hierarchy of management groups that fit your organization

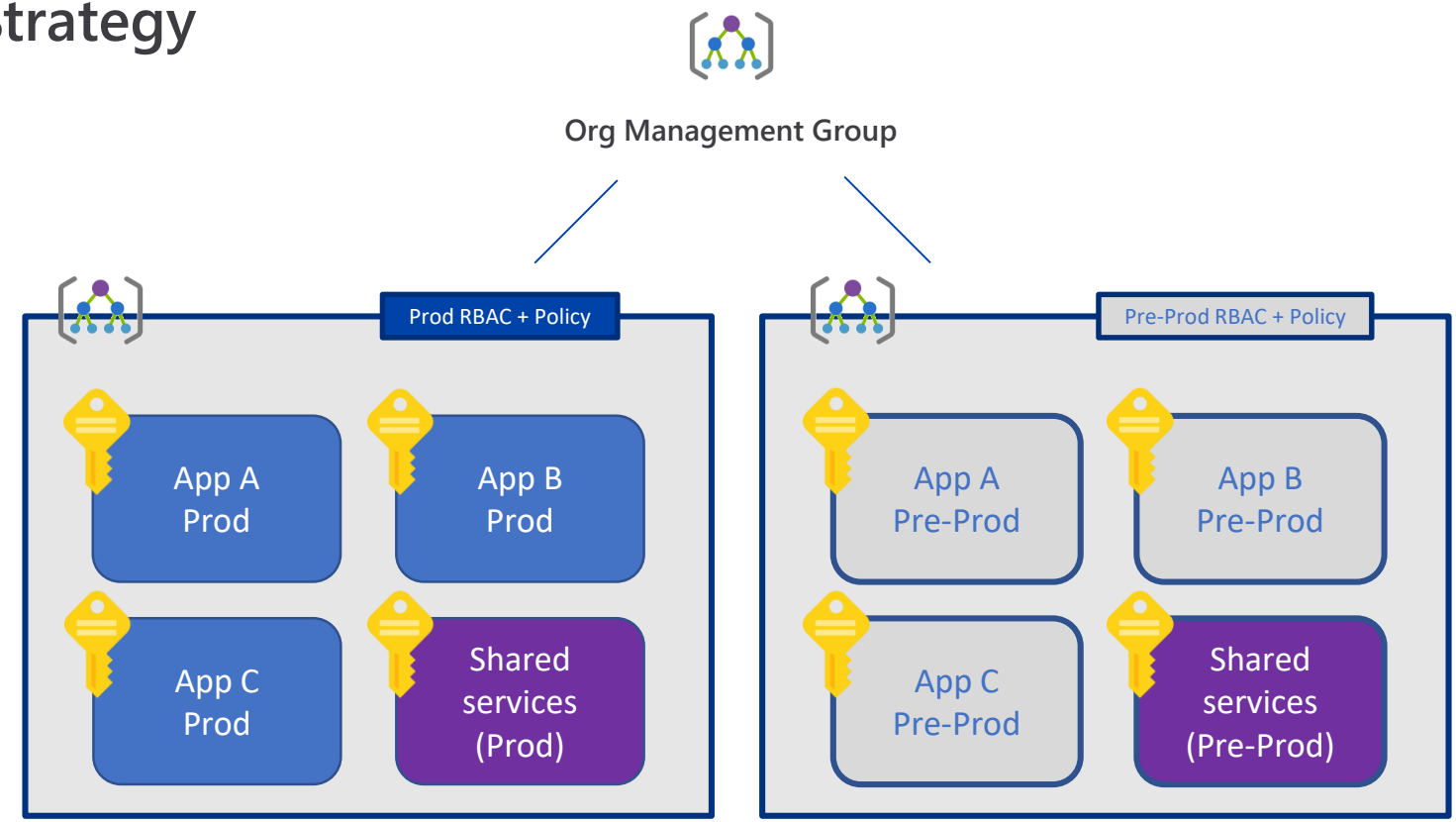
- Create a flexible hierarchy that can be updated quickly
- Hierarchy doesn't need to model the organizations billing hierarchy
- Can easily scale up or down depending on the organizational needs

Apply governance controls with policies and access controls along with other Azure services

- Azure Resource Manager (ARM) objects that allow integrations with other Azure services
- Azure services:
  - Azure Policy
  - RBAC
  - Azure Cost Management
  - Azure Blueprints
  - Azure Security Center

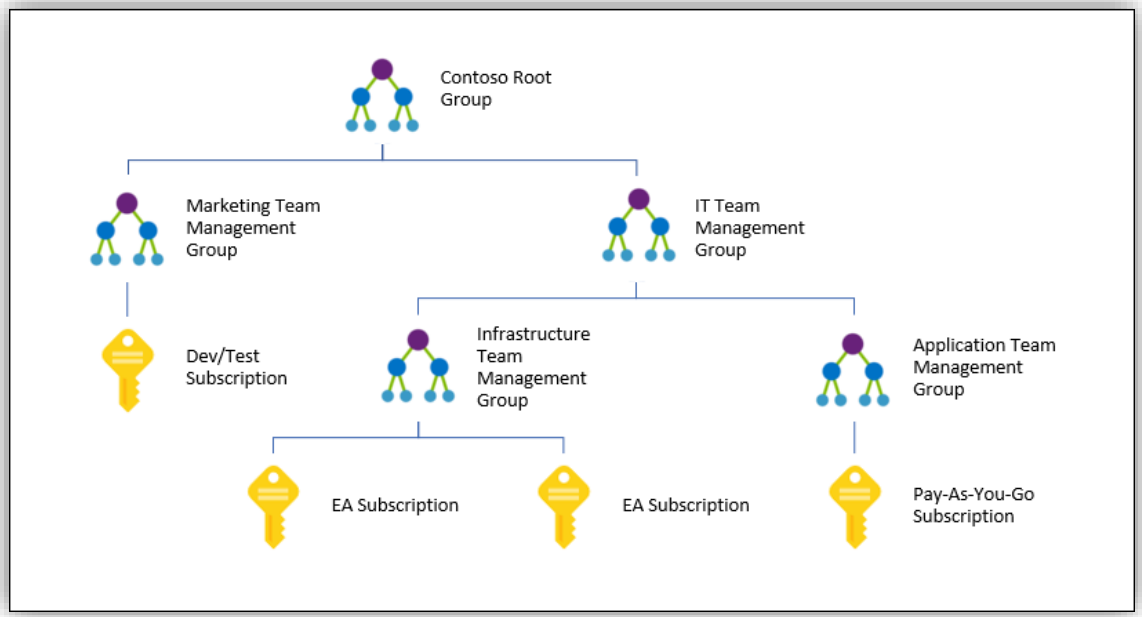
Management Group & Subscription Modeling Strategy

Microsoft Recommended



Governance: Management Groups

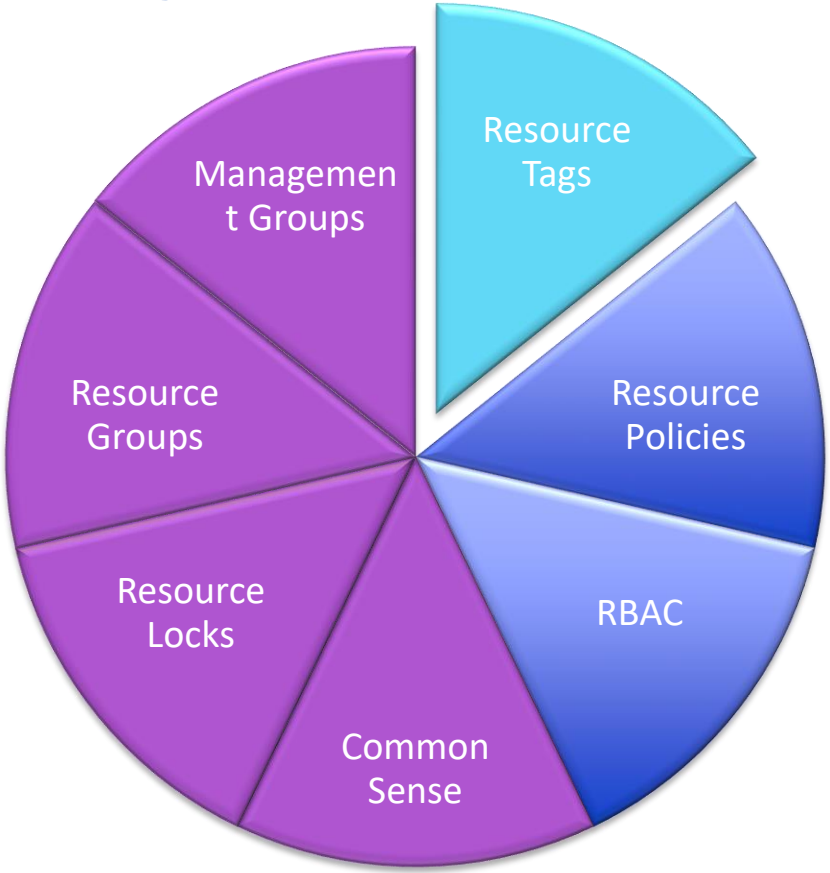
- Efficiently manage access, policies, and compliance
- Level of scope above subscriptions



Azure Management Group

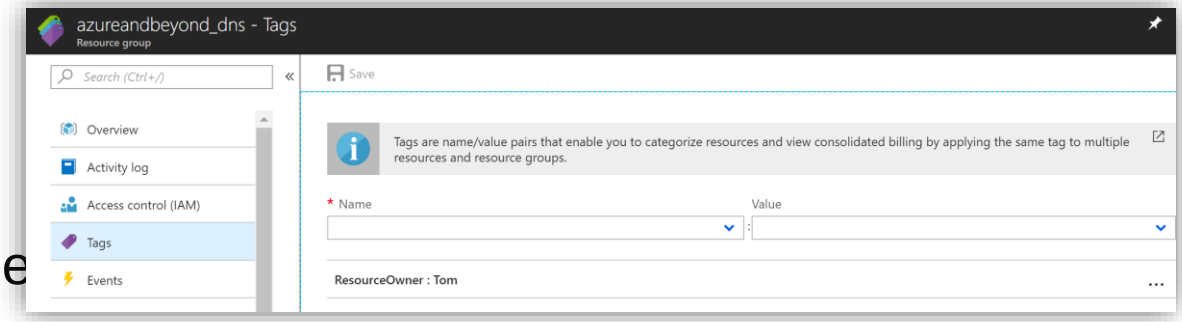
- It’s already there (sort of)
- Use inheritance wisely
- Use Management Group built-in roles (MG Contributor, MG Reader)

Governance: Resource Tags



Governance: Resource Tags

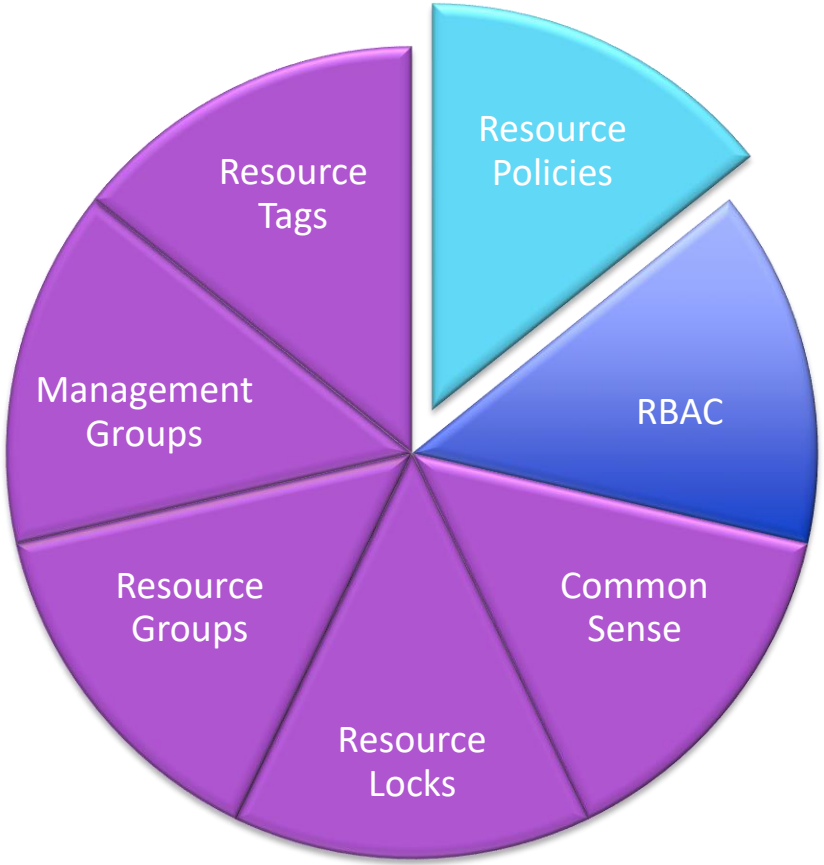
- Name:Value, e.g. CostCenter:ProdIT, ResourceOwner:Tom
- Help to define responsibility and view consolidated billing
- Always tag RGs
  - Owner
  - Dept
  - CostCenter
  - […]
- Tag resources as neede
- Define tags in advance




```
PS C:\> Get-AzureRmResource -TagName ResourceOwner -TagValue Tom | ft

Name              ResourceGroupName         ResourceType                    Location
----              -----------------         ------------                    --------
azureandbeyond.eu azureandbeyond_dns        Microsoft.Network/dnszones      global
lifecycletest     blobstorage-lifecyclemgmt Microsoft.Storage/storageAccounts westcentralus
```

Governance: Resource Policies



Azure Policy

- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation
- VM In-Guest Policy (NEW)

Enforcement & Compliance

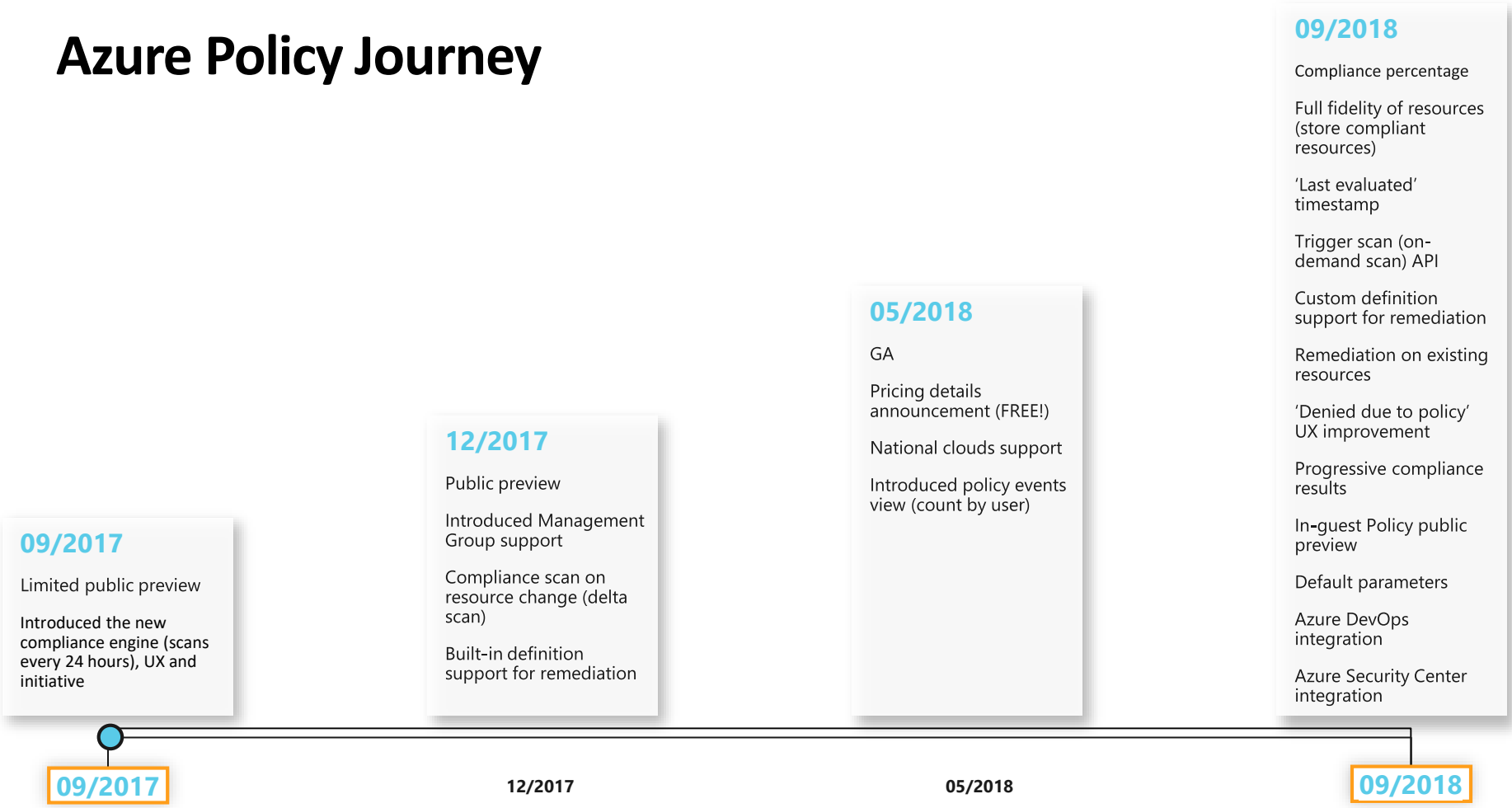
- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

Apply policies at scale

- Real time remediation
- Remediation on existing resources (NEW)

Remediation

Azure Policy Journey



Compliance evaluation frequency

On change

~15 min after resource change

On periodic cadence

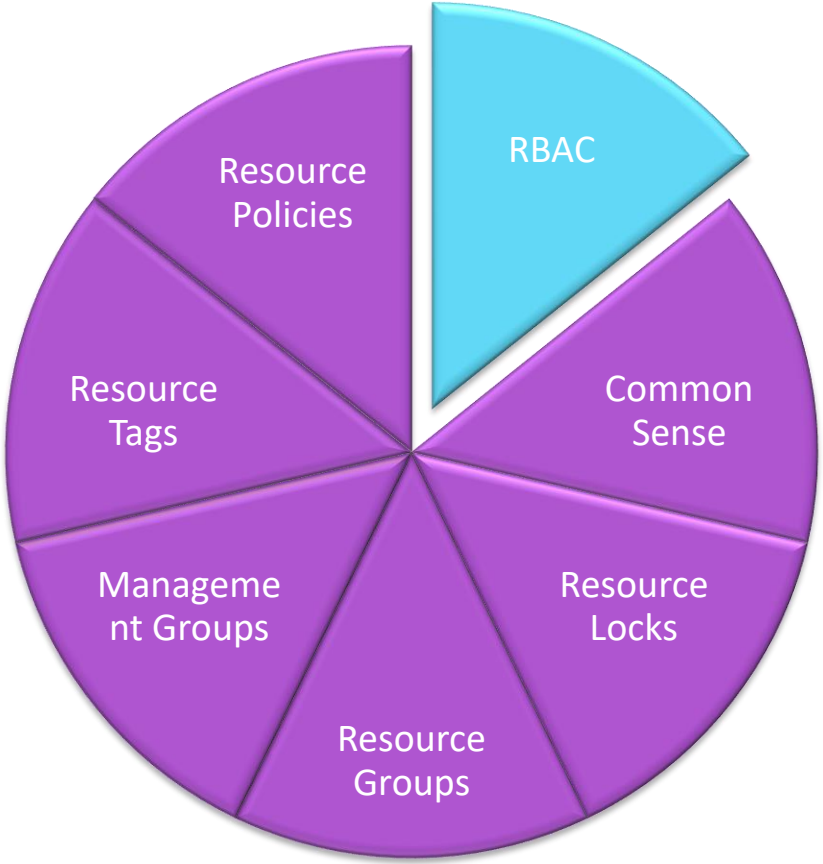
Every 24 hours

On demand

New/ updated assignment

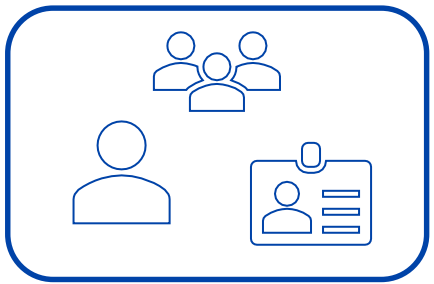
Trigger scan API

Governance: Role-based access control



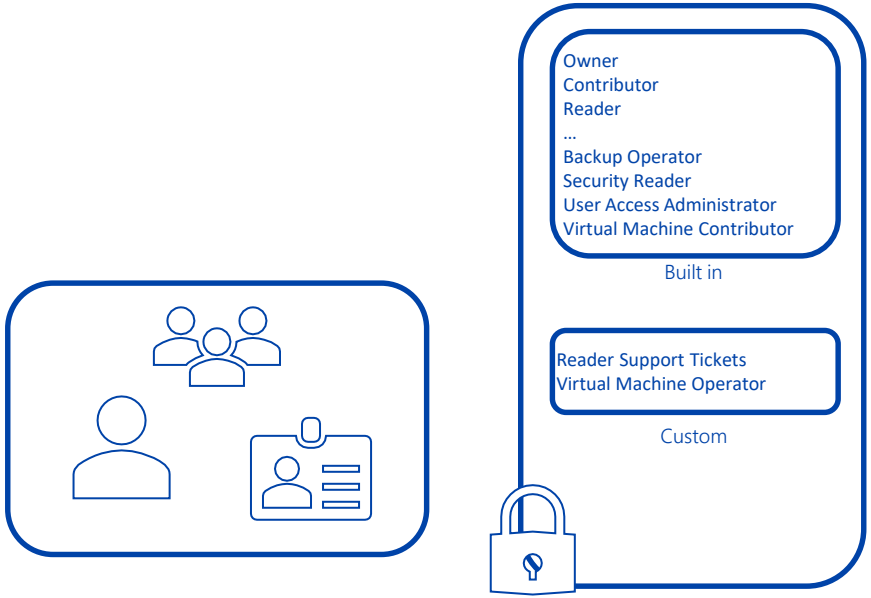
Governance: Role-based access control

1. Security principal = user, group, service principal



Governance: Role-based access control

1. Security principal = user, group, service principal
2. Role definition = set of management rights



Cloud Governance and Cloud Management must be cross functional responsibilities within a company and rarely if ever the dedicated responsibilities of a single employee or specific team.

Get In Touch

info@damianflynn.com

@damian_Flynn

www.DamianFlynn.com

linkedin.com/ie/DamianFlynn