Microsoft

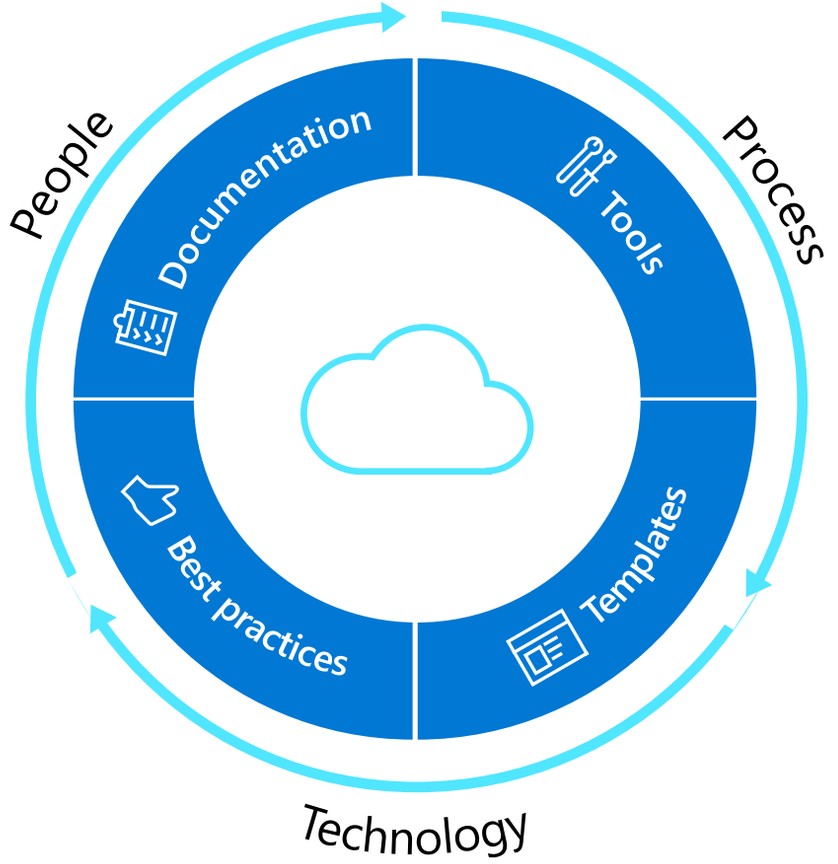
# Making Governance Easier for Customers
# Cloud Adoption Framework for Azure

# Microsoft Cloud Adoption Framework

# Overview

The Microsoft Cloud Adoption Framework (CAF) for Azure is a collection of documentation, technical guidance, best practices and tools that aligns strategies for business, organizational readiness, and technology to enable desired business outcomes faster and adopt the cloud with confidence

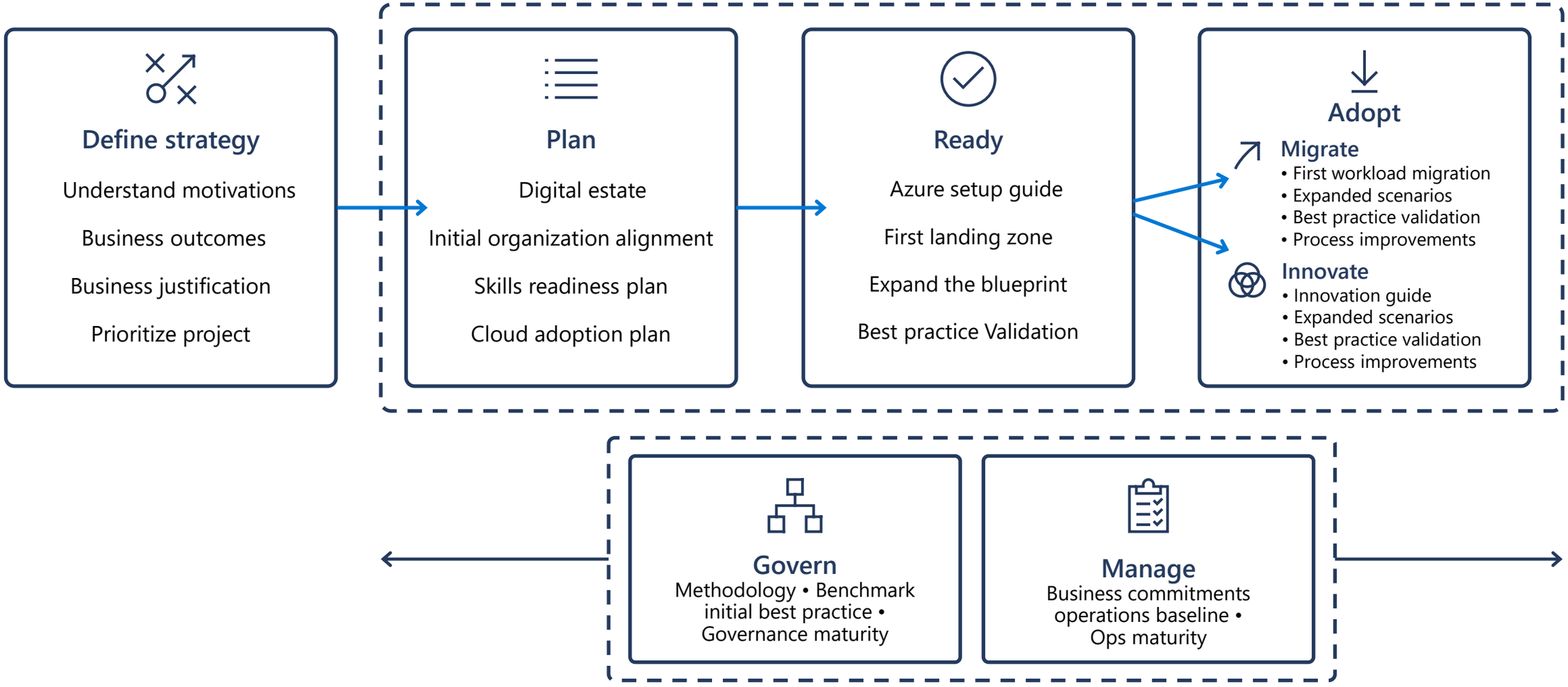
# Microsoft Cloud Adoption Framework for Azure





Align **business, people and technology strategy** to achieve business goals with **actionable, efficient, and comprehensive** guidance to deliver fast results with control and stability.

# Microsoft Cloud Adoption Framework for Azure

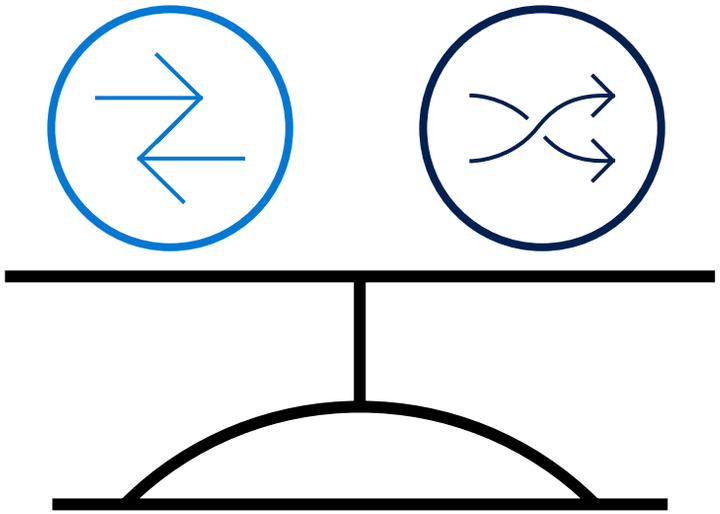


# Microsoft Cloud Adoption Framework

# Governance

# Objective of this Model: Create Balance

**Control & Stability**



**Speed & Results**

# Get started with cloud governance

1

## Methodology overview

Establish a basic understanding of cloud governance

2

## Governance benchmark

Assess your current state and the future state to get started

3

## Initial Governance Foundation

Begin establishing your governance foundation by implementing a set of governance tools

4

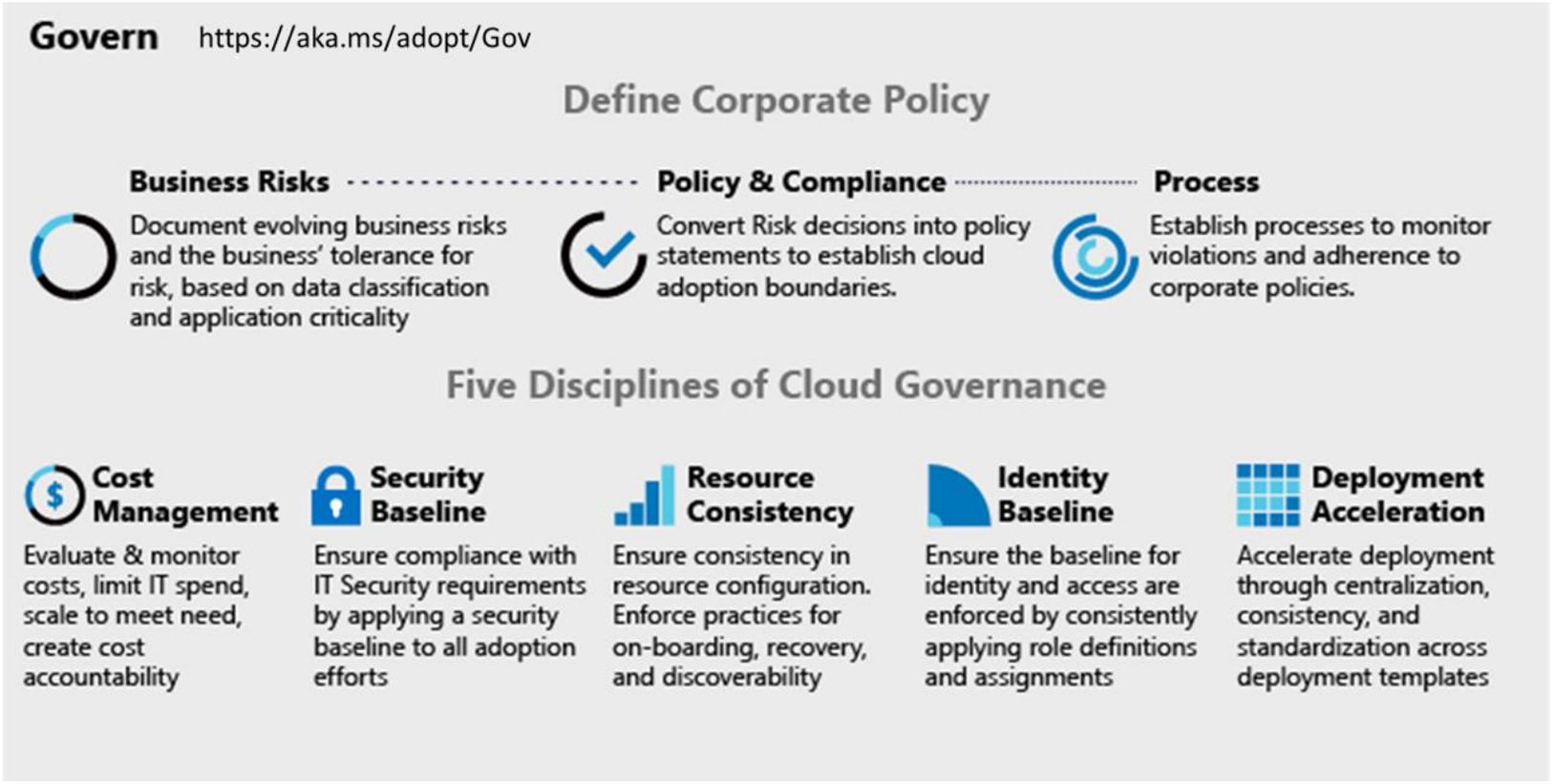
## Evolve Governance Foundation

Iteratively add governance controls to address risks

# 1. Governance methodology overview

# Cloud Adoption Framework | Governance Model

## Governance End State that fosters trust and builds confidence




### Corporate Policy

Governance is a big, intimidating topic. Establish proper scope by mitigating *tangible* risks through corporate policy.

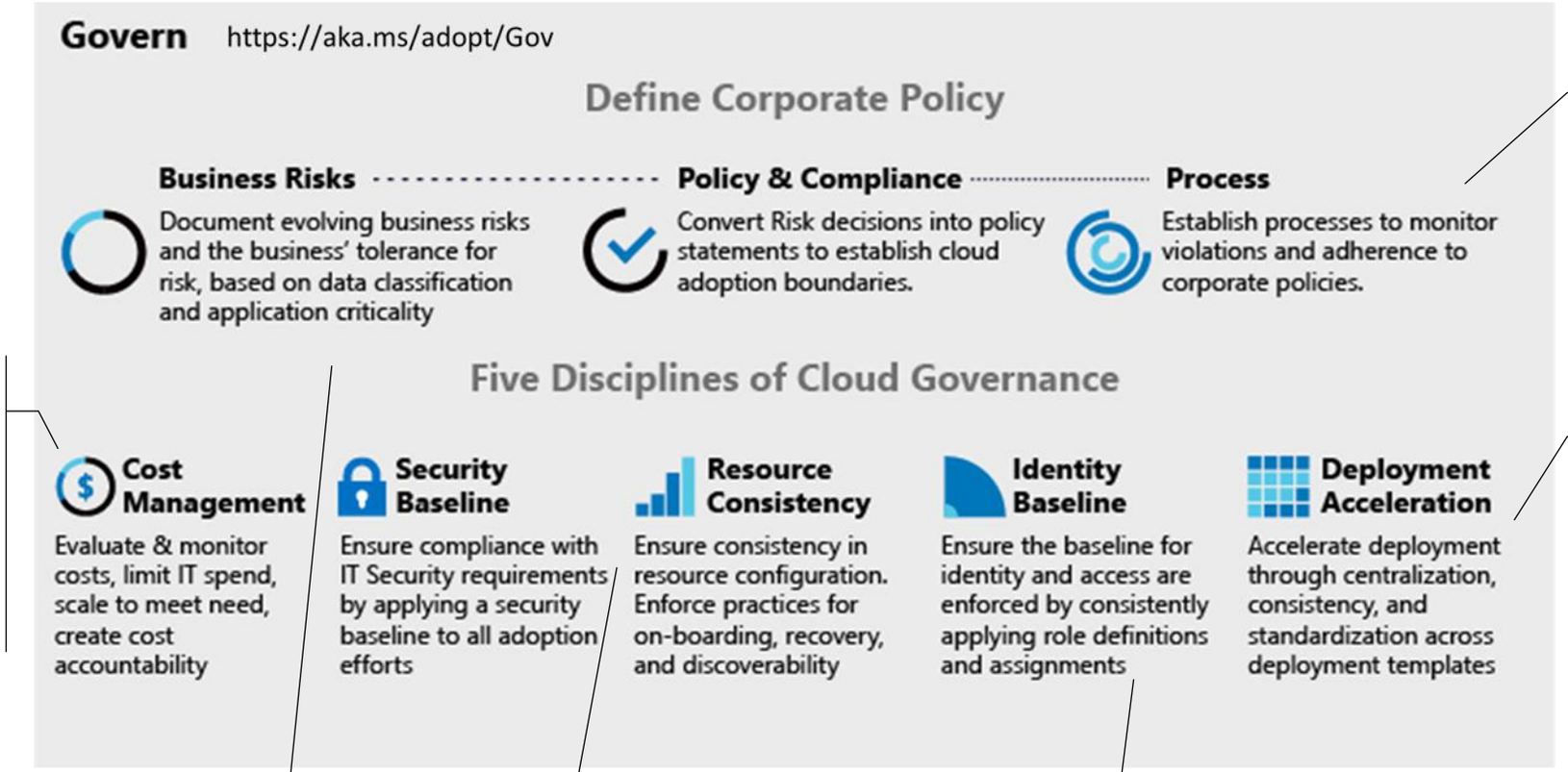
### Cloud Governance Disciplines

Governance is a team sport. Empower multiple team members by decomposing corporate policy changes into five actionable disciplines.

### Cloud Governance Team

A team of governance minded cloud architects can evolve these disciplines, ensure governance consistency, and accelerate deployment.

# Making Governance Actionable with Native Tools




**Azure Monitor**

- **Azure Blueprints**
- **Azure Policy**
- ***Azure Cost Management***
- ***Azure Advisor***
- Azure Portal
- Azure EA Content Pack

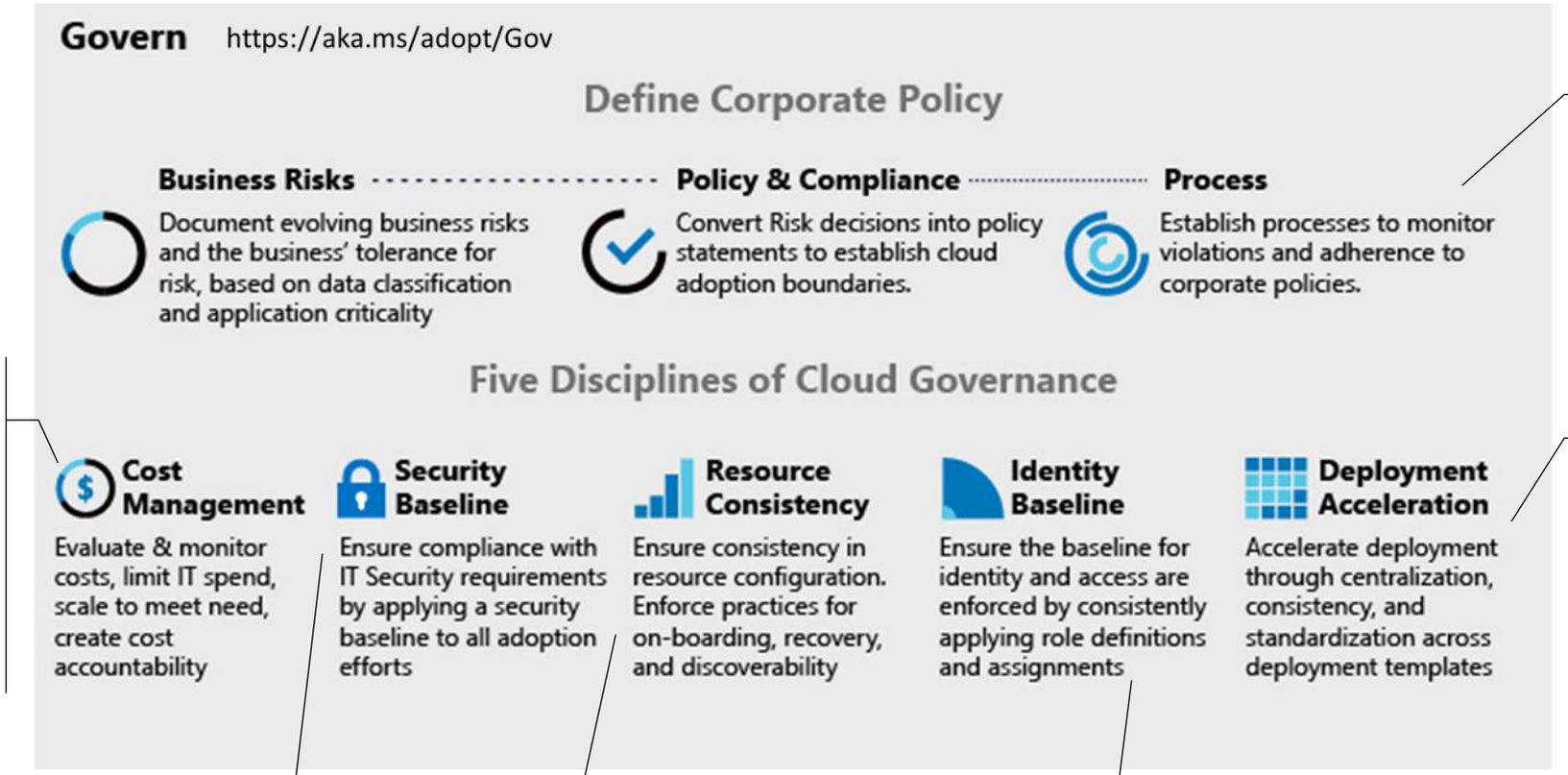
- **Azure Blueprint**
- **Azure Policy**
- **Resource Grouping & Tagging**
- **Resource Manager Templates**
- ***Azure Advisor***
- Azure DevOps
- Azure Site Recovery
- Azure Backup
- Azure Automation

- **Azure Blueprints**
- **Azure Policy**
- ***Azure Security Center***
- ***Azure Sentinel***
- Subscription Design
- Encryption
- Hybrid Identity
- Azure Networking
- Azure Automation

- **Azure Blueprints**
- **Azure Policy**
- ***Azure Monitor***
- ***Azure Advisor***
- Resource Manager Templates
- Resource Graph
- Management Groups

- **Azure Blueprints**
- ***RBAC***
- Azure AD
- Azure AD B2B
- Azure AD B2C
- Directory Federation
- Directory Replication

# Integrating 3rd Party Tools




**Monitoring 3rd parties**
- OpsCompass
- Splunk
- AppDynamics
- Solarwinds
- New Relic
- Data Dog

**Cost Management 3rd parties**
- HashiCorp Terraform (ROI tools)
- Cloudcheckr

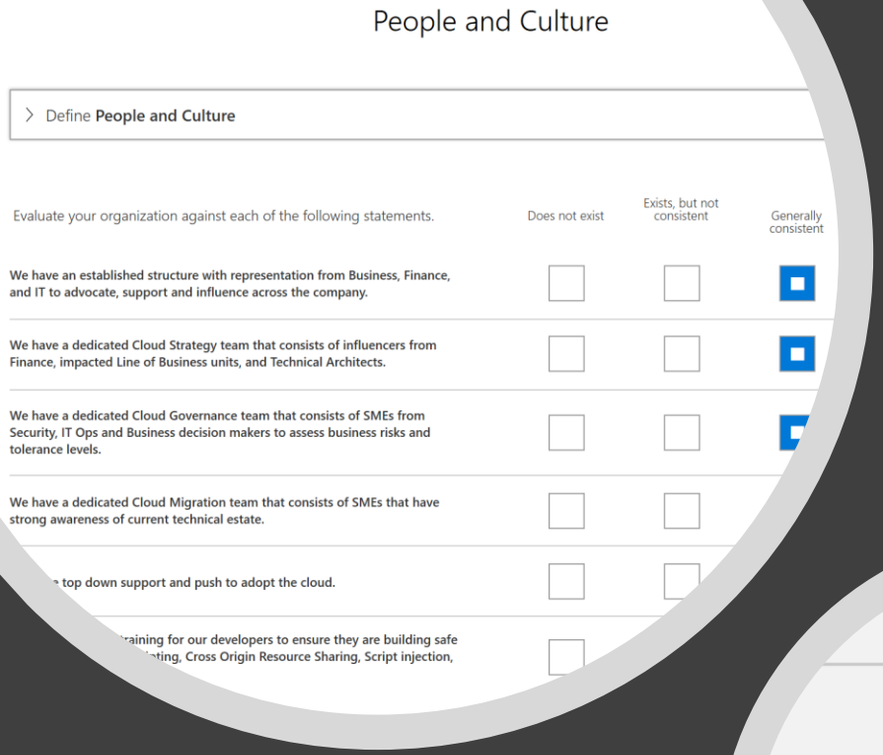
**Deployment 3rd parties**
- Nagios
- HashiCorp Terraform
- devops tools like Chef, Puppet, Ansible, Zabix

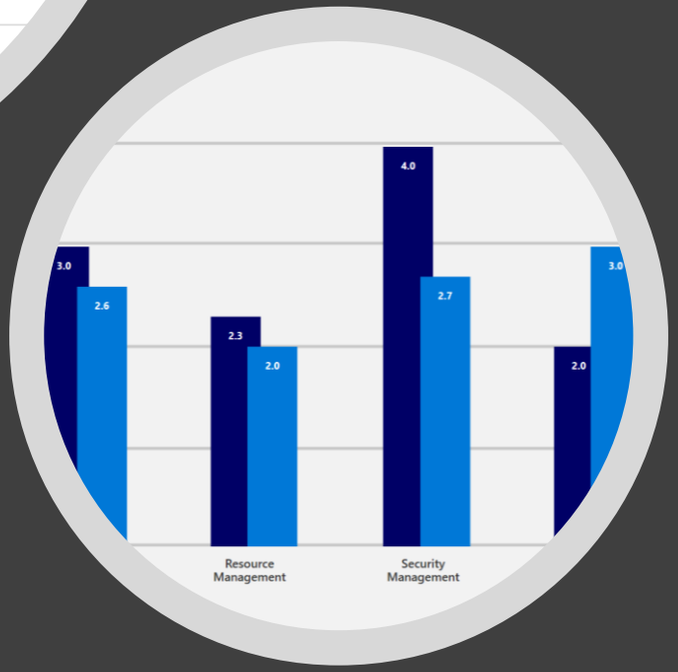
**Security baseline 3rd parties**
- Splunk
- HashiCorp Vault
- F5
- Gemalto
- Palo Alto
- CheckPoint
- Dome9

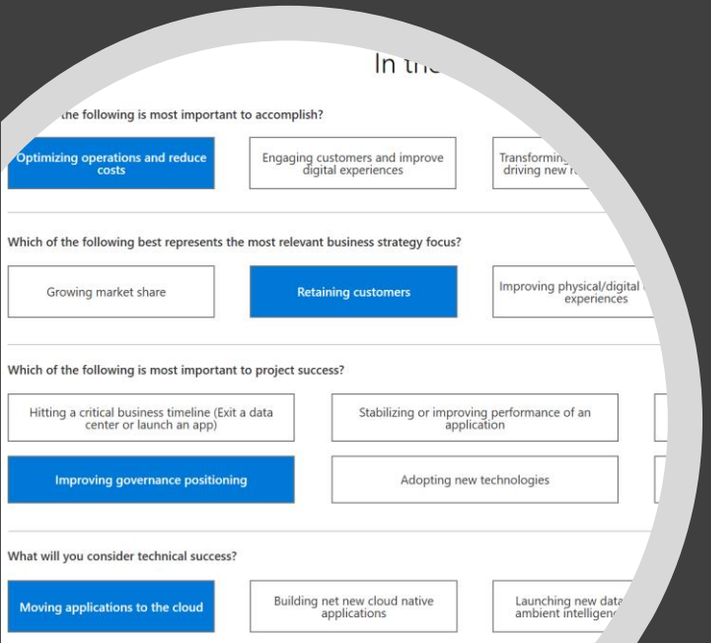
**Discovery, onboarding, and recovery 3rd parties**
- ServiceNow
- HashiCorp Terraform

**3rd party identity providers**
- HashiCorp Vault
- RSA
- Omada
- Ping Identity
- SailPoint

# 2. Benchmark your governance state




# Before we begin.....

Let's take a few minutes to capture current state of your governance using the "Governance Benchmark Tool"

http://aka.ms/adopt/gov/assess

# Workshop segment #1
# Engage stakeholders to understand business risks


Example:

1) What are your compliance requirements?
2) Have you identified your business risks as it relates to cloud?
3) What are your business priorities and reasons for moving to cloud?
4) How do you think about data risks and data governance?
5) Is there a list of applications which are prioritized by business impact?
6) Do you have specific application governance requirements?
7) How do you audit for compliance ?

# Workshop Lab A - Govern

## Governance Assessment

1. Read the Customer situation (slides are in the section called Customer situation)
2. Fill out the **Cloud Adoption Framework Governance Benchmark Tool** based on the information on the Customer situation.

   **Note:** Some of the information will be incomplete so feel free to take some liberties with the benchmark tool.

# 3. Defining Initial Governance for your organization

# Building the Governance MVP for your organization


## Governance MVP

Start small. Establish a foundation that can quickly evolve as cloud adoption and cloud governance mature. Mitigate tangible risks identified in the cloud adoption plans.

## Risk Evolutions

As additional iterations of cloud adoption are planned, the risk profile will change. The Cloud Governance Team monitors those adoption plans to identify risks and evolve corporate policy statements.

*Caution: take a balanced approach to implementation, audit then apply*


Microsoft
Build the Resource Consistency

# Workshop | Creating the resource mgmt. baseline

Estimated time frame: approx. ~ 2hrs

Participants: Cloud Architects

Outcomes:

- Management groups, Subscriptions, Tags

Requirements:

- Understanding of internal org structures, compliance requirements

Triggers:

- Getting started with Azure and need help in cloud environment setup
- Interested in learning about best practices in resource management in Azure

# Factors that influence the right setup

Organize Azure to reflect your organization, not the other way!

**Cost transparency:**

- Set up a cost structure that reflects the actual usage for departments and projects.
- Tagging and ownership
- Allowed resource types (policy)

**Roles and responsibility:**

- Who has access to what. Account owners and delegations (RBAC)
- Minimal access level to carry out the task.
- Design for Partners and 3rd parties

**Compliance and Security:**

- Allowed locations e.g. EU (policy)
- Network and connectivity (Internet facing, or using the approved VNETS? Policy and NSG)
- Continuous Monitoring and integration to existing ITSM (Azure Monitor)

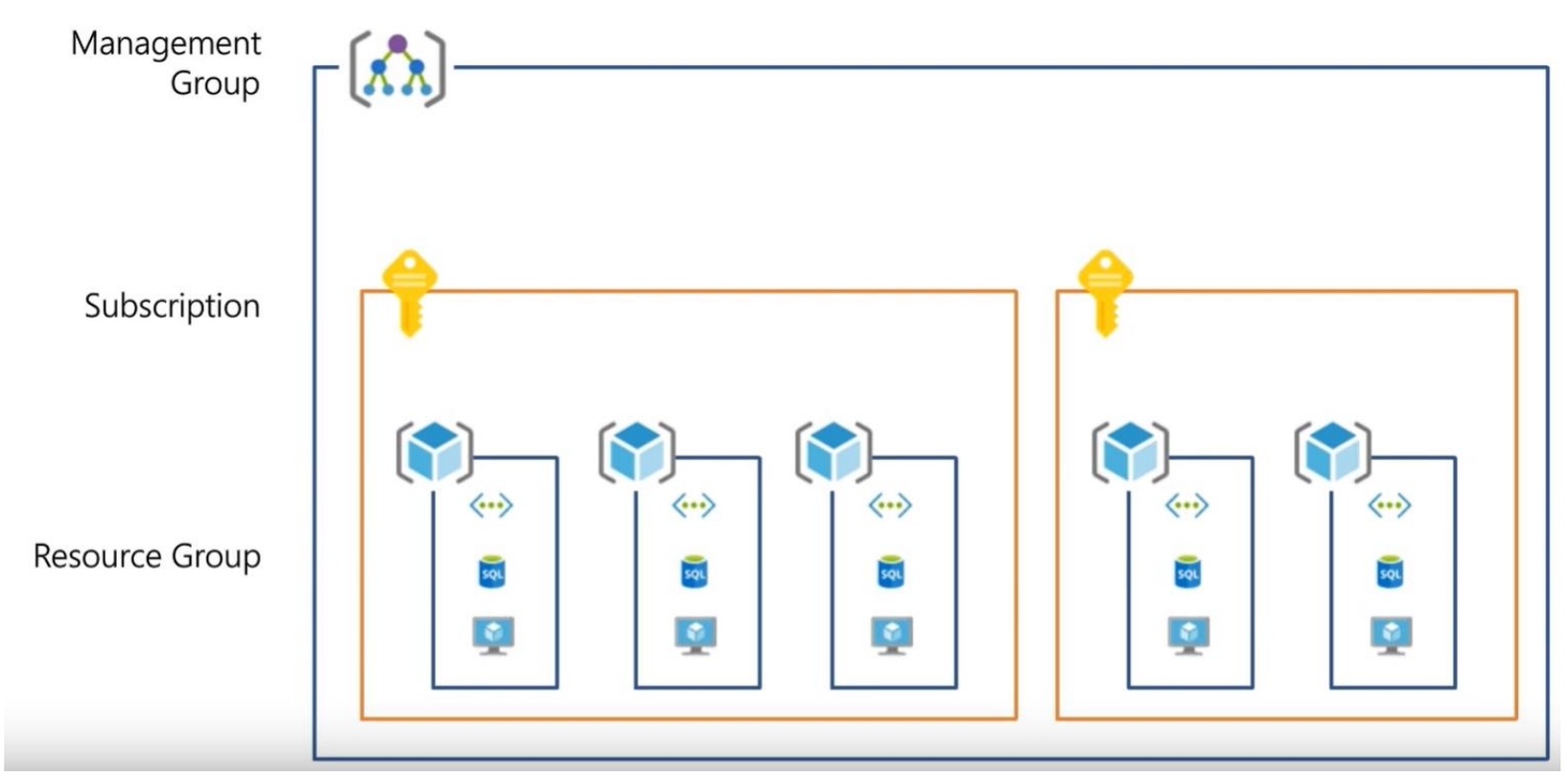
# What is Resource Consistency?

The basic foundation of all governance practices. Achieving the right Governance starts with the correct resource organization.

**Management Groups**: To reflect security, operations and business/accounting hierarchies

**Subscriptions**: To group similar resources into logical collections

**Resource Groups**: To further group applications or workloads into deployment and operations units

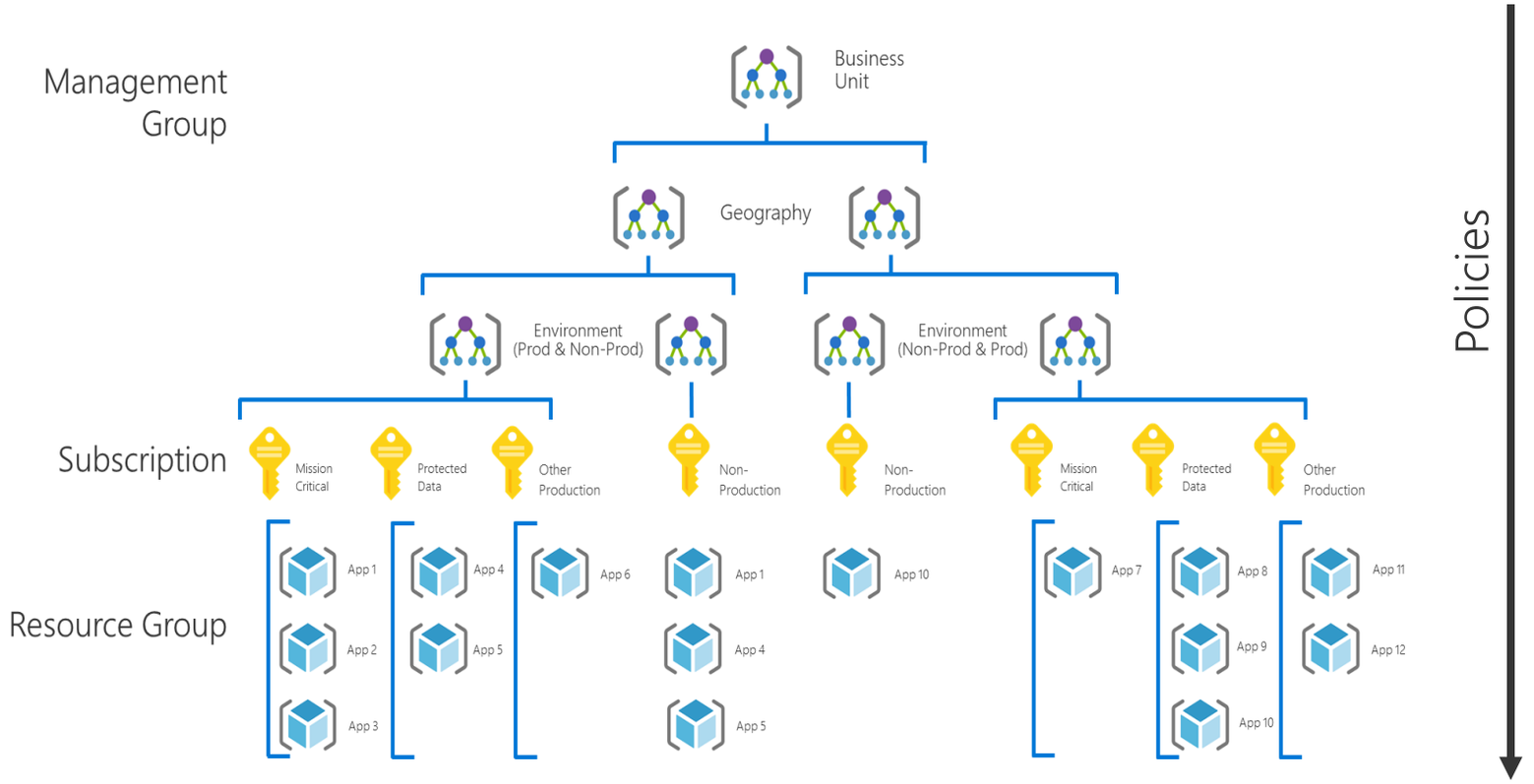


# Governance MVP Considerations

**Resource Organization:**

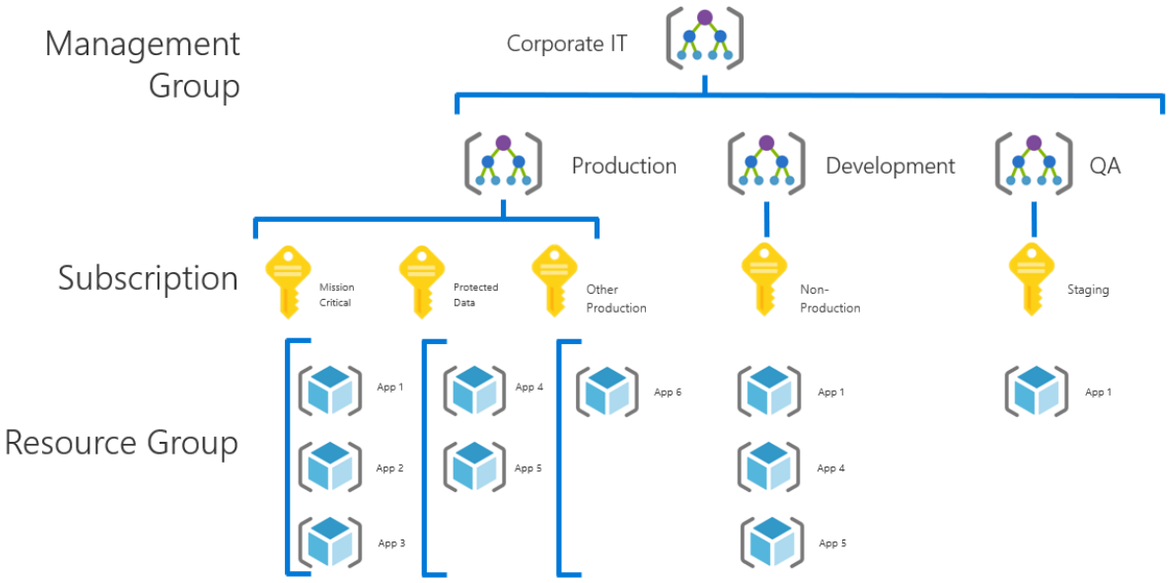
Build only what you need, add as the requirements are needed.

- Management Group Hierarchy: Business Unit, Geography, Environment.
- Subscription: Per Application Category; Pre-production, Dev environments, Production
- Resource Groups: Per Application



# Management Group best practices

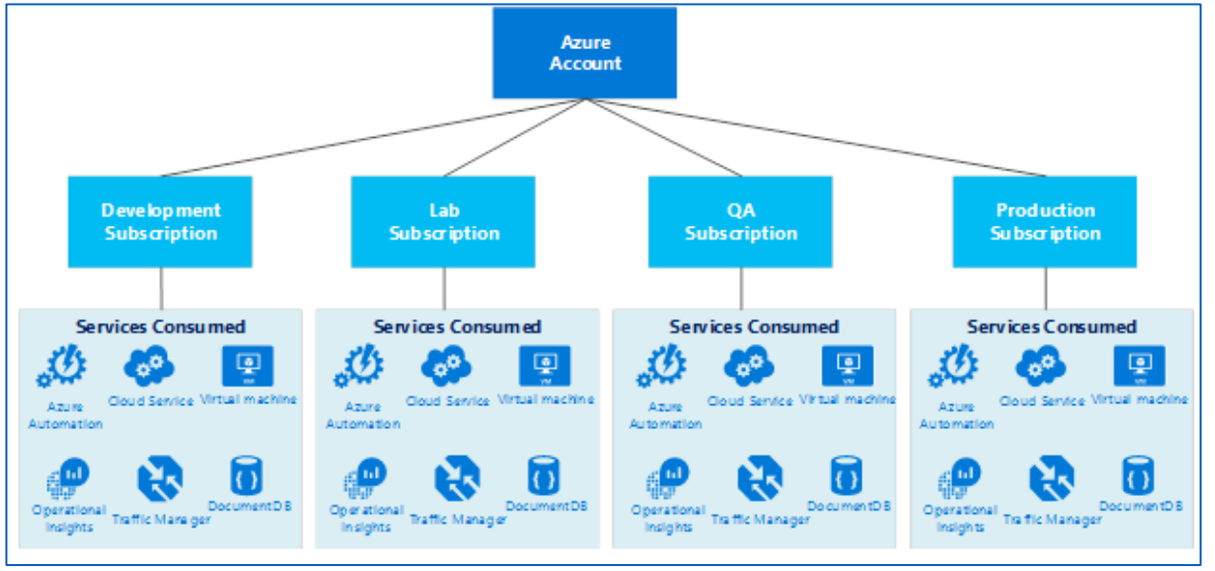
- Define your hierarchy based on organization and environment type (prod, pre-prod, etc.)
- The root MG is for global configuration
  - Be careful with MG level assignments as they will cascade through large chunks of your hierarchy
- Try not to repeat yourself. Assign common policies and RBAC higher up in your hierarchy
- Built-in RBAC roles for MGs (MG contributor, MG reader)
  - Need subscription owner access to move to another MG



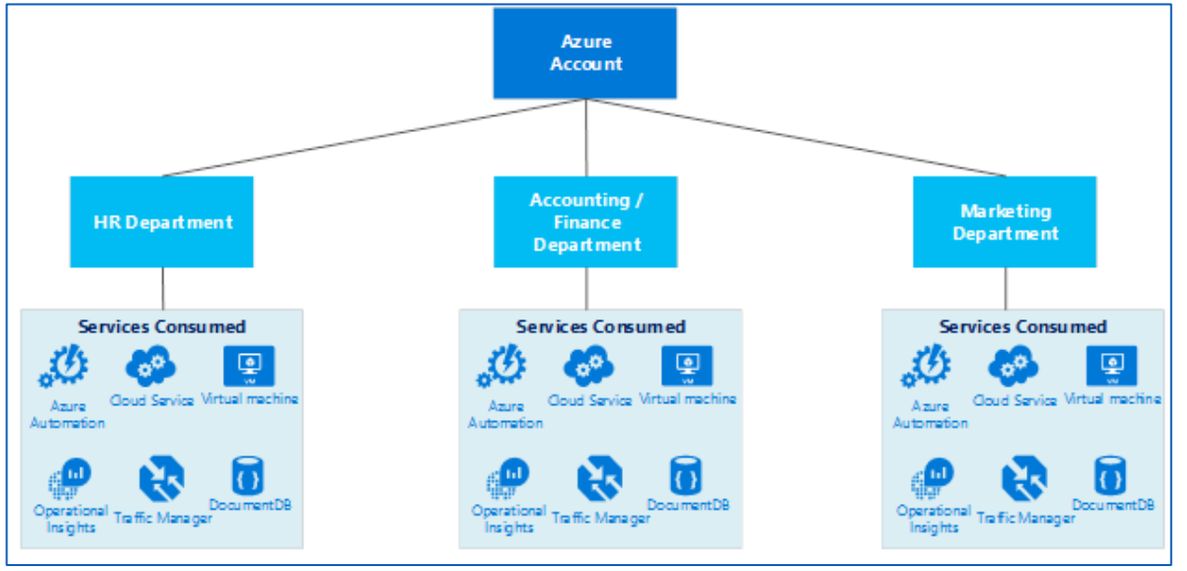
# Subscription | Design considerations

Develop the Subscription, Network, Storage, Availability and Administrative models together in order to have a cohesive approach.

Service (Process) Design Model




Organizational Unit Design Model




## Items to look at when designing the subscription model

Business Requirements
- Accountability
- Audit/Compliance
- Performance
- Availability & Recoverability

Technical Requirements
- Network Connectivity (shared or dedicated)
- Active directory requirements, clustering, identity, management tools

Security Requirements
- Who are the subscription administrators
- Least privilege model

Scalability Requirements
- Growth plans
- Allocation of limited resources
- Evolution over time (users, shared access, resource limits)

# Organize Subscriptions

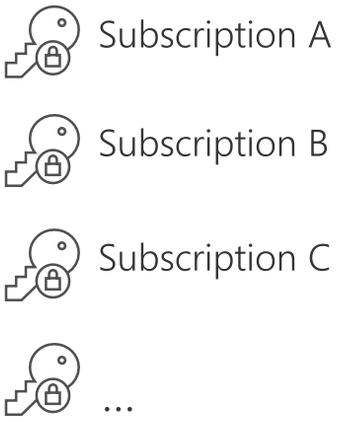
Ask yourself the following questions:

- Are there any capacity / technical limitations?
- Do we want to ensure separation of concerns? In example:
  - Separation of duties
  - Dev/Test Vs. Production
  - Different end customers
  - Different departments or business units
  - Different projects
- What is the right naming convention to be used?

  i.e.: `<Company> <Department (optional)> <Product Line (optional)> <Environment>`
- Use a dedicated subscription for shared infrastructure (i.e. Azure Active Directory, monitoring & patching tools…). You will be able to spread the cost of this mutualized infrastructure to app owners.

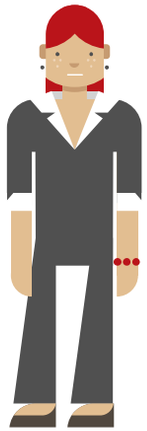
# Single subscriptions vs multiple | Considerations

- Subscriptions have different quota limits for different resource types
- At a certain level of usage you will need to create new subscriptions to scale out, so you need to have a strategy for doing so
  - A very crucial workflow that can slow down a lot of organizations
- Some questions you'll need to answer:
  - Who will be responsible for creating subscriptions?
  - What resources will be in a subscription by default?



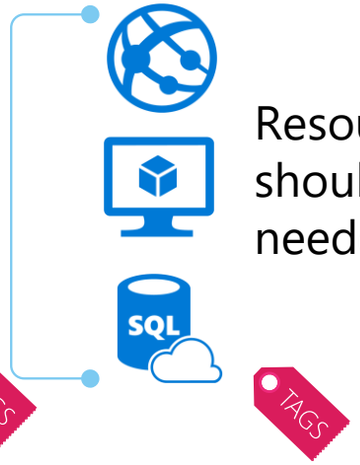
# Resource Groups, Tags and RBAC

Finance/Business



- Need to be able to break out costs by various dimensions such as Customer, Cost Center, Environment

Create Roles with Appropriate Permissions



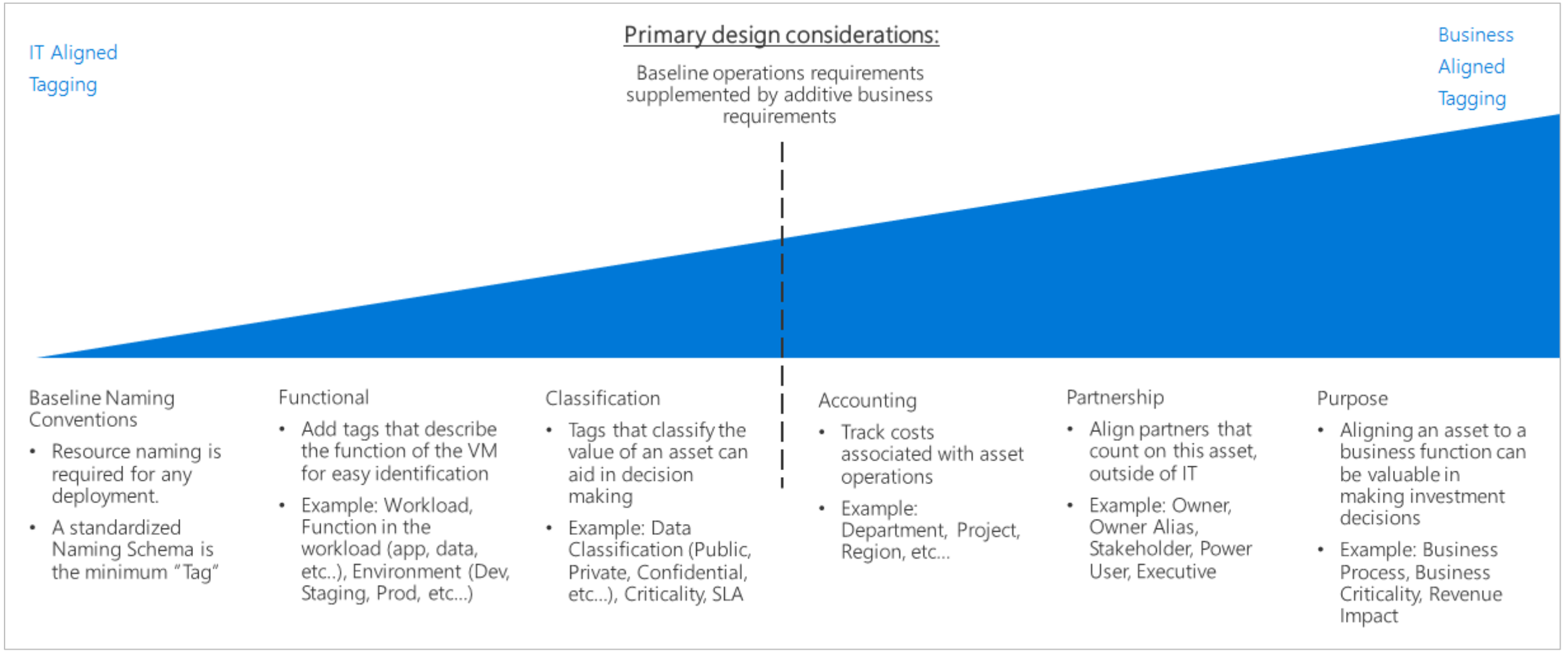

Resources in a RG should be tagged as needed

Always Tag!

- Owner
- Dept.
- Environment
- Application
- (Cost Center)

Best Practices on using Resource Tags: https://azure.microsoft.com/documentation/articles/resource-group-using-tags/
Custom RBAC Roles: https://azure.microsoft.com/documentation/articles/role-based-access-control-custom-roles/
Manage tag governance with Policy: https://docs.microsoft.com/azure/governance/policy/tutorials/govern-tags

# Tagging Decision Guide



# Tagging data classification in Azure

The data classification process categorizes data by sensitivity and business impact to identify risks. This protects important data from theft or loss.

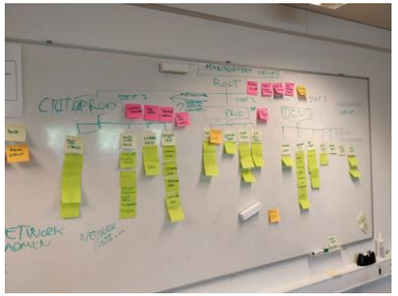
The following is a list of classifications Microsoft uses. Depending on your industry, these may already exist within your organization.

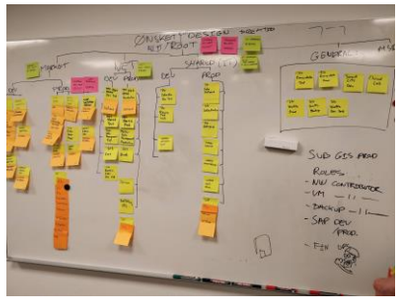
- **Non-business:** Data from your personal life that doesn't belong to Microsoft.
- **Public:** Business data that is freely available and approved for public consumption.
- **General:** Business data that isn't meant for a public audience.
- **Confidential:** Business data that can cause harm to Microsoft if overshared.
- **Highly confidential:** Business data that would cause extensive harm to Microsoft if overshared.

**Tagging data classification in Azure:**

- Resource tags are a good approach for metadata storage and can be used to apply data classification information to deployed resources. Although tagging cloud assets by classification isn't a replacement for a formal data classification process, it provides a valuable tool for managing resources and applying policy.

# Exercise 1 | Design Working Session





**Questions to drive discussion**

- What are your current rules for metadata tagging of resources and data?
- Who will be responsible for creating subscriptions and management groups?
- Will you have different governance rules for specific groups in the company?
- What are the regulatory rules you need to adhere to?
- How are you monitoring workload health and policy compliance violations?
- Classification of mission critical apps and data need to be protected

**Design**:

Management groups
Subscriptions
Resource groups
Applications
Policies
Roles and groups

**Implement: (Azure portal):**

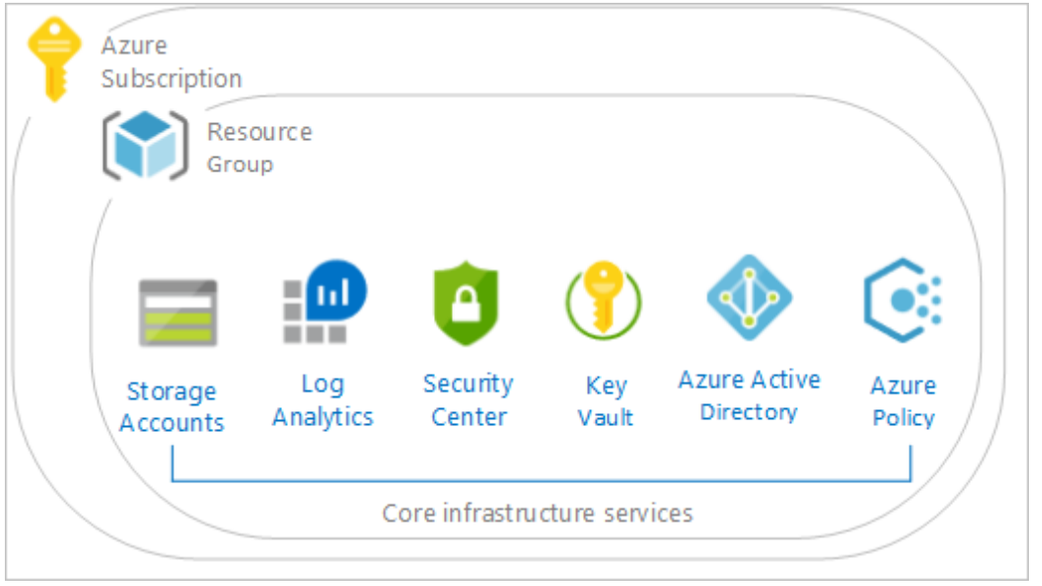
- Management groups
- Policy
- Groups and roles

# Sample policies

- All deployed assets must be categorized by criticality and data classification.
- Subnets containing mission-critical applications must be protected by a firewall solution capable of detecting intrusions and responding to attacks.
- Governance tooling must audit and enforce network configuration requirements defined by the Security Management team.
- Governance tooling must validate that all assets related to mission-critical apps or protected data are included in monitoring for resource depletion and optimization.
- Governance tooling must validate that the appropriate level of logging data is being collected for all mission-critical applications or protected data.
- Governance process must validate that backup, recovery, and SLA adherence are properly implemented for mission-critical applications and protected data.

# Deploy the policies using Azure blueprints to create Governance MVP

*Cloud Adoption Framework Foundation blueprint* deploys recommended infrastructure resources to put in place the foundation controls necessary to manage the cloud estate.




This environment is composed of:

- An Azure Key Vault
- Deploy Log Analytics
- Deploy Azure Security Center (standard version)
- The blueprint also defines and deploys Azure Policies, for
  - Tagging (CostCenter) applied to resources groups
  - Append resources in resource group with the CostCenter Tag
  - Allowed Azure Region for Resources and Resource Groups
  - Allowed Storage Account SKUs (choose while deploying)
  - Allowed Azure VM SKUs (choose while deploying)
  - Require Network Watch to be deployed
  - Require Azure Storage Account Secure transfer Encryption
  - Deny resource types (choose while deploying)
- Initiatives
  - Enable Monitoring in Azure Security Center (89 Policies)

# Where to go for more information

- Best Practices on using Resource Tags
- Organize your resources with Azure management groups
- CAF aligned Azure Blueprints

# Resource Consistency Discipline Activities

- Define Azure Management Groups & Subscriptions model & RACI
- Define resource consistency roles & responsibilities
- Define Resource Consistency Policies (Naming Conventions | Operational Tagging | Allowed Locations | Allowed Resource Types | Allowed Extensions | Auditing)

# Workshop Lab B - Govern

## Building a Cloud Governance MVP

Deploy the CAF Foundation landing zone blueprint to your subscription - https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/caf-foundation/

Based on the Customer situation and Customer needs (next slides) prioritize and implement **Resource consistency.**

# Customer Needs—Resource Consistency

- Allow the Cloud Governance team to control which Azure services can be used across the business units, while allowing controlled exceptions
  - **Control resource types and expensive configurations within common resource types**
  - Restrict Resourcegroup creation to approved groups
  - **Exceptions must be limited to a specific resource type and resource group**
- Prevent accidental deletion of resources
- Implement a common resource naming standard across the organization

# Customer Needs—Resource Consistency Control Backlog

- Rules that are too permissive may allow unintended network access and should be reviewed. Monitor unprotected endpoints, applications, and storage accounts. Endpoints and applications that aren't protected by a firewall, and storage accounts with unrestricted access can allow unintended access to information contained within the information system.
  - Audit unrestricted network access to storage accounts
  - Access through Internet facing endpoint should be restricted
  - Allowed locations
  - Allowed locations for resource groups
  - Audit use of classic storage accounts
  - Audit use of classic virtual machines
  - Audit VMs that do not use managed disks

Microsoft

# Cost Management

# Workshop | Creating the cost mgmt. baseline

Estimated time frame: approx. ~ 2hrs

**Participants**:

- Finance, cost center owners, application owners, IT teams

**Outcomes:**

- Budget setup, cost analysis, view bills and invoices, scope

**Requirements:**

- Management group, subscriptions and tagging

**Triggers:**

- Concerned about budgets
- Cost allocation across business units
- Need to implement cost guardrails
- Need to analyze cost of an application

# Let’s outline cost management

## Continuous cost optimization process

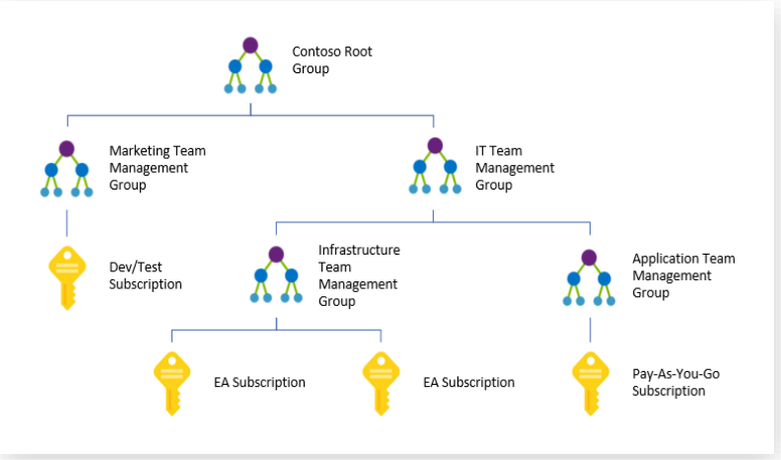
**Management teams**

**Finance teams**

**App teams**


- MG to govern tags
  Used as a cost scope for budget and Cost Analysis

Tags for visibility cross scopes



# Azure Cost Management

## Cost Management in Azure

Always on by default, no setup needed

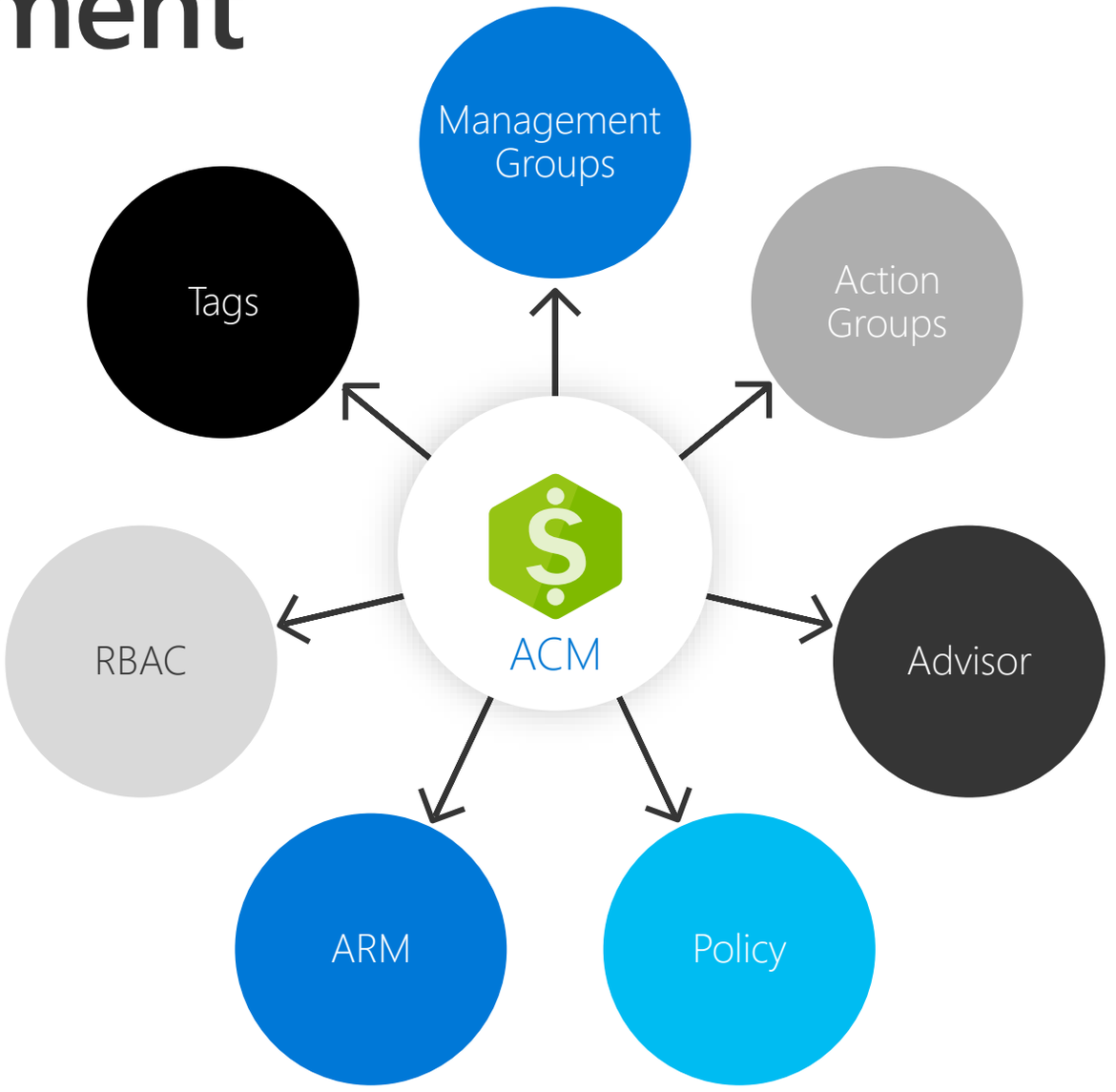
Data hygiene for tags and policies

Optimize through Azure Advisor

Notifications through action groups

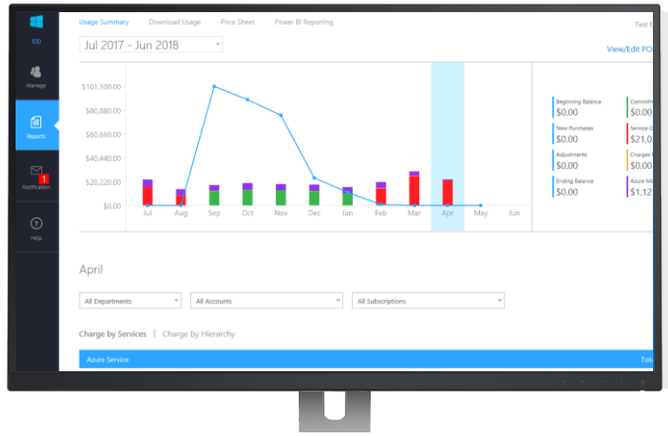
RBAC and management groups ensures better access controls

Manage AWS costs and usage in Azure

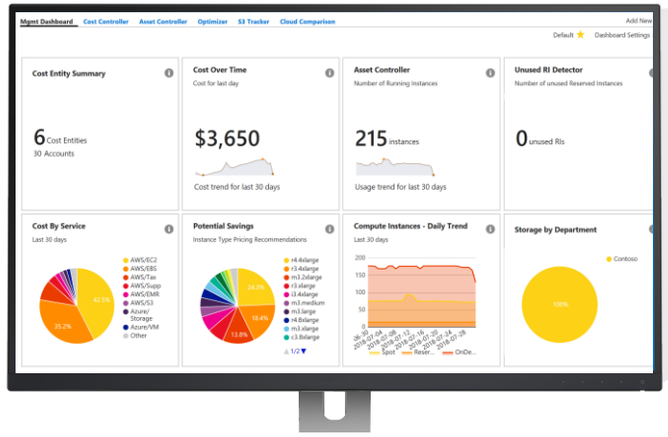


# Bring the best together in Azure Portal

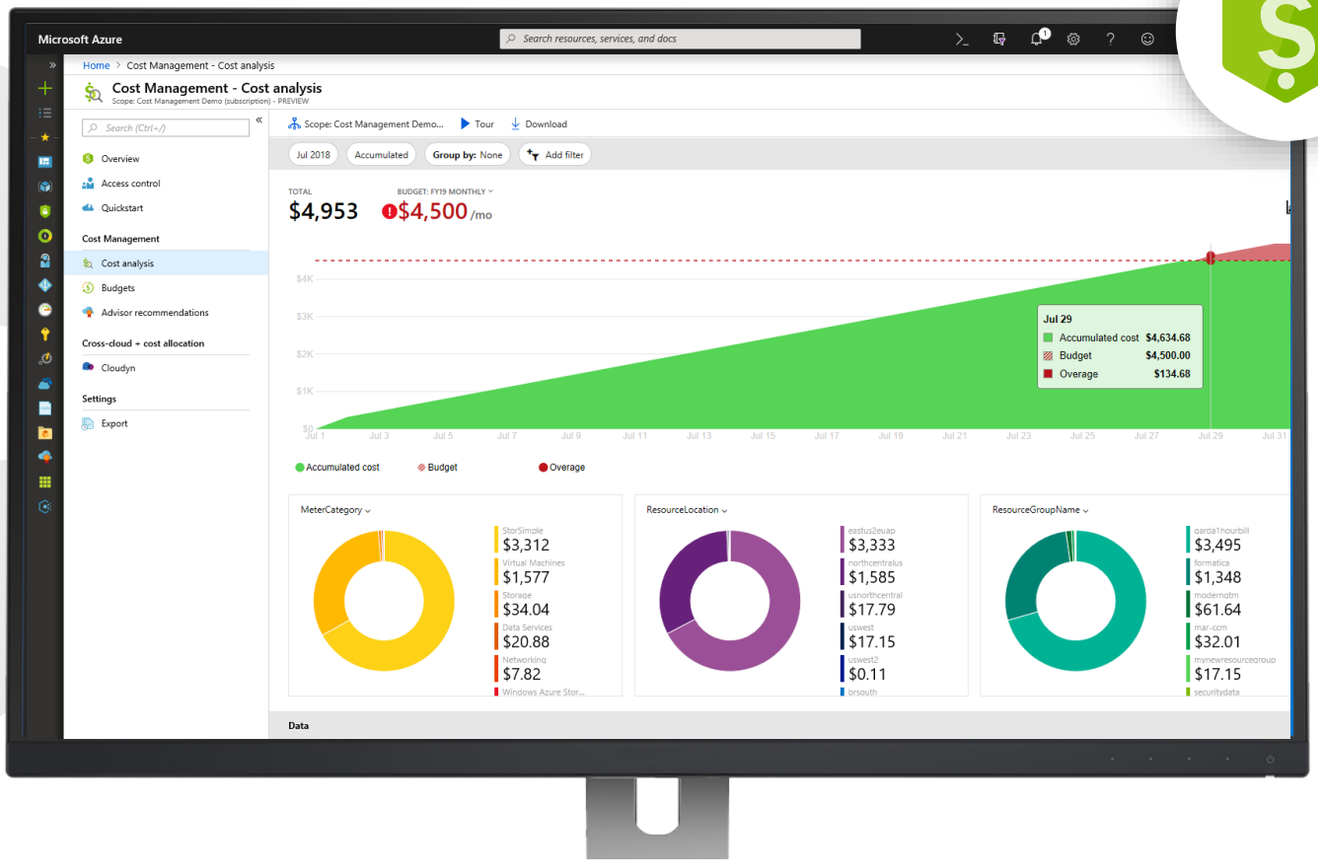
## Enterprise Portal




## Cost Management By Cloudyn




## Azure Cost Management



# Cost management solutions for a variety of needs

Cost Management in Azure Portal

Connectors to PowerBI

Azure APIs

Ready to use

Custom dashboards

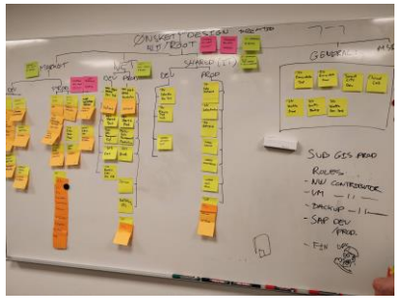
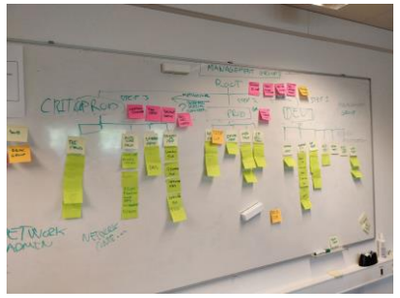
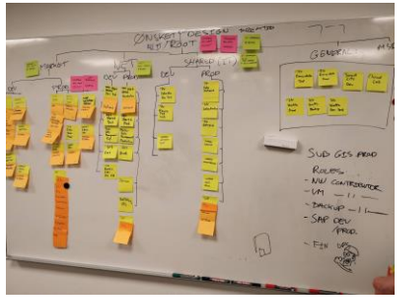
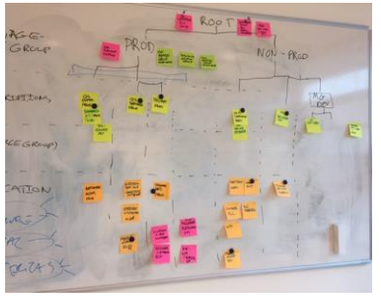
Custom solutions

# Cost Management tools in Azure

The following is a list of Azure native tools that can help mature the policies and processes that support this governance discipline.

| Tool | Azure portal | Azure Cost Management | Azure EA Content Pack | Azure Policy |
|---|---|---|---|---|
| Enterprise Agreement required? | No | No | Yes | No |
| Budget control | No | Yes | No | Yes |
| Monitor spending on single resource | Yes | Yes | Yes | No |
| Monitor spending across multiple resources | No | Yes | Yes | No |
| Control spending on single resource | Yes - manual sizing | Yes | No | Yes |
| Enforce spending across multiple resources | No | Yes | No | Yes |
| Enforce accounting metadata on resources | No | No | No | Yes |
| Monitor and detect trends | Yes | Yes | Yes | No |
| Detect spending anomalies | No | Yes | Yes | No |
| Socialize deviations | No | Yes | Yes | No |

# Exercise | Defining cost policies

- How are you landing accountability of budget?
- Are you going to allow the use of any Azure service / resource?
- What are the policies around budget over-run?
- What is the cadence in the business to set, review, adjust and optimize on budgets?
- Will there be different policies for spend based on internal use or a potential to impact customer experience?

# Sample policies

- Modify CostCenter Tag & Its value from Resource Group
- Modify CostCenter Tag to Resource Groups
- For tracking purposes, all assets must be assigned to an application owner within one of the core business functions.
- When cost concerns arise, additional governance requirements will be established with the finance team.
- Allowed Azure Region for Resources and Resource Groups
- Allowed Azure VM SKUs

# Where to go for more information

Azure Cost Management product page
https://azure.microsoft.com/services/cost-management/

Azure Cost Management documentation
https://docs.microsoft.com/azure/cost-management/

Azure Cost Management API reference
https://docs.microsoft.com/rest/api/cost-management/

FastTrack for Azure (deployment guidance)
https://azure.microsoft.com/programs/azure-fasttrack/

# Cost Management Discipline Activities

- Define Enterprise Enrollment Hierarchy Process & RACI
- Define Azure Cost Management Budgets & Alerts + RACI
- Define Cost Management RBAC Model
- Define Cost Management Policies (Tagging | Allowed VM SKUs | Allowed Storage SKUs | Allowed Networking SKUs | Allowed Database SKUs)

# Workshop Lab B - Govern

## Building a Cloud Governance MVP

Deploy the CAF Foundation landing zone blueprint to your subscription - https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/caf-foundation/

Based on the Customer situation and Customer needs (next slides) prioritize and implement **Cost Management.**

# Customer Needs—Cost Management

- Provide cost management tools for budgets, alerts, dashboards, spending reports, forecasts, anomaly detection and investigation, and cost-saving recommendations
- Implement a charge back mechanism for the business units for resources they consume based on the IO code for each application
- Enable allocation of costs between categories: Development and Test, Production, Support Services, and Infrastructure

# Customer Needs—Cost Management Controls Backlog

- You should associate all assets deployed to the cloud with a billing unit and application/workload. This policy will ensure that future Cost Management efforts will be effective.

Microsoft

# Build the Identity Baseline

# Workshop | Creating the Identity mgmt. baseline

Estimated time frame: approx. ~ 2hrs

Participants: Cloud Architects

Outcomes:

- Management groups, subscriptions, RBAC

Requirements:

- Understanding of internal org structures, compliance requirements?

Triggers:

- Getting started with Azure and need help in cloud environment setup
- Interested in learning about best practices in resource management in Azure

# Identity Management and Access Control

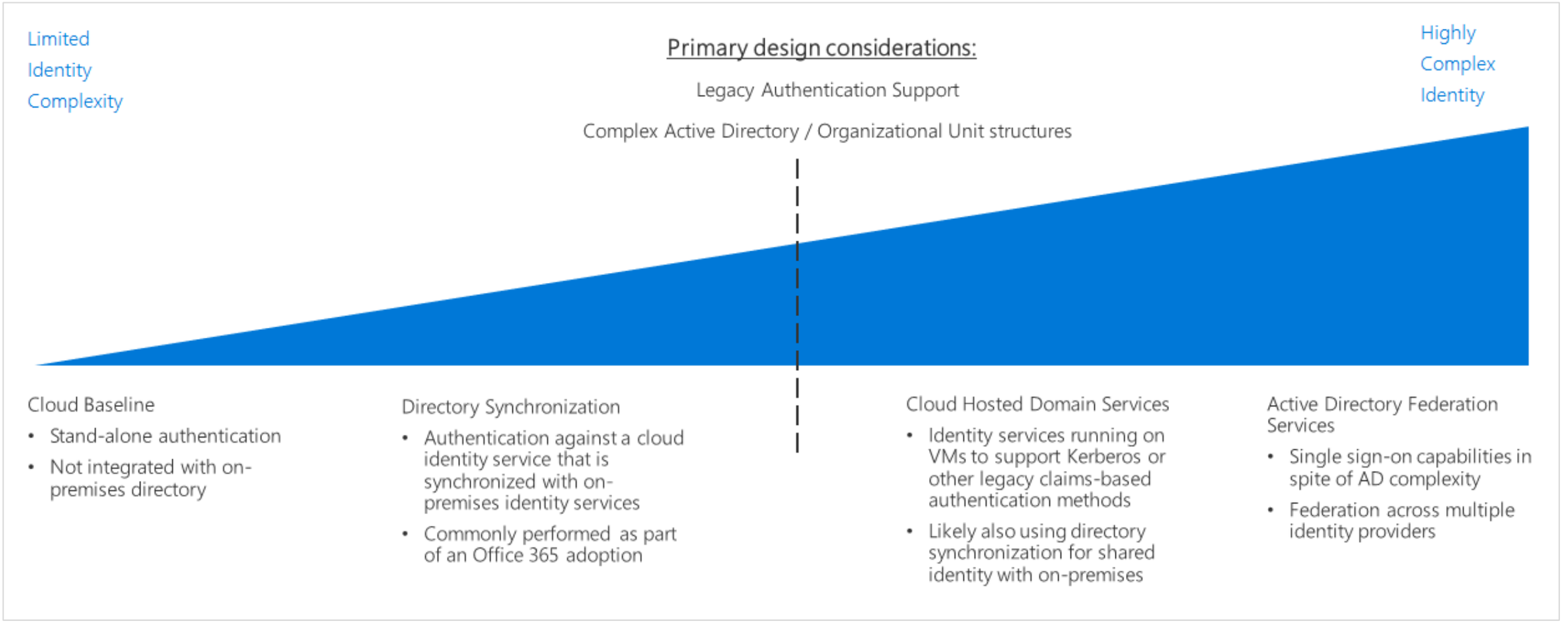
*Best Practices*

Central to protecting your data and assets in the cloud is a combination of identity management and access control. Here are some of the key practices to follow:

- ✓ Treat identity as the primary security perimeter
- ✓ Centralize Identity Management
- ✓ Manage connected tenants
- ✓ Enable single sign-on
- ✓ Turn on conditional access
- ✓ Plan for routine security improvements
- ✓ Enable password management
- ✓ Enable multifactor verification for users
- ✓ Use role-based access control
- ✓ Lower exposure of privileged accounts
- ✓ Control locations where resources are created
- ✓ Actively monitor for suspicious activities
- ✓ Use Azure AD for storage authentication

Learn more: Azure Identity Management and access control security best practices.

# Identity management decision guide




- Several options are available for managing identity in a cloud environment which vary in cost and complexity.
- A key factor in structuring your cloud-based identity services is the level of integration required with your existing on-premises identity infrastructure.
- Cloud-based identity management is an iterative process.

# Identity management patterns

| | Cloud Baseline (Azure AD) | Directory Synchronization | Cloud-hosted domain services | Active Directory Federation Services |
|---|---|---|---|---|
| *When to use* | Organization lacks an on-premises identity solution, and plans on migrating workloads to be compatible with cloud-based authentication mechanisms | For organizations with existing on-premises Active Directory infrastructure; best solution for preserving existing user and access management | Workloads that depend on claims-based authentication using legacy protocols such as Kerberos or NTLM, and they cannot be refactored to accept modern authentication protocols such as SAML or OAuth and OpenID Connect. | Identity federation establishes trust relationships across multiple identity management systems to allow common authentication and authorization capabilities. |
| *Assumptions* | • Cloud-based resources will not have dependencies on on-premises directory services or Active Directory servers<br>• Workloads being migrated either support authentication mechanisms compatible with Azure AD<br>• Existing workloads that depend on legacy authentication methods such as Kerberos might need to be refactored | • You need to maintain a common set of user accounts and groups across your cloud and on-premises IT infrastructure.<br>• Your on-premises identity services support replication with Azure AD. | • Your workloads depend on claims-based authentication using protocols like Kerberos or NTLM.<br>• Your workload virtual machines need to be domain-joined for management or application of Active Directory group policy purposes. | • You need single sign on capability across multiple identity management systems |

*Learn more*

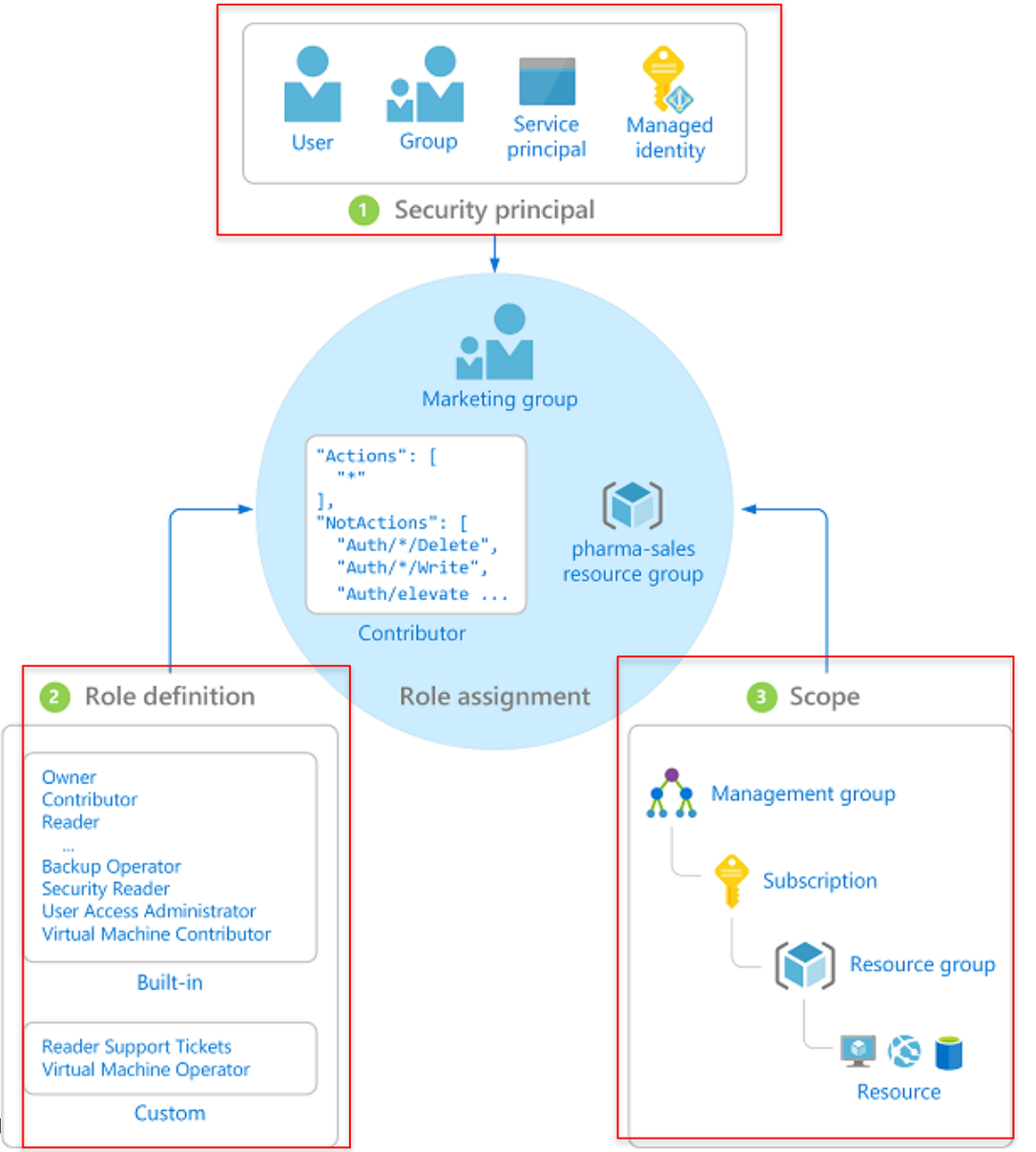
# Determine Identity Integration Requirements

| Question | Cloud baseline | Directory synchronization | Cloud-hosted domain services | Active Directory Federation Services |
|---|---|---|---|---|
| Do you currently lack an on-premises directory service? | Yes | No | No | No |
| Do your workloads need to use a common set of users and groups between the cloud and on-premises environment? | No | Yes | No | No |
| Do your workloads depend on legacy authentication mechanisms, such as Kerberos or NTLM? | No | No | Yes | Yes |
| Do you require single sign-on across multiple identity providers? | No | No | No | Yes |

- Start with a cloud-native solution with a small set of users and corresponding roles for an initial deployment.
- As your migration matures, integrate your identity solution using directory synchronization or add domains services as part of your cloud deployments.
- Revisit your identity strategy in every iteration of your migration process.

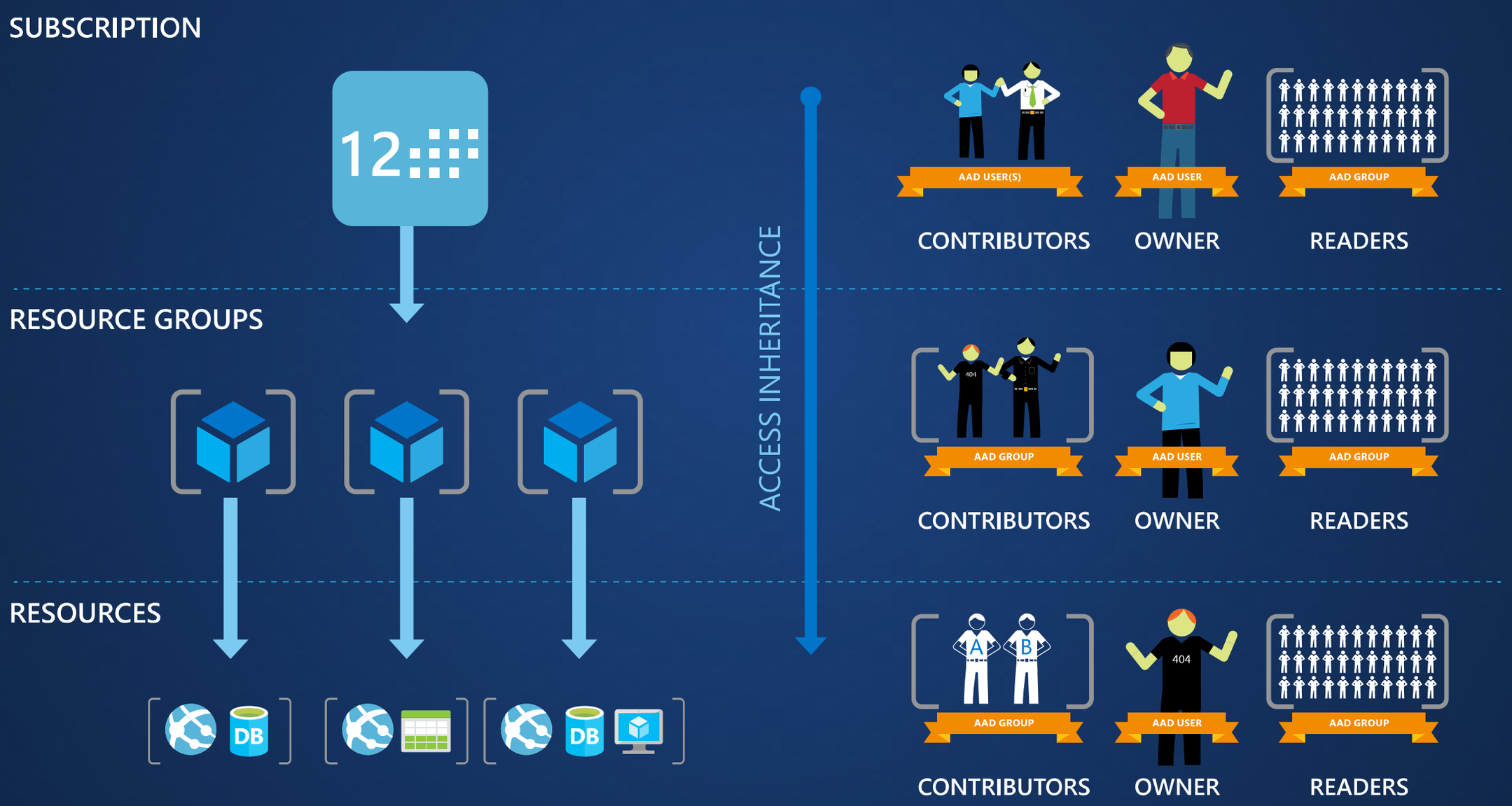
# Azure Role-Based Access Control (RBAC)

- Fine-grained access control to Azure "control plane"
- Grant access by assigning Security Principal a Role at a Scope
  - Security Principal: User, group, or service principal
  - Role: Built-in or custom role
  - Scope: Subscription, resource group, or resource
- Assignments are inherited down the resource hierarchy



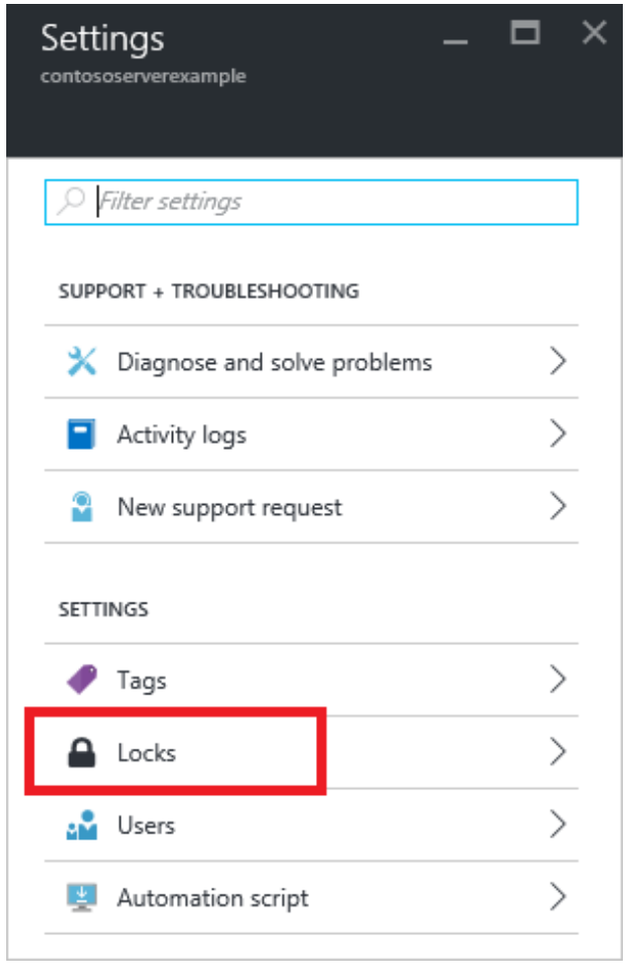

Learn more https://aka.ms/azureiam

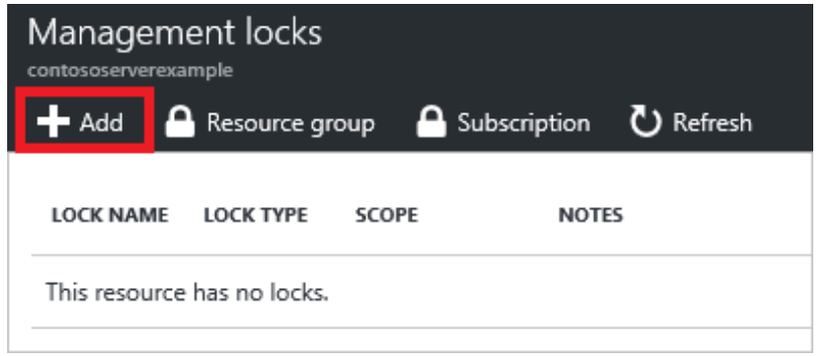
# Role Based Access Control

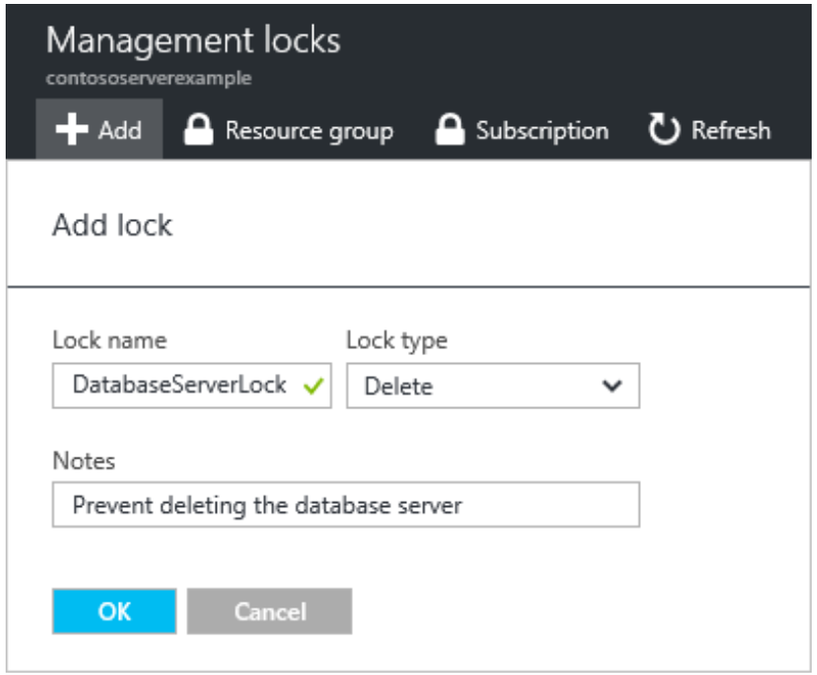


# Resource Lock

BEST PRACTICE  CHOICE



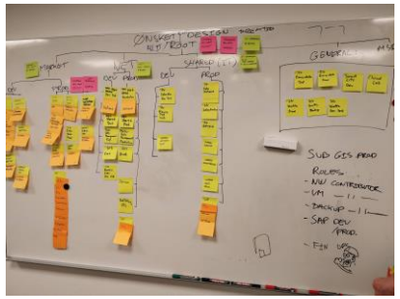
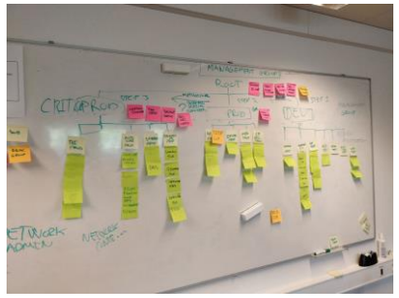




- Lock a Subscription, resource group, or resource to prevent accidental deletion or modification.
- **CanNotDelete / ReadOnly**
- Locks apply only to management operations, not to resources functions

- **Caution**: ReadOnly can cause unexpected results
  - Lock on a storage account prevents all users from listing keys
  - Lock on App Service prevents Visual Studio Server Explorer from displaying files for the resource because that interaction requires write access

# Workshop | Defining Identity baseline policies

- Do you have a consistent way of applying access control?
- What are the different roles and functions that you will consider for defining access policies?
- Have you done the mapping of on-premise roles to the cloud roles to ensure cloud resources can perform necessary functions
- Are you planning on using multi-factor authentication?
- As your teams build apps you need to ensure that you have compatible identity providers for customer authentication

# Sample policies

- All assets deployed to the cloud should be controlled using identities and roles approved by current governance policies.
- A least-privilege access model will be applied to any resources involved in mission-critical applications or protected data.
- Elevated permissions should be an exception, and any such exceptions must be recorded with the cloud governance team. Exceptions will be audited regularly.
- All groups in the on-premises Active Directory infrastructure that have elevated privileges should be mapped to an approved RBAC role.
- All accounts are required to sign in to secured resources using a multi-factor authentication method.
- Deployment of any applications that require customer authentication must use an approved identity provider that is compatible with the primary identity provider for internal users.

# Where to go for more information

- Learn more about RBAC
- Azure Identity Management Best Practices

# Identity Baseline Discipline Activities

- Define Azure RBAC Model
- Define Azure Access Management Process & RACI
- Operationalize Azure Privileged Identity Management

# Workshop Lab B - Govern

## Building a Cloud Governance MVP

Deploy the CAF Foundation landing zone blueprint to your subscription - https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/caf-foundation/

Based on the Customer situation and Customer needs (next slides) prioritize and implement **Identity Management.**

# Customer Needs—Identity Baseline

- Delegate access management to business units for each application they own
  - **Business unit administrators should not be able to change or override policies defined by the Cloud Governance team**
- Ensure staff have access to what they need, but no more, while enforcing that only built-in roles are used
- Identify a solution to streamline identity management and provide remote access for e-commerce team contingent staff

# Customer Needs—Identity Baseline Controls Backlog

- [Preview]: Audit deprecated accounts on a subscription
- [Preview]: Audit deprecated accounts with owner permissions on a subscription
- [Preview]: Audit external accounts with owner permissions on a subscription
- [Preview]: Audit external accounts with write permissions on a subscription

Microsoft

# Build the Security Baseline

# Workshop | Implementing security baseline

**Estimated time frame:** Approx 2hrs

**Participants:**

- Security team, compliance, application owners, IT teams

**Outcomes:**

- Clear set of baseline policies to protect assets and resources.

**Triggers:**

- Customer is blocked for security concerns
- The CSO would like to understand security guardrails in Azure

**Pre-requisite**

- Management group, RBAC, hub & spoke, subscriptions and tagging

# What is Security Baseline?

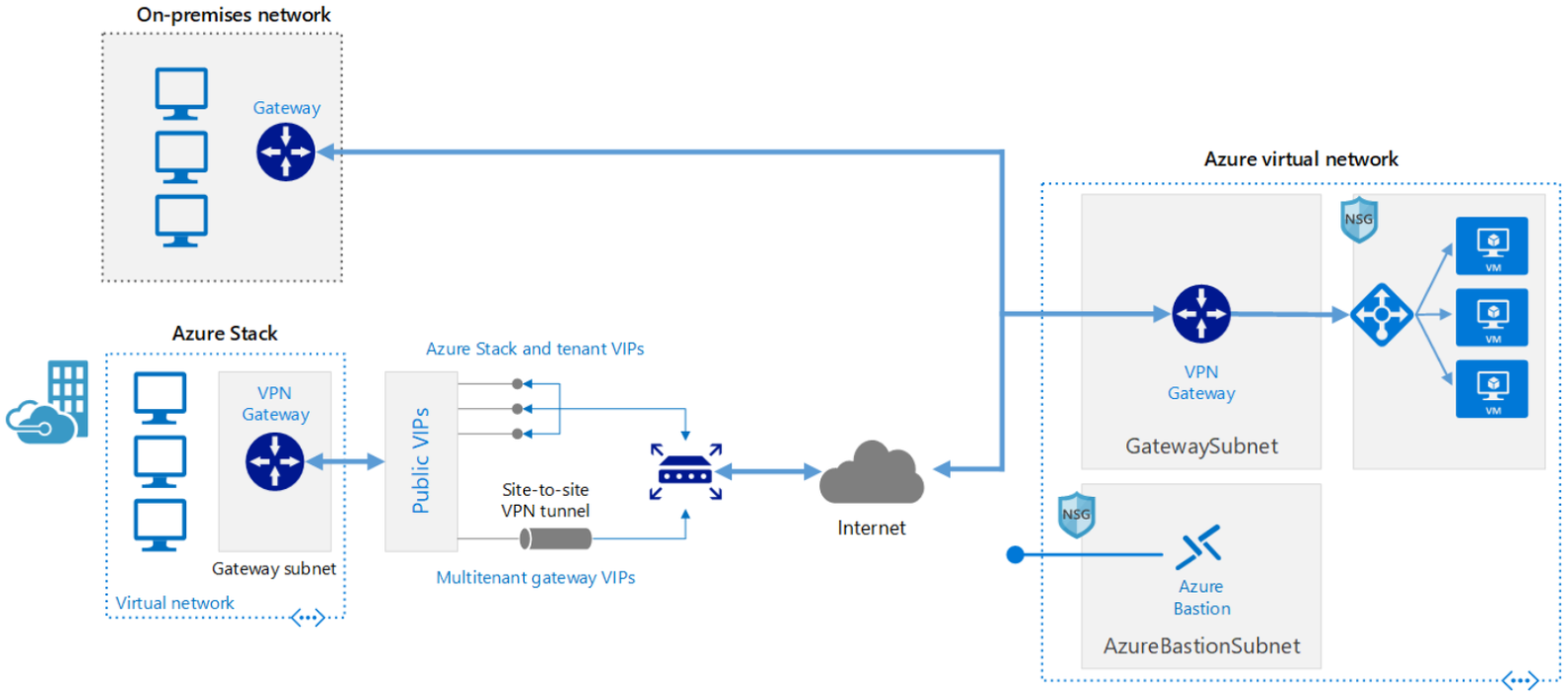
- This discipline focuses on ways of establishing policies that protect the network, assets, and data that will reside on a cloud provider's solution.
- It also includes documentation of risks, business tolerance, and mitigation strategies associated with the security of the data, assets, and network.
- From a technical perspective, this includes making decisions regarding network requirements, hybrid identity strategies, encryption and the processes used to develop cloud Security Baseline policies.

# Potential activities to create security baseline

- Determine your organization's encryption strategy for cloud-hosted data.
- Evaluate your cloud deployment's identity strategy. Determine how your cloud-based identity solution will coexist or integrate with on-premises identity providers.
- Determine network boundary policies for your Software Defined Networking (SDN) design to ensure secure virtualized networking capabilities.
- Evaluate your organization's least-privilege access policies,and use task-based roles to provide access to specific resources.
- Apply security and monitoring mechanisms to all cloud services and virtual machines.
- Automate security policies where possible.

# Network Security | Secure hybrid VNet

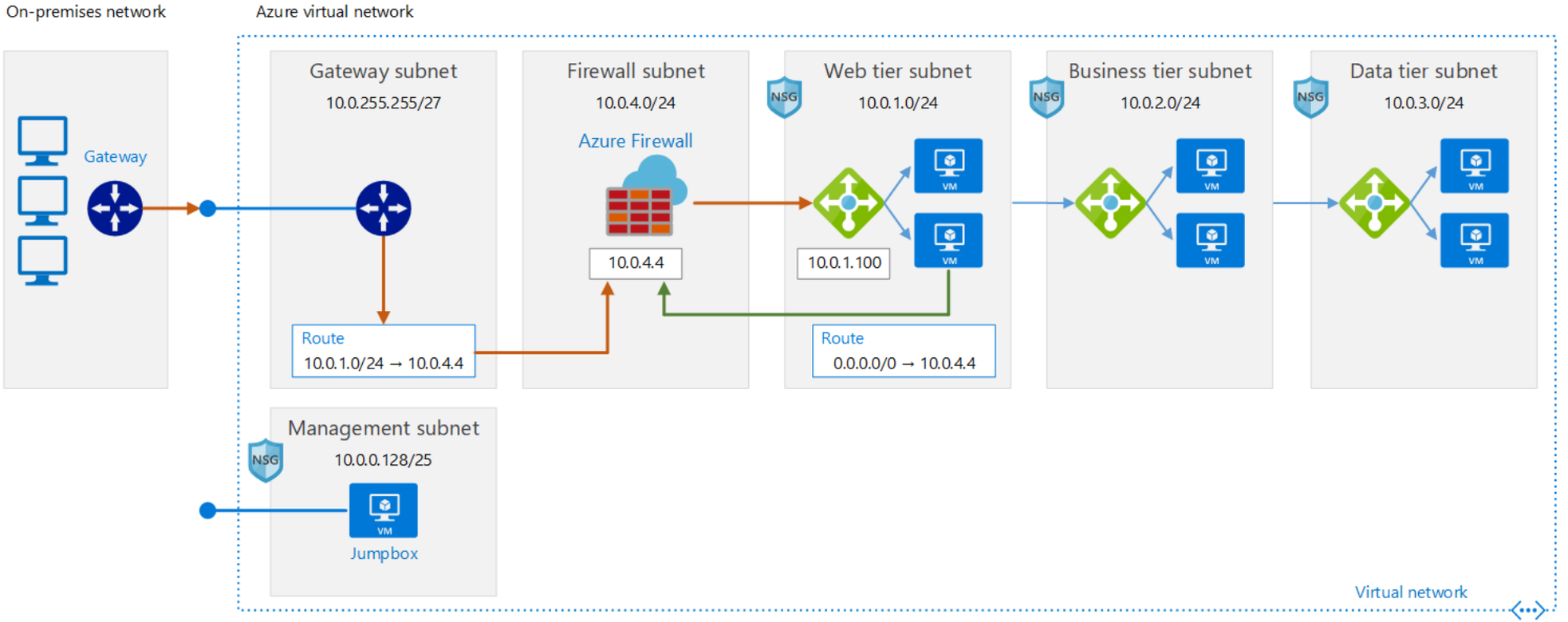
- Subscriptions often require some level of access to on-premises resources. This is common in migration scenarios.
- It is important to control and monitor any allowed communication between on-premises environment and cloud workloads,
- The On-premises network has to be secured against potential unauthorized access from cloud-based resources.




*This reference architecture shows how to extend a network from on premises or from Azure Stack into an Azure virtual network, using a site-to-site virtual private network (VPN).*

# Cloud DMZ networking pattern

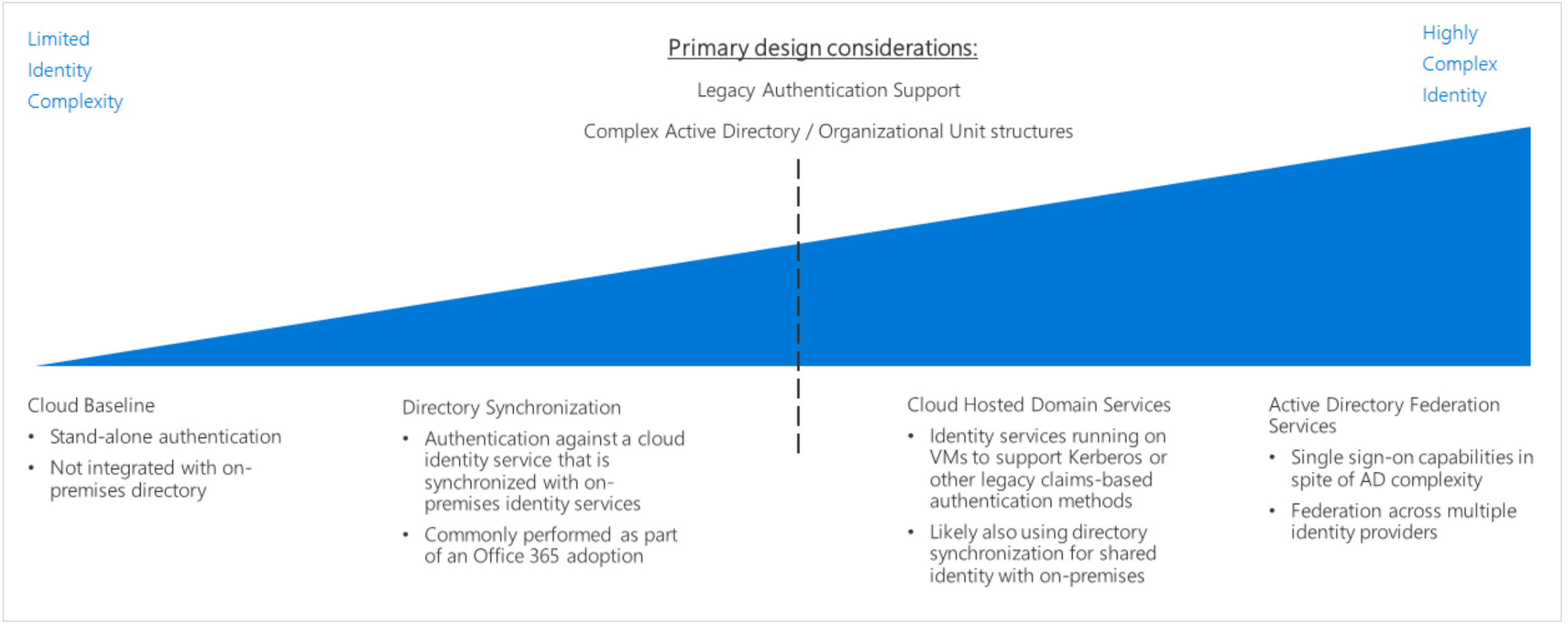
*A pattern for  a "maturing" security baseline*




This architecture is designed to support scenarios where your organization wants to start integrating cloud-based workloads with on-premises workloads but may not have fully matured cloud security policies or acquired a secure dedicated WAN connection between the two environments. As a result, cloud networks should be treated like a demilitarized zone to ensure on-premises services are secure.

*Learn more about Software Designed Networks patterns*

# Identity management | Decision guide




- Several options are available for managing identity in a cloud environment which vary in cost and complexity.
- A key factor in structuring your cloud-based identity services is the level of integration required with your existing on-premises identity infrastructure.
- Cloud-based identity management is an iterative process.

# Identity management patterns

| | Cloud Baseline (Azure AD) | Directory Synchronization | Cloud-hosted domain services | Active Directory Federation Services |
|---|---|---|---|---|
| *When to use* | Organization lacks an on-premises identity solution, and plans on migrating workloads to be compatible with cloud-based authentication mechanisms | For organizations with existing on-premises Active Directory infrastructure; best solution for preserving existing user and access management | Workloads that depend on claims-based authentication using legacy protocols such as Kerberos or NTLM, and they cannot be refactored to accept modern authentication protocols such as SAML or OAuth and OpenID Connect. | Identity federation establishes trust relationships across multiple identity management systems to allow common authentication and authorization capabilities. |
| *Assumptions*<br><br>*Learn more* | • Cloud-based resources will not have dependencies on on-premises directory services or Active Directory servers<br>• Workloads being migrated either support authentication mechanisms compatible with Azure AD<br>• Existing workloads that depend on legacy authentication methods such as Kerberos might need to be refactored | • You need to maintain a common set of user accounts and groups across your cloud and on-premises IT infrastructure.<br>• Your on-premises identity services support replication with Azure AD. | • Your workloads depend on claims-based authentication using protocols like Kerberos or NTLM.<br>• Your workload virtual machines need to be domain-joined for management or application of Active Directory group policy purposes. | • You need single sign on capability across multiple identity management systems |

# Encryption | Best practices

- ✓ Encrypting data protects it against unauthorized access.
- ✓ Corporate policy and third-party compliance are the biggest drivers when planning an encryption strategy.
- ✓ Encrypting resources is desirable, however, encryption has costs that can increase latency and overall resource usage.
- ✓ For demanding workloads, striking the correct balance between encryption and performance, and determining how data and traffic is encrypted can be essential.
- ✓ Encryption mechanisms can vary in cost and complexity, and both technical and policy requirements can influence your decisions on how encryption is applied and how you store and manage critical secrets and keys.

# Data protection

- Develop clear, simple, and well-communicated guidelines to identify, protect, and monitor the most important data assets
- Establish the strongest protection for high value assets. Perform stringent analysis of HVA lifecycle and security dependencies and establish appropriate security controls and conditions.

- Once the data you need to protect has been identified, consider how you will protect the data *at rest* and data *in transit*.
  - **Data at rest**: Data that exists statically on physical media, whether magnetic or optical disk, on premises or in the cloud.
  - **Data in transit**: Data while it is being transferred between components, locations or programs, such as over the network, across a service bus (from on-premises to cloud and vice-versa), or during an input/output process.

To further learn about protecting your data at rest or in transit, see Azure Data Security and Encryption Best Practices.

# Security baseline tools in Azure

The following list of Azure tools can help mature the policies and processes that support Security Baseline.

| Tool | Azure portal and Azure Resource Manager | Azure Key Vault | Azure AD | Azure Policy | Azure Security Center | Azure Monitor |
|---|---|---|---|---|---|---|
| Apply access controls to resources and resource creation | Yes | No | Yes | No | No | No |
| Secure virtual networks | Yes | No | No | Yes | No | No |
| Encrypt virtual drives | No | Yes | No | No | No | No |
| Encrypt PaaS storage and databases | No | Yes | No | No | No | No |
| Manage hybrid identity services | No | No | Yes | No | No | No |
| Restrict allowed types of resource | No | No | No | Yes | No | No |
| Enforce geo-regional restrictions | No | No | No | Yes | No | No |
| Monitor security health of networks and resources | No | No | No | No | Yes | Yes |
| Detect malicious activity | No | No | No | No | Yes | Yes |
| Preemptively detect vulnerabilities | No | No | No | No | Yes | No |
| Configure backup and disaster recovery | Yes | No | No | No | No | No |

For a complete list of Azure security tools and services, see Security services and technologies available on Azure.

# Establish security compliance processes

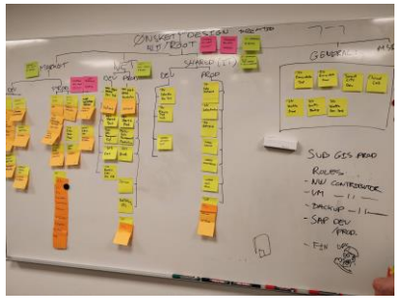
The best *Security Baseline* tools in the cloud are only as good as the processes and policies that they support.

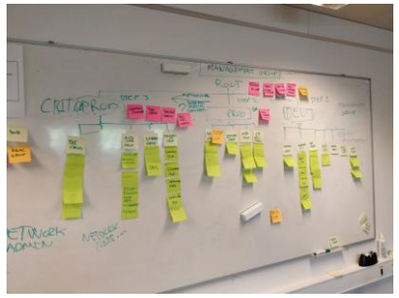
- The following is a set of example processes commonly involved in the Security Baseline discipline which you can leverage to update security policy based on inputs from stakeholders.

  - Initial risk assessment and planning
  - Deployment planning and testing
  - Quarterly review and planning
  - Education and training
  - Monthly audit and reporting views
  - Ongoing monitoring processes

Learn more about security baseline compliance processes.

# Exercise | Defining security baseline policies






- How are you addressing asset classification?
- What are the data encryption rules?
- Are you isolating your networks to present data leaks?
- What is the policy around external access to public data?
- We need to ensure that we protect from DDoS attacks
- How are you monitoring and remediating against configuration changes?
- Need to ensure that there is an ongoing security review.

# Sample policies

- All deployed assets must be categorized by criticality and data classification.
- All protected data must be encrypted when at rest.
- Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.
- All connections between the on-premises and cloud networks must take place either through a secure encrypted VPN connection or a dedicated private WAN link.
- No public facing web site backed by IaaS should be exposed to the internet without DDoS.
- Governance tooling must audit and enforce network configuration requirements defined by the Security Baseline team.
- Trends and potential exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tooling used in the cloud.

# Where to go for more information

- Learn more about Security Baseline Implementation
- Azure tools for Security Baseline
- Learn more about Microsoft Trust Center for documentation on risk assessments
- Azure SQL security playbook

# Security Baseline Discipline Activities

- Operationalize Azure Security Center
- Define Azure Security Center RBAC Model
- Define Azure Security Center Compliance Process & RACI
- Define security roles & responsibilities

# Workshop Lab B - Govern

## Building a Cloud Governance MVP

Deploy the CAF Foundation landing zone blueprint to your subscription - https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/caf-foundation/

Based on the Customer situation and Customer needs (next slides) prioritize and implement **Security Baseline.**

# Customer Needs—Security Baseline

- Enable investigation of changes leading up to any outage
  - **Who, when, what – including before/after state for each Azure resource**
  - **Azure resources and in-VM configuration**
- Ensure Windows and Linux VMs meet password complexity requirements
- Enable logging across all components (identity, virtual network, virtual machine, web, and database) to support an all-encompassing monitoring solution.

# Customer Needs—Security Baseline

- Setup auditing such that software installs are monitored across Azure virtual machine resources.
- When specific security events are detected (such as a port scan), allow for the execution of actions to remediate, start the investigative process or prevent further information leakage or damage
- The organization's security gateways (e.g. firewalls) enforce security policies and are configured to filter traffic between domains, block unauthorized access, and are used to maintain segregation between internal wired, internal wireless, and external network segments (e.g., the Internet) including DMZs and enforce access control policies for each of the domains.

# Customer Needs—Security Baseline Controls Backlog

- Awareness of VMs in violation of the password strength policy helps you take corrective actions to ensure passwords for all VM user accounts are compliant with policy.
  - [Preview]: Deploy VM extension to audit Windows VM enforces password complexity requirements
  - [Preview]: Deploy VM extension to audit Windows VM maximum password age 70 days
  - [Preview]: Deploy VM extension to audit Windows VM minimum password age 1 day
  - [Preview]: Deploy VM extension to audit Windows VM passwords must be at least 14 characters
  - [Preview]: Deploy VM extension to audit Windows VM should not allow previous 24 passwords
  - [Preview]: Audit Windows VM enforces password complexity requirements
  - [Preview]: Audit Windows VM maximum password age 70 days
  - [Preview]: Audit Windows VM minimum password age 1 day
  - [Preview]: Audit Windows VM passwords must be at least 14 characters
  - [Preview]: Audit Windows VM should not allow previous 24 passwords

Microsoft

# Build the Deployment Acceleration

# Workshop | Creating the Deployment Acceleration baseline

Estimated time frame: approx. ~ 2hrs

Participants: Cloud Architects

Outcomes:

- Management groups, Subscriptions, Tags

Requirements:

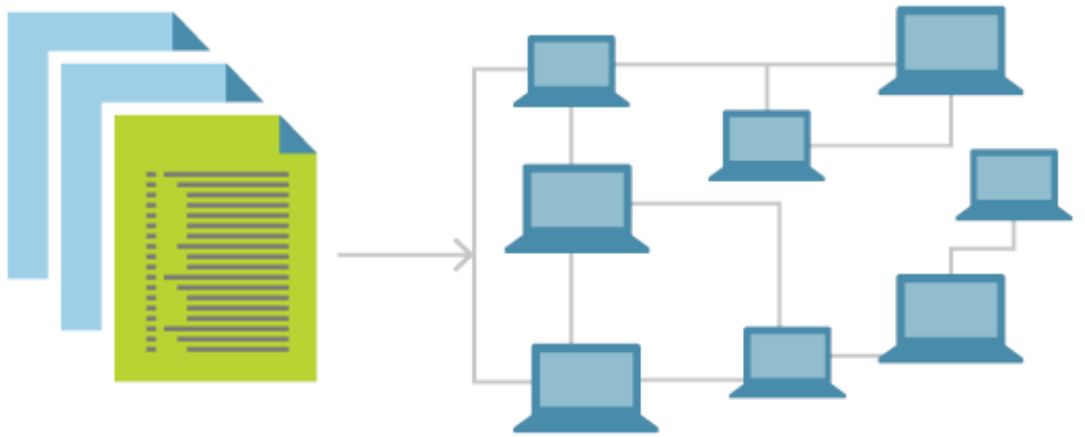
- Understanding of internal org structures, policies and compliance requirements

Triggers:

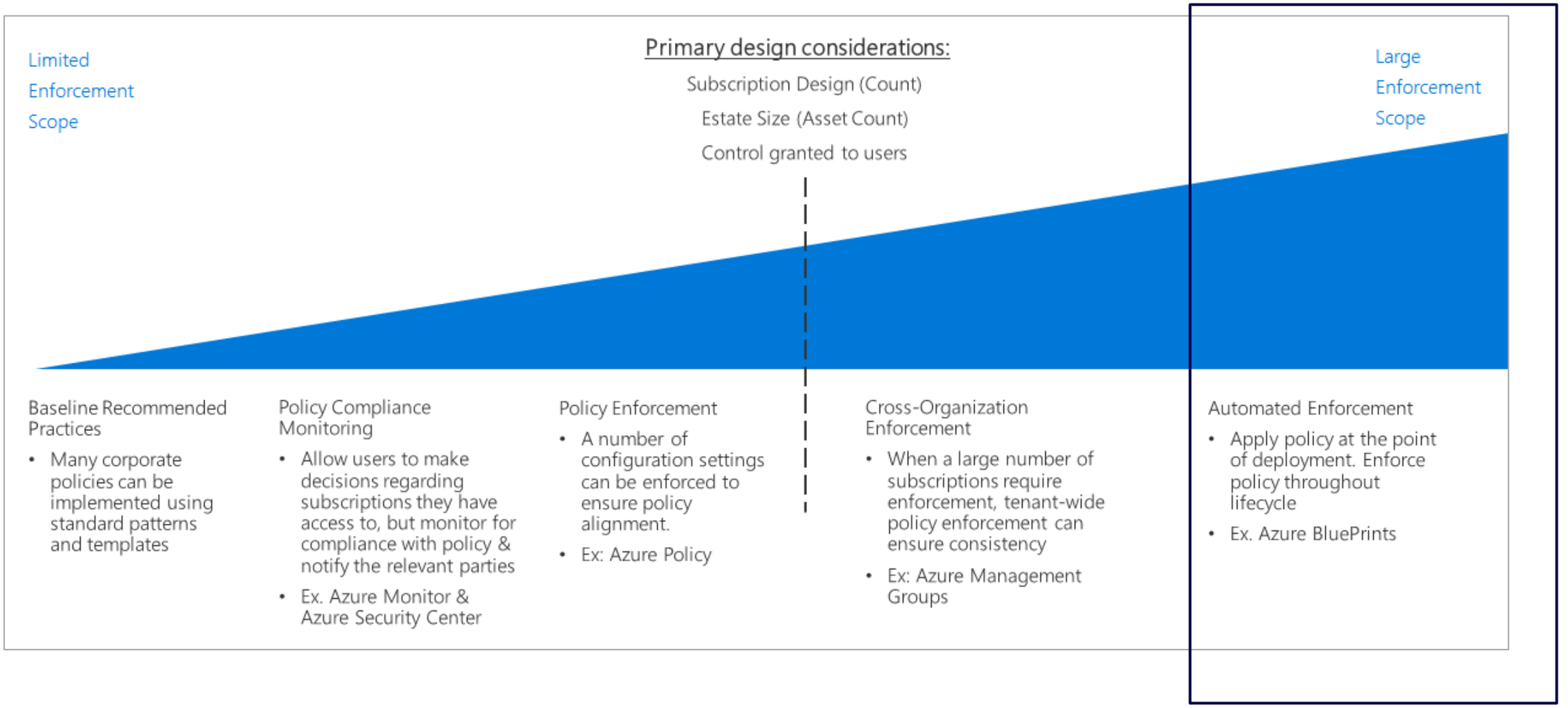
- Getting started with Azure and need help in cloud environment setup
- Need for automation and policy enforcement

# Deployment Acceleration Overview

- This discipline focuses on ways of **establishing policies** to govern asset configuration or deployment which could be manual or fully automated through DevOps.
- The DevOps practices that are leveraged in this discipline include **Infrastructure as Code, Continuous Integration and Continuous Deployment**.
- Azure services that enable deployment acceleration include **Azure Blueprints**



# Policy enforcement decision guide




Deployment Acceleration enables automated policy enforcement

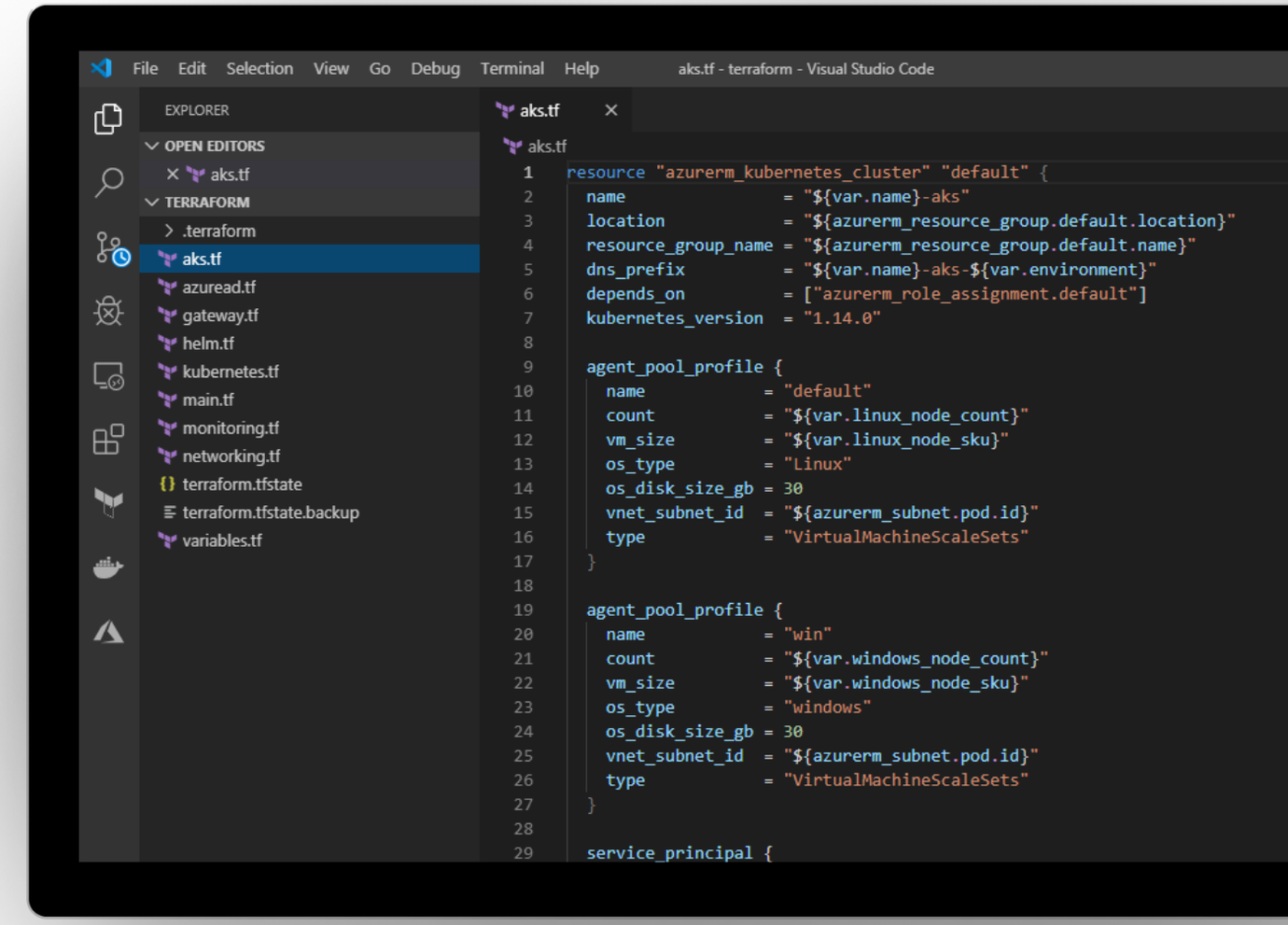
# Infrastructure as code

Stand up environments in the fastest means possible.

Remove the human element and reliably and repeatable deploy every time.

Improve environment visibility and improve developer efficiency

Store your infrastructure definitions alongside your application code.



# CI / CD Pipeline

## Automating workflows from code to cloud

### Accelerate delivery through automation

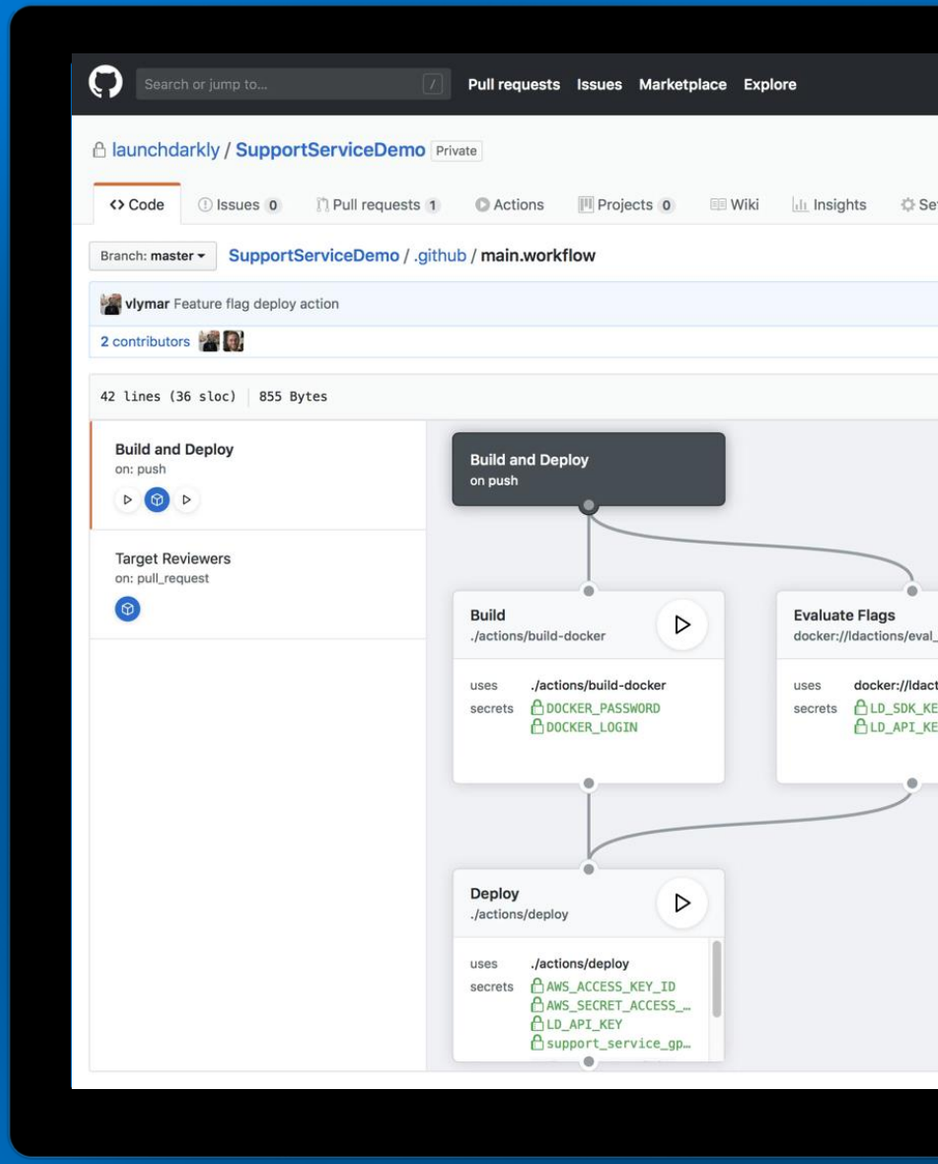
Automation triggers for 20+ project events allows for automation beyond just CI/CD to any available API

### Simple and easy to use

Configuration based on YAML with a host of sample workflows to learn from and get started

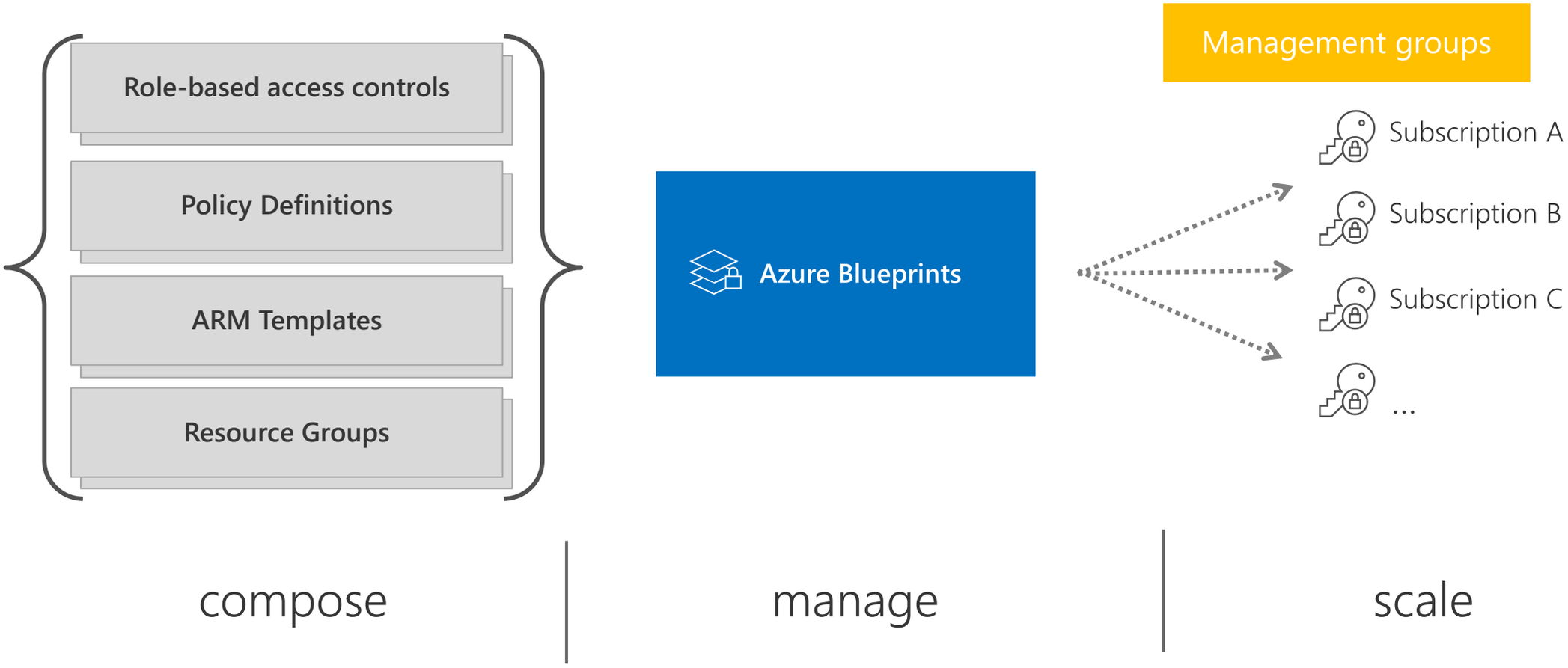
### Global community for actions

Thousands of open source Actions, maintained by the community and by companies offering integrations, including Microsoft Azure



# Azure Blueprints

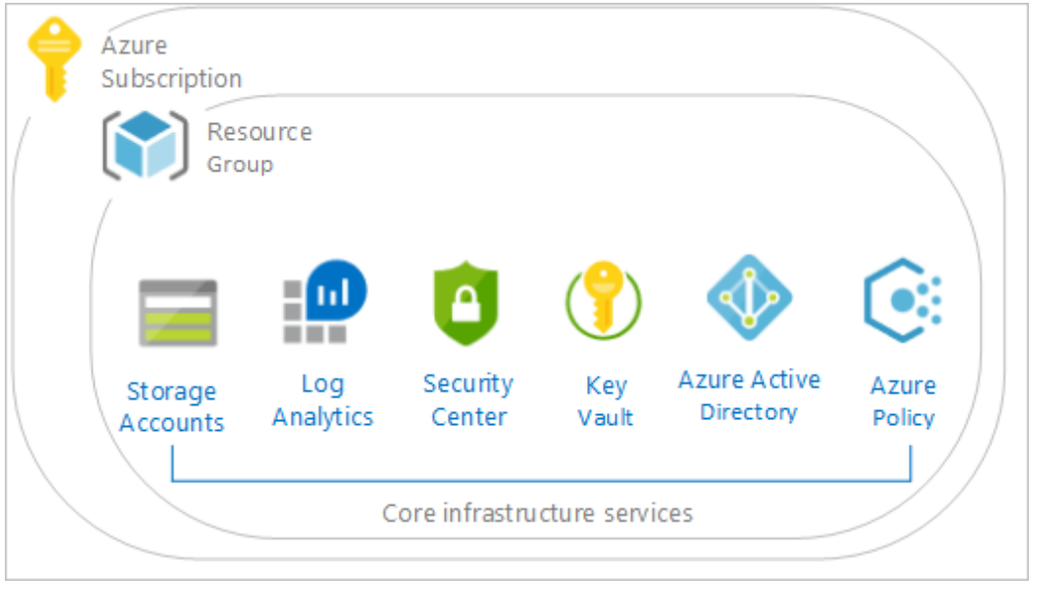
deploy and update cloud environments in a repeatable manner using composable artifacts




compose | manage | scale

# Deploy the policies using Azure blueprints to create Governance MVP

*Cloud Adoption Framework Foundation blueprint* deploys recommended infrastructure resources to put in place the foundation controls necessary to manage the cloud estate.

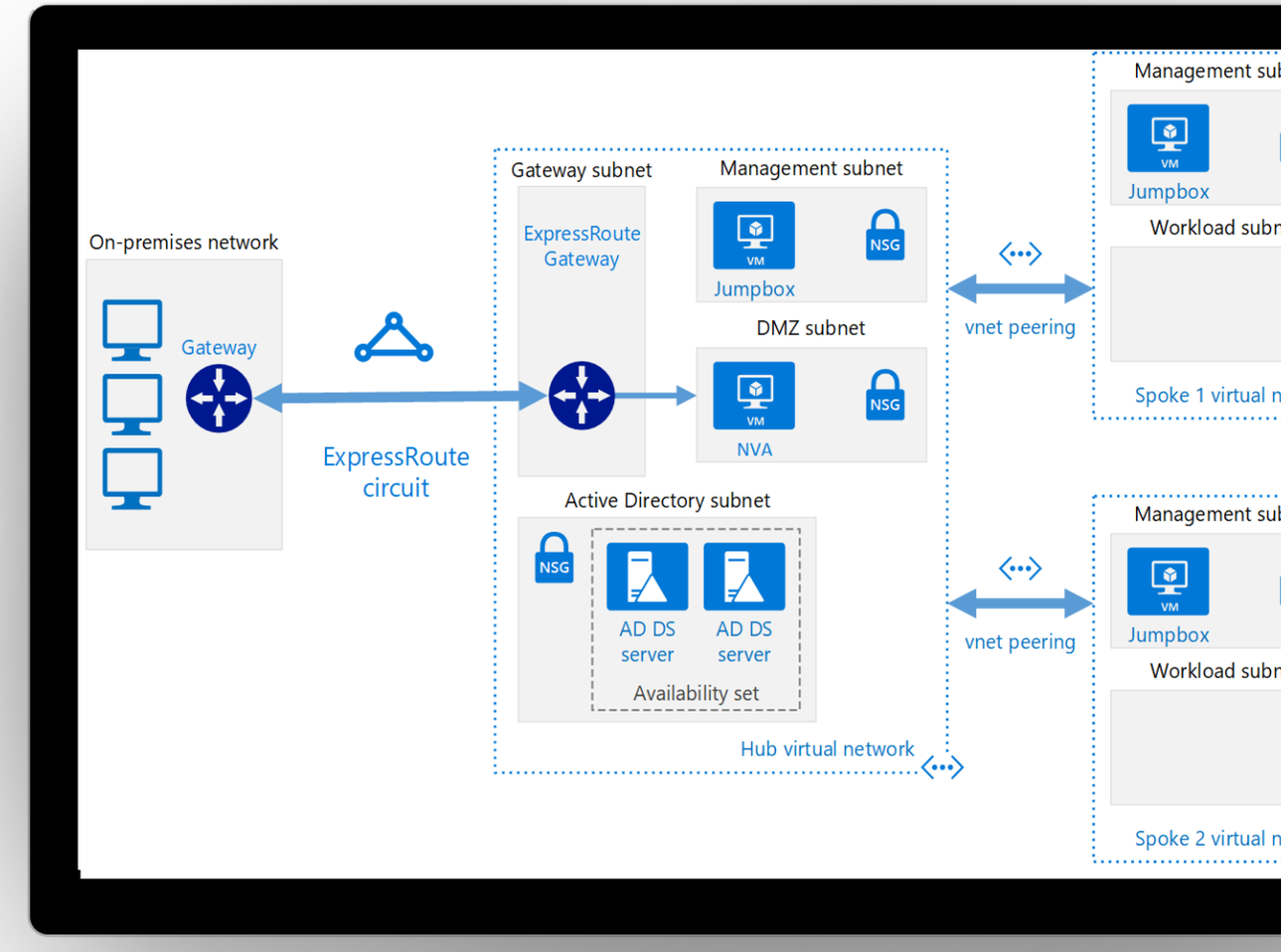



This environment is composed of:

- An Azure Key Vault
- Deploy Log Analytics
- Deploy Azure Security Center (standard version)
- The blueprint also defines and deploys Azure Policies, for
  - Tagging (CostCenter) applied to resources groups
  - Append resources in resource group with the CostCenter Tag
  - Allowed Azure Region for Resources and Resource Groups
  - Allowed Storage Account SKUs (choose while deploying)
  - Allowed Azure VM SKUs (choose while deploying)
  - Require Network Watch to be deployed
  - Require Azure Storage Account Secure transfer Encryption
  - Deny resource types (choose while deploying)
- Initiatives
  - Enable Monitoring in Azure Security Center (89 Policies)

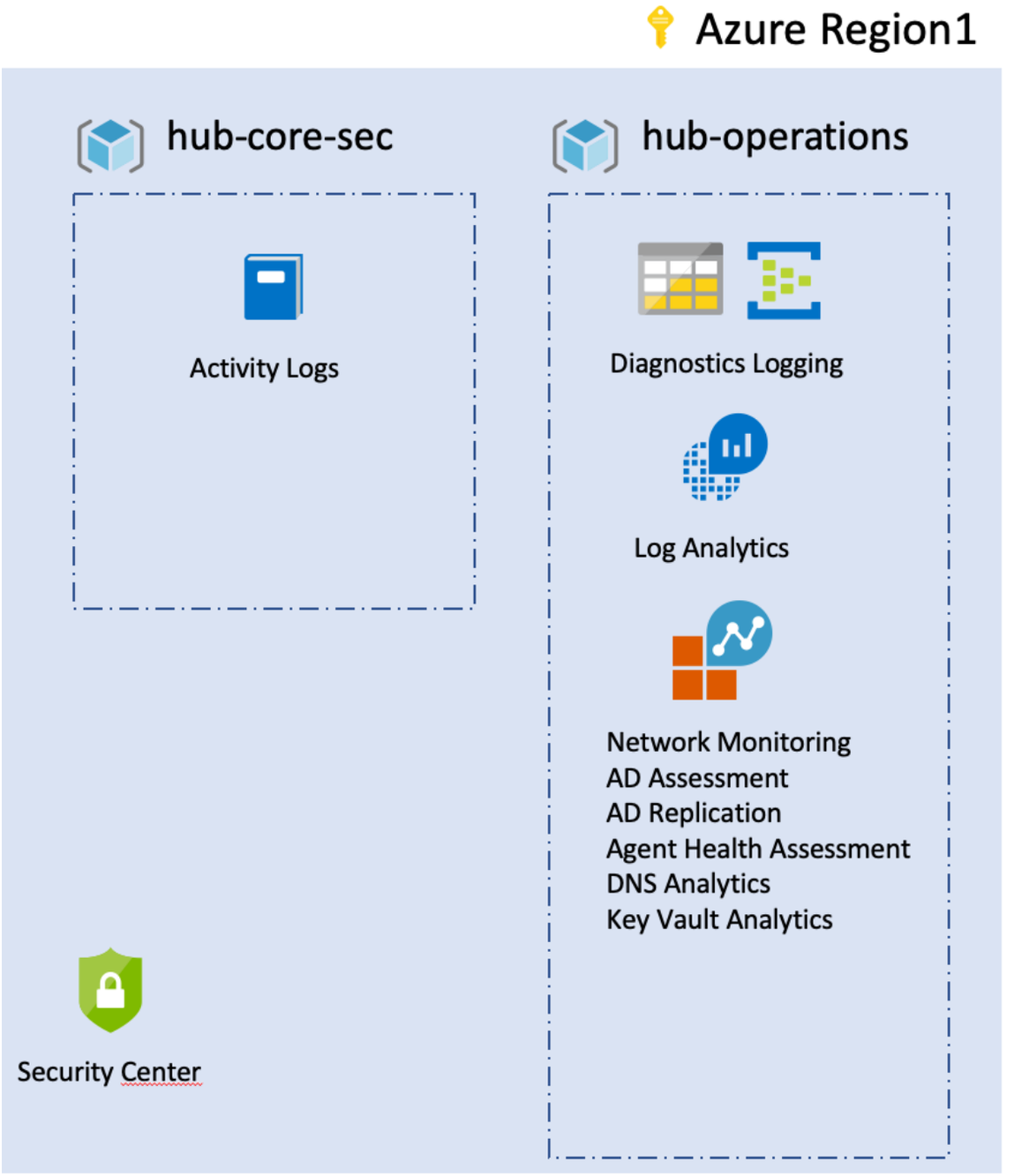
# Azure Terraform landing zones - Value proposition

- Aligned on Cloud Adoption Framework
- Enterprise grade - Inspired by FSI requirements
- Best practices in a-box
- Lower entry cost to Infrastructure as Code
- Community based
- Easy to customize | deploy | reuse
- Comes with prescriptive deployment techniques



# Terraform landing zone blueprint

- The Cloud Adoption Framework foundational landing zone for Terraform has a set of responsibilities and features to enforce logging, accounting, and security.
- This landing zone uses standard components known as Terraform modules to enforce consistency across resources deployed in the environment.
- This edition can be extended by:
  - Adding other modules to the blueprint.
  - Layering additional landing zones on top of it which is a good practice for decoupling systems, versioning each component that you're using, and allowing fast innovation and stability for your infrastructure as code deployment.



# Potential activities to create deployment acceleration baseline

- Introduce fully automated deployments early in the development process. This will improve the reliability of your testing processes and ensure consistency across your development, QA, and production environments.
- Store all deployment artifacts such as deployment templates or configuration scripts using a source-control platform such as GitHub or Azure DevOps.
- Store all secrets, passwords, certificates, and connection strings in Azure Key Vault
- Evaluate the logical and physical architecture of your applications,and identify opportunities to automate the deployment of application resources or improve portions of the architecture using other cloud-based resources.
- Define a continuous integration and continuous deployment (CI/CD) pipeline to fully manage releasing updates to your application through your development, QA, and production environments.
- Leverage infrastructure as Code technologies like ARM templates, Terraform

# Deployment Acceleration tools in Azure

The following is a list of Azure tools that can help mature the policies and processes that support this governance discipline.

| | Azure Policy | Azure Management Groups | Azure Resource Manager | Azure Blueprints | Azure Resource Graph | Azure Cost Management |
|---|---|---|---|---|---|---|
| Implement corporate policies | Yes | No | No | No | No | No |
| Apply policies across subscriptions | Required | Yes | No | No | No | No |
| Deploy defined resources | No | No | Yes | No | No | No |
| Create fully compliant environments | Required | Required | Required | Yes | No | No |
| Audit policies | Yes | No | No | No | No | No |
| Query Azure resources | No | No | No | No | Yes | No |
| Report on cost of resources | No | No | No | No | No | Yes |

# Workshop | Defining deployment acceleration policies

- Are you using templates to deploy resources or is it a manual effort?
- Do you have visibility into operational issues?
- How are you managing configuration drift within your cloud environment?

# Sample policies

- All assets deployed to the cloud should be deployed using templates or automation scripts whenever possible.
- Key metrics and diagnostics measures will be identified for all production systems and components.
- Operations will consider using monitoring and diagnostic tools in nonproduction environments such as Staging and QA to identify system issues before they occur in the production environment.
- Cloud governance processes must include monthly review with configuration management teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

# Where to go for more information

Learn more about ARM Templates

Learn more about CAF aligned Azure Blueprints for landing zones

Learn about Terraform landing zones

# Deployment Acceleration Discipline Activities

- Define use cases for ARM templates, Azure Blueprints, Deployment pipelines, etc.
- Identify Azure solutions or workloads as candidates for acceleration
- Prepare for the next phase of cloud acceleration

# Workshop Lab B - Govern

## Building a Cloud Governance MVP

Deploy the CAF Foundation landing zone blueprint to your subscription - https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/caf-foundation/

Based on the Customer situation and Customer needs (next slides) prioritize and implement **Deployment Acceleration.**

# Customer Needs—Deployment Acceleration

- Implement deployment automation while allowing controlled divergence between environments
  - **E.g. smaller footprint for Dev/Test environments**
- Provide a means to track and update existing best-practice reference implementation deployments to meet updated best practices
- Provide a means to prevent best-practice reference implementation deployments being modified outside the control of the Cloud Governance team

# Customer Needs—Deployment Acceleration Controls Backlog

- Key metrics and diagnostics measures will be identified for all production systems and components, and monitoring and diagnostic tools will be applied to these systems and monitored regularly by operations personnel.
- Operations will consider using monitoring and diagnostic tools in nonproduction environments such as Staging and QA to identify system issues before they occur in the production environment.

Microsoft

# Next Steps

# Next Steps

- Do another run of this workshop to implement all the 5 pillars of governance
- After design sessions are complete, define the SoW for actual implementation

# Appendix

# Best practices by security area for Azure SQL

| Area | Best practices |
|---|---|
| Authentication | • Use Azure Active Directory (Azure AD) for centralized identity management to:<br>  ○ Stop the proliferation of user identities across Azure SQL logical servers and databases<br>  ○ Simplify permission management<br>  ○ Flexible configuration<br>  ○ Manage applications at scale<br>• Enable MFA in Azure AD using Conditional Access and use interactive authentication.<br>• Minimize the use of password-based authentication for users. Enable Azure Managed Identity. Alternatively use integrated or certificate-based authentication.<br>• Use Azure Key Vault to store passwords and secrets. Whenever applicable, use MFA for SQL DB with Azure AD users.<br>• Support legacy scenarios, tools, and applications not enabled for Azure AD authentication; Use SQL authentication |
| Access Management | • Implement Principle of Least Privilege<br>  ○ In Azure Portal:  Use custom RBAC roles to assign just the necessary permissions<br>  ○ In SQL Data Plane:  Use granular permissions and user-defined database roles (or server-roles in MI)<br>• Implement separation of duties through permissions<br>  ○ Identify the required level of Separation of Duties. Examples: Between development/test and production environments; Security-wise sensitive tasks vs DBA management level tasks vs Developer tasks<br>  ○ Identify a comprehensive hierarchy of users (and automated processes) that access the system.<br>  ○ Create roles according to the needed usergroups and assign permissions to roles.<br>• Avoid overprovisioning of permissions, unused logins and roles<br>  ○ Perform regular checks using VA to test for too many permissions or empty roles<br>  ○ Audit changes to Permissions and role membership as well as impersonation attempts |

Learn more https://aka.ms/AzureSQLDBSecurityPlaybook

# Best practices by security area for Azure SQL (cont.)

| Area | Best practices |
|---|---|
| Data Protection | • Encrypt data in transit applications and your database<br>• Encrypt data at rest<br>• Protect sensitive data in use from high privileged, unauthorized users<br>• Control access of application users to sensitive data via encryption<br>• Protect data against unauthorized viewing by application users while preserving data format |
| Network Security | • Ensure that client machines connecting to SQL server are using Transport Layer Security.<br>• Use Azure DDoS Protection to monitor public IP addresses associated to resources deployed in virtual networks<br>• Use Advanced Threat Protection for Azure SQL Database to detect DOS attacks against databases |
| Monitoring, Logging and auditing | • Enable SQL Database Auditing to track database events and write them to an audit log in your Azure storage account, Log Analytics workspace or Event Hubs<br>• Secure audit logs; When logging access to sensitive data, consider securing the data with data encryption. |
| Security Management | • Ensure that the database(s) are configured to meet security best practices<br>• Enable SQL Vulnerability Assessment (VA) to scan your database for security issues, and to automatically run periodically on your databases.<br>• Identify and tag sensitive data<br>• Track access to sensitive data<br>• Visualize security and compliance status<br>  • Monitor SQL-related security recommendations and active threats in Azure Security Center |

Learn more https://aka.ms/AzureSQLDBSecurityPlaybook

# Azure Customer Challenges

Designing and Building Governed Azure Subscriptions

## Challenging to setup foundational infrastructure

Cumbersome to create and redeploy infra. Takes ~7 months to setup foundational infra

## Inability to create governed subscriptions

No central way to compose and enforce what goes into or made available in a subscription. Customer use a ton a scripts to try and accomplish this.

## Protecting foundational resources

Subscription owners can modify resources and remove policies breaking best practices defined by Cloud Architects

# Customer situation

## Trey Research

- Consumer products manufacturing (Manufacturing and Resources) company
- Annual revenues of USD $29.6 billion
- 10,000 - 14,999 Employees
- Global company
  - Headquarters in New Jersey
  - Major offices in the UK, France, and Japan
  - Data centers and branch offices scattered across the United States
- Looking to mitigate creeping costs as well as start the transition to a modern cloud enterprise architecture
- Large EA commitment to Azure

# Customer situation - Leadership

**Ken Greenwald, Trey Research's CTO**

- Understands the value of the cloud
- Focus on best practices and controls
- Wants to avoid mistakes that lead to trouble later on

**Laura Knight, Head of Cloud Governance team**

- Reports to Ken
- Responsible for defining, implementing and enforcing Azure governance
- Works with other teams to ensure best practices are adopted
- Wants to adopt Microsoft's Cloud Adoption Framework as a baseline for Azure governance

# Customer situation - Business strategy and focus

- **Short-term (Horizon 1)**
  - ***Reliability, Scalability, Agility, Security*** - Datacenter exit Q2
  - ***Profitability*** - Ability to provide cost of acquisition/operations for partners
  - ***Business Value Realization*** - Financial justification
- **Medium-term (Horizon 2)**
  - ***Optimize Operations*** - Data segmentation for business partners
  - ***Innovation*** - Enable developers and business units to rapidly build new services
- **Long-term (Horizon 3)**
  - ***Enable Business Agility*** - Move existing assets to micro services as a means of driving greater efficiency

# Customer situation - Business justification

- Trey Research seeks to create a financial model to showcase the long-term cash savings of the migration. In addition, provide deeper analytics for the fully burdened cost by partner enabling the ability to increase profitability. Microsoft can partner with Trey Research financial teams to build out a financial modelling to support the onboarding of new partners.

# Customer situation - Organizational alignment

Cloud Strategy Team

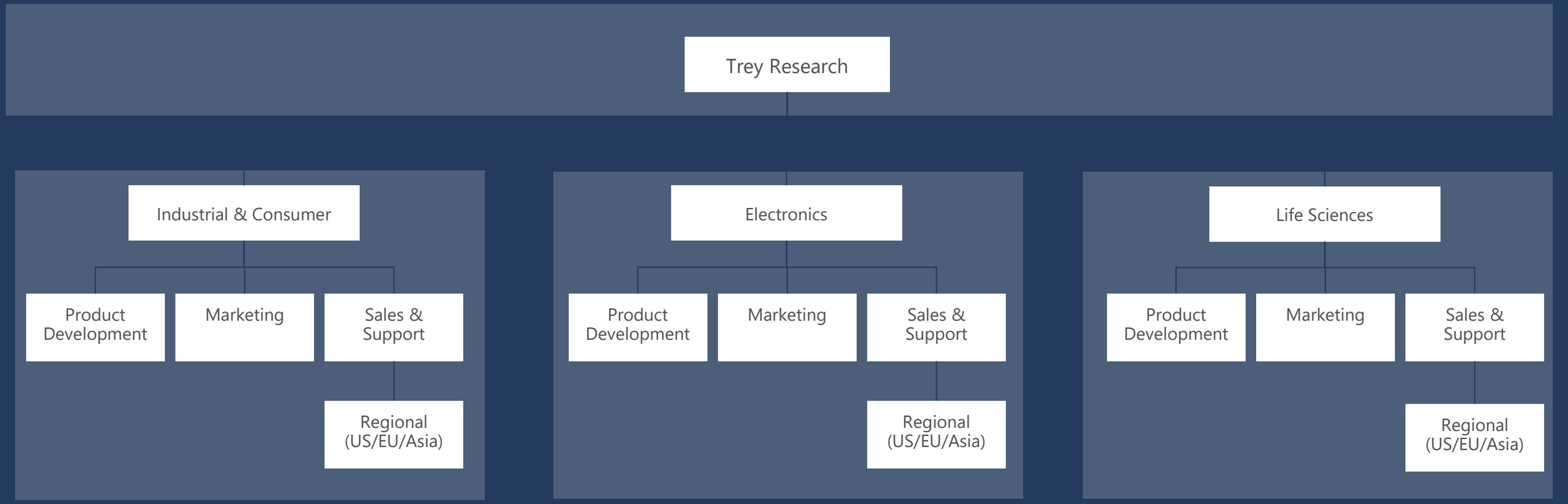
- Finance
- Line of business
- Human resources
- Operations
- Enterprise architecture
- IT infrastructure
- Application groups
- Project managers (Often with Agile project management experience)
-

Cloud Governance Team

- IT governance
- Enterprise architecture
- Security
- IT operations
- IT infrastructure
- Networking
- Identity
- Virtualization
- Business continuity and disaster recovery
- Application owners within IT
- Finance owners

# IT organization

- Each business unit has its own IT resources and IT budget
- Track and alert on costs by business unit, project, and workload type
- Delegate management to business unit IT



# Customer situation

- Sprawling IT estate, including a substantial legacy server footprint
  - Windows servers including both x32 and x64 hardware running Windows Server 2003 through to 2016
  - Linux servers running a mix of RHEL 6.10 and 7 series (7.2 through 7.6) and Ubuntu 16.04
  - The above servers comprise both physical machines as well as VMs hosted on VMware infrastructure managed by vCenter 6.5
  - Multiple database engines, including Microsoft SQL Server, PostGreSQL, and Cassandra
- 448 servers identified
- No clear view of entire estate

# Customer objections

- Per-subscription configuration won't scale to an organization the size of Trey Research. How can governance controls be implemented with minimum per-subscription configuration overhead?
- As well as implementing our governance rules on how Azure is used, we need a way to audit that no deployments have been made that bypass those rules. This audit needs to scale across the entire organization.

# Customer objections

- How can we ensure our deployments meet Azure security best practices, and how can we protect our Production workloads even if the security perimeter is compromised?
- How can Azure help control the costs associated with non-Production VMs left running out-of-hours?