Large enterprise governance journey

02/11/2019 • 7 minutes to read • Contributors

In this article

Best practice overview

This governance journey follows the experiences of a fictional company through various stages of governance maturity. It is based on real customer journeys. The suggested best practices are based on the constraints and needs of the fictional company.

As a quick starting point, this overview defines a minimum viable product (MVP) for governance based on best practices. It also provides links to some governance evolutions that add further best practices as new business or technical risks emerge.

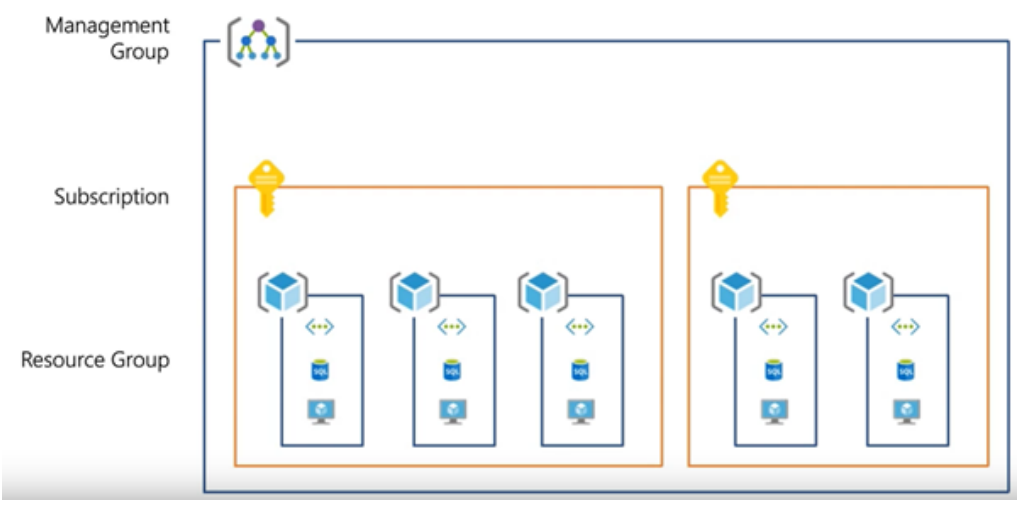
> ⚠ **Warning**
>
> This MVP is a baseline starting point, based on a set of assumptions. Even this minimal set of best practices is based on corporate policies driven by unique business risks and risk tolerances. To see if these assumptions apply to you, read the **longer narrative** that follows this article.

Governance best practice

This best practice serves as a foundation that an organization can use to quickly and consistently add governance guardrails across multiple Azure subscriptions.

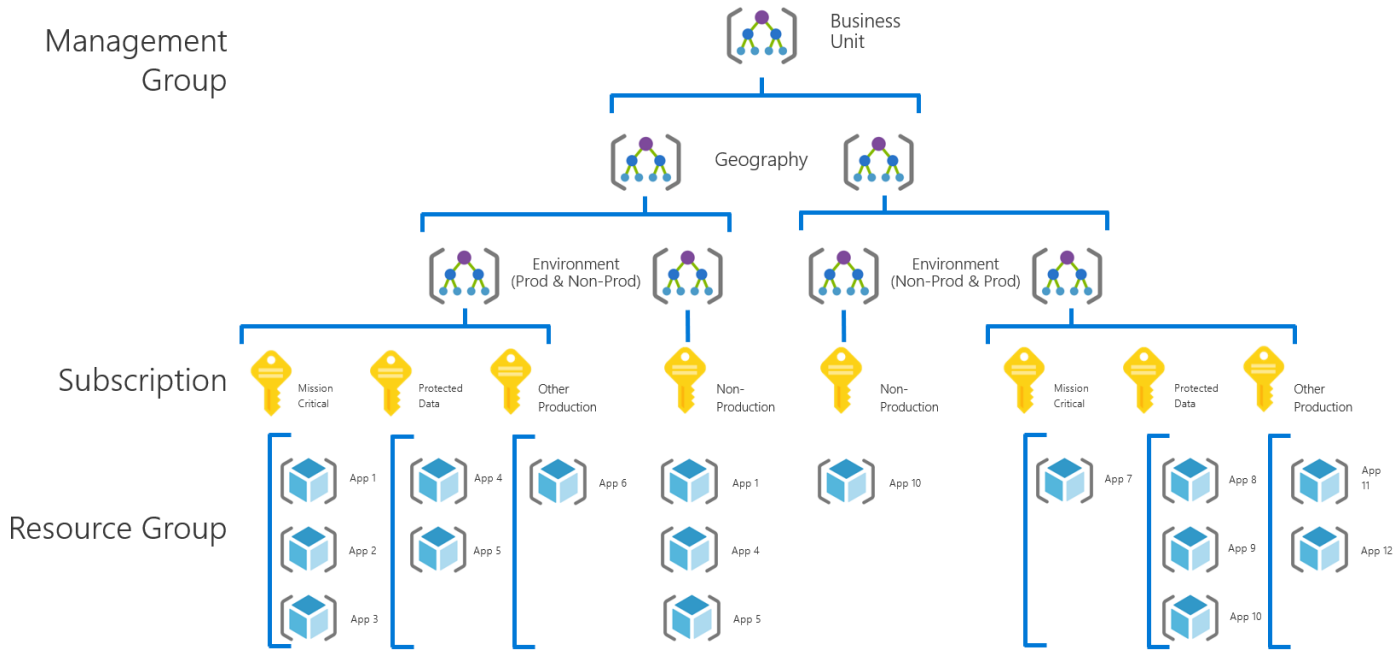
Resource organization

The following diagram shows the governance MVP hierarchy for organizing resources.



Every application should be deployed in the proper area of the management group, subscription, and resource group hierarchy. During deployment planning, the Cloud Governance team will create the necessary nodes in the hierarchy to empower the cloud adoption teams.

1. A management group for each business unit with a detailed hierarchy that reflects geography then environment type (for example, Production or Nonproduction).
2. A subscription for each unique combination of business unit, geography, environment, and "Application Categorization."
3. A separate resource group for each application.
4. Consistent nomenclature should be applied at each level of this grouping hierarchy.



These patterns provide room for growth without complicating the hierarchy unnecessarily.

> **Note**
>
> In the event of changes to your business requirements, Azure Management Groups allow you to easily reorganize your management hierarchy and subscription group assignments. However, keep in mind that policy and role assignments applied to a management group are inherited by all subscriptions underneath that group in the hierarchy. If you plan to reassign subscriptions between management groups, make sure that you are aware of any policy and role assignment changes that may result. See the Azure Management Groups documentation for more information.

Governance of resources

A set of global policies and RBAC roles will provide a baseline level of governance enforcement.

Azure provides several built-in policies and role definitions that you can assign to any management group, subscription, or resource group. However, to meet the Cloud Governance team's policy requirements, implementation of the governance MVP requires completing the following tasks:

1. Define the custom Azure Policy definitions needed to enforce business requirements.
2. Create a blueprint definition using these custom policy and the role assignments required by the governance MVP.
3. Apply policies and configuration globally by assigning the blueprint definition to all subscriptions.

Create custom policies

Custom policy definitions are saved to either a management group or a subscription and are inherited through the management group hierarchy. If a policy definition's save location is a management group, that policy definition is available to assign to any of that group's child management groups or subscriptions.

Since the policies required to support the governance MVP are meant to apply to all current subscriptions, the following business requirements will be created as policy definitions in the root management group:

1. Restrict the list of available role assignments to a set of built-in Azure roles authorized by your Cloud Governance team.
2. Require the use of the following tags on all resources: *Department/Billing Unit*, *Geography*, *Data Classification*, *Criticality*, *SLA*, *Environment*, *Application Archetype*, *Application*, and *Application Owner*.
3. Require that the *Application* tag for resources should match the name of the relevant resource group.

For information on defining custom policies see the Azure Policy documentation. For guidance and examples of custom policies, consult the Azure Policy samples site and the associated GitHub repository.

Assign Azure Policy and RBAC roles using Azure Blueprints

Although the policy requirements defined in this governance MVP apply to all current subscriptions, it's very likely that future deployments will require exceptions or alternative policies. As a result, assigning policy using management groups, with all child subscriptions inheriting these assignments, may not be flexible enough to support these scenarios.

Azure Blueprints allow the consistent assignment of policy and roles, application of Resource Manager templates, and deployment of resource groups across multiple subscriptions. As with policy definitions, blueprint definitions are saved to management groups or subscriptions, and are available through inheritance to any children in the management group hierarchy.

The Cloud Governance team has decided that enforcement of required Azure Policy and RBAC assignments across subscriptions will be implemented through Azure Blueprints and associated artifacts:

1. In the root management group, create a blueprint definition named `governance-baseline`.
2. Add the following blueprint artifacts to the blueprint definition:
   a. Policy assignments for the custom Azure Policy definitions defined at the management group root.
   b. Resource group definitions for any groups required in subscriptions created or governed by the Governance MVP.
   c. Standard role assignments required in subscriptions created or governed by the Governance MVP.
3. Publish the blueprint definition.
4. Assign the `governance-baseline` blueprint definition to all subscriptions.

See the Azure Blueprints documentation for more information on creating and using blueprint definitions.

Demilitarized Zone (DMZ)

Specific subscriptions often require some level of access to on-premises resources. This is common in migration scenarios or dev scenarios where dependent resources reside in the on-premises datacenter.

Until trust in the cloud environment is fully established it's important to tightly control and monitor any allowed communication between the on-premises environment and cloud workloads, and that the on-premises network is secured against potential unauthorized access from cloud-based resources. To support these scenarios, the governance MVP adds the following best practices:

1. Establish a cloud DMZ.
   a. The VPN reference architecture establishes a pattern and deployment model for creating a VPN Gateway in Azure.

   b. Validate that on-premises security and traffic management mechanisms are treat connected cloud networks as untrusted. Resources and services hosted in the cloud should only have access to authorized on-premises services.
   c. Validate that the local edge device in the on-premises datacenter is compatible with Azure VPN Gateway requirements and is configured to access the public internet.
2. In the root management group, create a second blueprint definition named `dmz`.
   a. Add the Resource Manager template for the VPN Gateway as an artifact of the blueprint definition.
   b. Publish the blueprint definition.
3. Assign the `dmz` blueprint definition to any subscriptions requiring on-premises connectivity. This definition should be assigned in addition to the `governance-baseline` blueprint definition.

One of the biggest concerns raised by IT security and traditional governance teams is the risk that early stage cloud adoption will compromise existing assets. The above approach allows cloud adoption teams to build and migrate hybrid solutions, with reduced risk to on-premises assets. As trust in the cloud environment increases, later evolutions may remove this temporary solution.

> **Note**
>
> The above is a starting point to quickly create a baseline governance MVP. This is only the beginning of the governance journey. Further evolution will be needed as the company continues to adopt the cloud and takes on more risk in the following areas:
>
> - Mission-critical workloads
> - Protected data
> - Cost management
> - Multicloud scenarios
>
> Moreover, the specific details of this MVP are based on the example journey of a fictional company, described in the articles that follow. We highly recommend becoming familiar with the other articles in this series before implementing this best practice.

Governance evolutions

Once this MVP has been deployed, additional layers of governance can be quickly incorporated into the environment. Here are some ways to evolve the MVP to meet specific business needs:

- Security Baseline for protected data
- Resource configurations for mission-critical applications
- Controls for Cost Management
- Controls for multicloud evolution

What does this best practice do?

In the MVP, practices and tools from the Deployment Acceleration discipline are established to quickly apply corporate policy. In particular, the MVP uses Azure Blueprints, Azure Policy, and Azure management groups to apply a few basic corporate policies, as defined in the narrative for this fictional company. Those corporate policies are applied using Azure Resource Manager templates and Azure policies to establish a small baseline for identity and security.

Evolving the best practice

Over time, this governance MVP will be used to evolve the governance practices. As adoption advances, business risk grows. Various disciplines within the Cloud Adoption Framework governance model will evolve to manage those risks. Later articles in this series discuss the evolution of corporate policy affecting the fictional company. These evolutions happen across four disciplines:

- Identity Baseline, as migration dependencies evolve in the narrative.
- Cost Management, as adoption scales.
- Security Baseline, as protected data is deployed.
- Resource Consistency, as IT Operations begins supporting mission-critical workloads.

Next steps

Now that you're familiar with the governance MVP and have an idea of the governance evolutions to follow, read the supporting narrative for additional context.

Read the supporting narrative