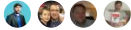


Large enterprise: Best practice explained

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

In this article

[Governance MVP \(Cloud Adoption Foundation\)](#)

[Implementation process](#)

[Dependent decisions](#)

[Policy enforcement](#)

[Applying the dependent patterns](#)

[Application of governance-defined patterns](#)

[Evolution of governance processes](#)

[Alternative patterns](#)

[Next steps](#)

The governance journey starts with a set of initial [corporate policies](#). These policies are used to establish a minimum viable product (MVP) for governance that reflects [best practices](#).

In this article, we discuss the high-level strategies that are required to create a governance MVP. The core of the governance MVP is the [Deployment Acceleration](#) discipline. The tools and patterns applied at this stage will enable the incremental evolutions needed to expand governance in the future.

Governance MVP (Cloud Adoption Foundation)

Rapid adoption of governance and corporate policy is achievable, thanks to a few simple principles and cloud-based governance tooling. These are the first of the three governance disciplines to approach in any governance process. Each discipline will be explained further on in this article.

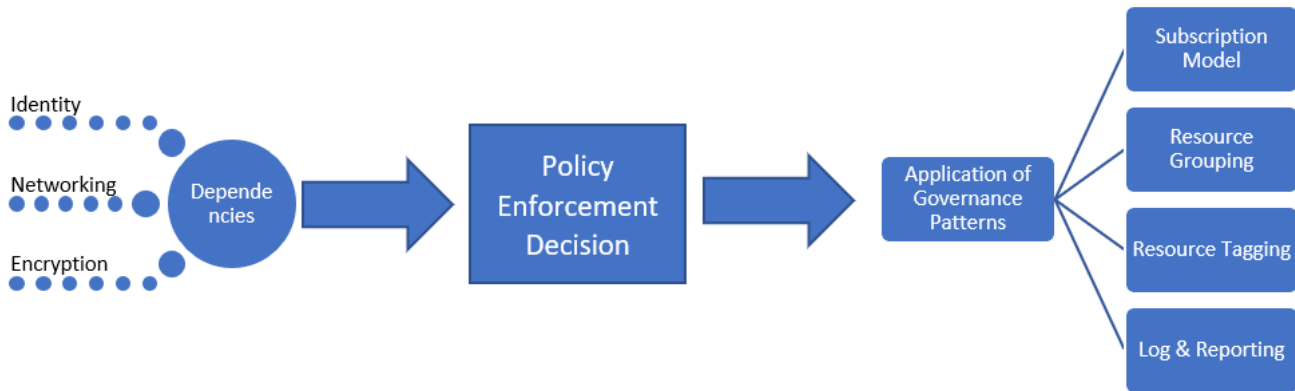
To establish the starting point, this article will discuss the high-level strategies behind Identity Baseline, Security Baseline, and Deployment Acceleration that are required to create a governance MVP, which will serve as the foundation for all adoption.



Implementation process

The implementation of the governance MVP has dependencies on Identity, Security, and Networking. Once the dependencies are resolved, the Cloud Governance team will decide a few aspects of governance. The decisions from

the Cloud Governance team and from supporting teams will be implemented through a single package of enforcement assets.



This implementation can also be described using a simple checklist:

1. Solicit decisions regarding core dependencies: Identity, Network, and Encryption.
2. Determine the pattern to be used during corporate policy enforcement.
3. Determine the appropriate governance patterns for the Resource Consistency, Resource Tagging, and Logging and Reporting disciplines.
4. Implement the governance tools aligned to the chosen policy enforcement pattern to apply the dependent decisions and governance decisions.

Dependent decisions

The following decisions come from teams outside of the Cloud Governance team. The implementation of each will come from those same teams. However, the Cloud Governance team is responsible for implementing a solution to validate that those implementations are consistently applied.

Identity Baseline

Identity Baseline is the fundamental starting point for all governance. Before attempting to apply governance, identity must be established. The established identity strategy will then be enforced by the governance solutions. In this governance journey, the Identity Management team implements the [Directory Synchronization](#) pattern:

- RBAC will be provided by Azure Active Directory (Azure AD), using the directory synchronization or "Same Sign-On" that was implemented during company's migration to Office 365. For implementation guidance, see [Reference Architecture for Azure AD Integration](#).
- The Azure AD tenant will also govern authentication and access for assets deployed to Azure.

In the governance MVP, the governance team will enforce application of the replicated tenant through subscription governance tooling, discussed later in this article. In future evolutions, the governance team could also enforce rich tooling in Azure AD to extend this capability.

Security Baseline: Networking

Software Defined Network is an important initial aspect of the Security Baseline. Establishing the governance MVP depends on early decisions from the Security Management team to define how networks can be safely configured.

Given the lack of requirements, IT security is playing it safe and has required a [Cloud DMZ](#) Pattern. That means governance of the Azure deployments themselves will be very light.

- Azure subscriptions may connect to an existing datacenter via VPN, but must follow all existing on-premises IT governance policies regarding connection of a demilitarized zone to protected resources. For implementation

guidance regarding VPN connectivity, see [VPN Reference Architecture](#).

- Decisions regarding subnet, firewall, and routing are currently being deferred to each application/workload lead.
- Additional analysis is required before releasing of any protected data or mission-critical workloads.

In this pattern, cloud networks can only connect to on-premises resources over an existing VPN that is compatible with Azure. Traffic over that connection will be treated like any traffic coming from a demilitarized zone. Additional considerations may be required on the on-premises edge device to securely handle traffic from Azure.

The Cloud Governance team has proactively invited members of the networking and IT security teams to regular meetings, in order to stay ahead of networking demands and risks.

Security Baseline: Encryption

Encryption is another fundamental decision within the Security Baseline discipline. Because the company currently does not yet store any protected data in the cloud, the Security Team has decided on a less aggressive pattern for encryption. At this point, a [cloud-native pattern for encryption](#) is suggested but not required of any development team.

- No governance requirements have been set regarding the use of encryption, because the current corporate policy does not permit mission-critical or protected data in the cloud.
- Additional analysis will be required before releasing any protected data or mission-critical workloads.

Policy enforcement

The first decision to make regarding Deployment Acceleration is the pattern for enforcement. In this narrative, the governance team decided to implement the [Automated Enforcement](#) pattern.

- Azure Security Center will be made available to the security and identity teams to monitor security risks. Both teams are also likely to use Security Center to identify new risks and evolve corporate policy.
- RBAC is required in all subscriptions to govern authentication enforcement.
- Azure Policy will be published to each management group and applied to all subscriptions. However, the level of policies being enforced will be very limited in this initial Governance MVP.
- Although Azure management groups are being used, a relatively simple hierarchy is expected.
- Azure Blueprints will be used to deploy and update subscriptions by applying RBAC requirements, Resource Manager Templates, and Azure Policy across management groups.

Applying the dependent patterns

The following decisions represent the patterns to be enforced through the policy enforcement strategy above:

Identity Baseline. Azure Blueprints will set RBAC requirements at a subscription level to ensure that consistent identity is configured for all subscriptions.

Security Baseline: Networking. The Cloud Governance team maintains a Resource Manager template for establishing a VPN gateway between Azure and the on-premises VPN device. When an application team requires a VPN connection, the Cloud Governance team will apply the gateway Resource Manager template via Azure Blueprints.

Security Baseline: Encryption. At this point in the journey, no policy enforcement is required in this area. This will be revisited during later evolutions.

Application of governance-defined patterns

The Cloud Governance team will be responsible for the following decisions and implementations. Many will require inputs from other teams, but the Cloud Governance team is likely to own both the decision and implementation. The

following sections outline the decisions made for this use case and details of each decision.

Subscription design

The decision on what subscription design to use determines how Azure subscriptions get structured and how Azure management groups will be used to efficiently manage access, policies, and compliance of these subscription. In this narrative, the governance team has chosen the [Mixed](#) subscription design pattern.

- As new requests for Azure resources arise, a "Department" should be established for each major business unit in each operating geography. Within each of the Departments, "Subscriptions" should be created for each application archetype.
- An application archetype is a means of grouping applications with similar needs. Common examples include: Applications with protected data, governed applications (such as HIPAA or FedRAMP), low-risk applications, applications with on-premises dependencies, SAP or other mainframe applications in Azure, or applications that extend on-premises SAP or mainframe applications. Each organization has unique needs based on data classifications and the types of applications that support the business. Dependency mapping of the digital estate can help define the application archetypes in an organization.
- A common naming convention should be agreed on as part of the subscription design, based on the above two bullets.

Resource consistency

Resource consistency decisions determine the tools, processes, and effort required to ensure Azure resources are deployed, configured, and managed consistently within a subscription. In this narrative, [Hierarchical Consistency](#) has been chosen as the primary resource consistency pattern.

- Resource groups should be created for each application. Management groups should be created for each application archetype. Azure Policy should be applied to all subscriptions in the associated management group.
- As part of the deployment process, Resource Consistency templates for all assets should be stored in source control.
- Each resource group should align to a specific workload or application.
- The Azure management group hierarchy defined should represent billing responsibility and application ownership using nested groups.
- Extensive implementation of Azure Policy could exceed the team's time commitments and may not provide much value at this point. However, a simple default policy should be created and applied to each resource group to enforce the first few cloud governance policy statements. This serves to define the implementation of specific governance requirements. Those implementations can then be applied across all deployed assets.

Resource tagging

Resource tagging decisions determine how metadata is applied to Azure resources within a subscription to support operations, management, and accounting purposes. In this narrative, the [Accounting](#) pattern has been chosen as the default model for resource tagging.

- Deployed assets should be tagged with values for the following: Department/Billing Unit, Geography, Data Classification, Criticality, SLA, Environment, Application Archetype, Application, and Application Owner.
- These values along with the Azure management group and subscription associated with a deployed asset will drive governance, operations, and security decisions.

Logging and reporting

Logging and reporting decisions determine how your store log data and how the monitoring and reporting tools that keep IT staff informed on operational health are structured. In this narrative a [Hybrid monitoring](#) pattern for logging and reporting is suggested, but not required of any development team at this point.

- No governance requirements are currently set regarding the specific data points to be collected for logging or reporting purposes. This is specific to this fictional narrative and should be considered an antipattern. Logging standards should be determined and enforced as soon as possible.
- Additional analysis is required before the release of any protected data or mission-critical workloads.
- Before supporting protected data or mission-critical workloads, the existing on-premises operational monitoring solution must be granted access to the workspace used for logging. Applications are required to meet security and logging requirements associated with the use of that tenant, if the application is to be supported with a defined SLA.

Evolution of governance processes

Some of the policy statements cannot or should not be controlled by automated tooling. Other policies will require periodic effort from IT Security and on-premises Identity Baseline teams. The Cloud Governance team will need to oversee the following processes to implement the last eight policy statements:

Corporate policy changes: The Cloud Governance team will make changes to the governance MVP design to adopt the new policies. The value of the governance MVP is that it will allow for the automatic enforcement of the new policies.

Adoption acceleration: The Cloud Governance team has been reviewing deployment scripts across multiple teams. They've maintained a set of scripts that serve as deployment templates. Those templates can be used by the cloud adoption teams and DevOps teams to more quickly define deployments. Each script contains the requirements for enforcing governance policies, and additional effort from cloud adoption engineers is not needed. As the curators of these scripts, they can implement policy changes more quickly. Additionally, they are viewed as accelerators of adoption. This ensures consistent deployments without strictly enforcing adherence.

Engineer training: The Cloud Governance team offers bimonthly training sessions and has created two videos for engineers. Both resources help engineers get up to speed quickly on the governance culture and how deployments are performed. The team is adding training assets to demonstrate the difference between production and nonproduction deployments, which helps engineers understand how the new policies affect adoption. This ensures consistent deployments without strictly enforcing adherence.

Deployment planning: Before deploying any asset containing protected data, the Cloud Governance team will be responsible for reviewing deployment scripts to validate governance alignment. Existing teams with previously approved deployments will be audited using programmatic tooling.

Monthly audit and reporting: Each month, the Cloud Governance team runs an audit of all cloud deployments to validate continued alignment to policy. When deviations are discovered, they are documented and shared with the cloud adoption teams. When enforcement doesn't risk a business interruption or data leak, the policies are automatically enforced. At the end of the audit, the Cloud Governance team compiles a report for the Cloud Strategy team and each cloud adoption team to communicate overall adherence to policy. The report is also stored for auditing and legal purposes.

Quarterly policy review: Each quarter, the Cloud Governance team and Cloud Strategy team to review audit results and suggest changes to corporate policy. Many of those suggestions are the result of continuous improvements and the observation of usage patterns. Approved policy changes are integrated into governance tooling during subsequent audit cycles.

Alternative patterns

If any of the patterns chosen in this governance journey don't align with the reader's requirements, alternatives to each pattern are available:

- [Encryption patterns](#)
- [Identity patterns](#)

- [Logging and Reporting patterns](#)
- [Policy Enforcement patterns](#)
- [Resource Consistency patterns](#)
- [Resource Tagging patterns](#)
- [Software Defined Networking patterns](#)
- [Subscription Design patterns](#)

Next steps

Once this guidance is implemented, each cloud adoption team can proceed with a solid governance foundation. The Cloud Governance team will work in parallel to continually update the corporate policies and governance disciplines.

Both teams will use the tolerance indicators to identify the next evolution needed to continue supporting cloud adoption. The next step for the company in this journey is to evolve their governance baseline to support applications with legacy or third-party multi-factor authentication requirements.

Identity Baseline evolution