Small-to-medium enterprise: Best practice explained

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

In this article

The governance journey starts with a set of initial corporate policies. These policies are used to establish a governance MVP 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)

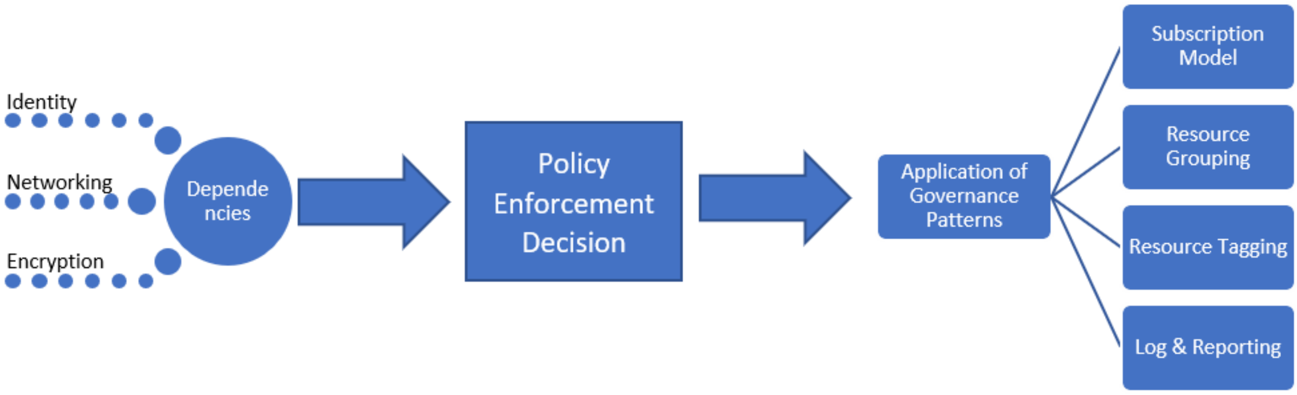
Rapid adoption of governance and corporate policy is achievable, thanks to a few simple principles and cloud-based governance tooling. These are the first three disciplines to approach in any governance process. Each discipline will be further described in this article.

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.

Identity Baseline
Security Baseline
Deployment Acceleration

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 Loging 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 is responsible for the following decisions and implementations. Many require inputs from other teams, but the Cloud Governance team is likely to own both the decision and the 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 Application Category subscription design pattern.

- An application archetype is a way to group 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 mainframes in Azure, or applications that extend on-premises SAP or mainframes. These archetypes are unique per organization, based on data classifications and the types of applications that power the business. Dependency mapping of the digital estate can aid in defining the application archetypes in an organization.
- Departments are not likely to be required given the current focus. Deployments are expected to be constrained within a single billing unit. At the stage of adoption, there may not even be an enterprise agreement to centralize billing. It's likely that this level of adoption is being managed by a single pay-as-you-go Azure subscription.
- Regardless of the use of the EA portal or the existence of an enterprise agreement, a subscription model should still be defined and agreed on to minimize administrative overheard beyond just billing.
- In the **Application Category** pattern, subscriptions are created for each application archetype. Each subscription belongs to an account per environment (Development, Test, and Production).
- A common naming convention should be agreed on as part of the subscription design, based on the previous two points.

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, Deployment Consistency has been chosen as the primary resource consistency pattern.

- Resource groups are created for each application. Management groups are created for each application archetype. Azure Policy should be applied to all subscriptions from the associated management group.
- As part of the deployment process, Azure Resource Consistency templates for the resource group should be stored in source control.
- Each resource group is associated with a specific workload or application.
- Azure management groups enable updating governance designs as corporate policy matures.
- Extensive implementation of Azure Policy could exceed the team's time commitments and may not provide a great deal of value at this time. However, a simple default policy should be created and applied to each management group to enforce the small number of current cloud governance policy statements. This policy will 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 Classification pattern has been chosen as the default model for resource tagging.

- Deployed assets should be tagged with the following values: Data Classification, Criticality, SLA, and Environment.
- These four values will drive governance, operations, and security decisions.
- If this governance journey is being implemented for a business unit or team within a larger corporation, tagging should also include metadata for the billing unit.

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 cloud-native pattern** for logging and reporting is suggested, but not required of any development team at this point.

- No governance requirements have been set regarding the data to be collected for logging or reporting purposes.
- Additional analysis will be needed before releasing any protected data or mission-critical workloads.

Evolution of governance processes

As governance evolves, some policy statements can’t or shouldn’t be controlled by automated tooling. Other policies will result in effort by the IT Security team and the on-premises Identity Management team over time. To help manage new risks as they arise, the Cloud Governance team will oversee the following processes.

Adoption acceleration: The Cloud Governance team has been reviewing deployment scripts across multiple teams. They maintain a set of scripts that serve as deployment templates. Those templates are used by the cloud adoption and DevOps teams to define deployments more quickly. Each of those scripts contains the necessary requirements to enforce a set of governance policies with no additional effort from cloud adoption engineers. As the curators of these scripts, the Cloud Governance team can more quickly implement policy changes. As a result of script curation, the Cloud Governance team is seen as a source of adoption acceleration. This creates consistency among deployments, without strictly forcing adherence.

Engineer training: The Cloud Governance team offers bimonthly training sessions and has created two videos for engineers. These materials help engineers quickly learn the governance culture and how things are done during deployments. The team is adding training assets that show the difference between production and nonproduction deployments, so that engineers will understand how the new policies will affect adoption. This creates consistency among deployments, without strictly forcing adherence.

Deployment planning: Before deploying any asset containing protected data, the Cloud Governance team will review 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 the Cloud Strategy team will 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 selected 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 guide is implemented, each cloud adoption team can go forth with a sound governance foundation. The Cloud Governance team will work in parallel to continuously update the corporate policies and governance disciplines.

The two teams will use the tolerance indicators to identify the next evolution needed to continue supporting cloud adoption. For the fictional company in this journey, the next step is evolving the Security Baseline to support moving protected data to the cloud.

Security Baseline evolution