

Actionable governance journeys

The governance journeys in this section illustrate the incremental approach of the Cloud Adoption Framework governance model. You can establish an agile governance platform that will evolve to meet the needs of any cloud governance scenario.

Review and adopt cloud governance best practices

To start down an adoption path, choose one of the following journeys. Each journey outlines a series of best practices, based on a set of fictional customer experiences. For readers who are new to the incremental approach of the Cloud Adoption Framework governance model, it is advised that you review the high-level governance theory introduction below, before adopting either best practice.

Small-to-Medium Enterprise

A governance journey for enterprises that own fewer than five datacenters and manage costs through a central IT or showback model.

Large Enterprise

A governance journey for enterprises that own more than five datacenters and manage costs across multiple business units.

An incremental approach to cloud governance

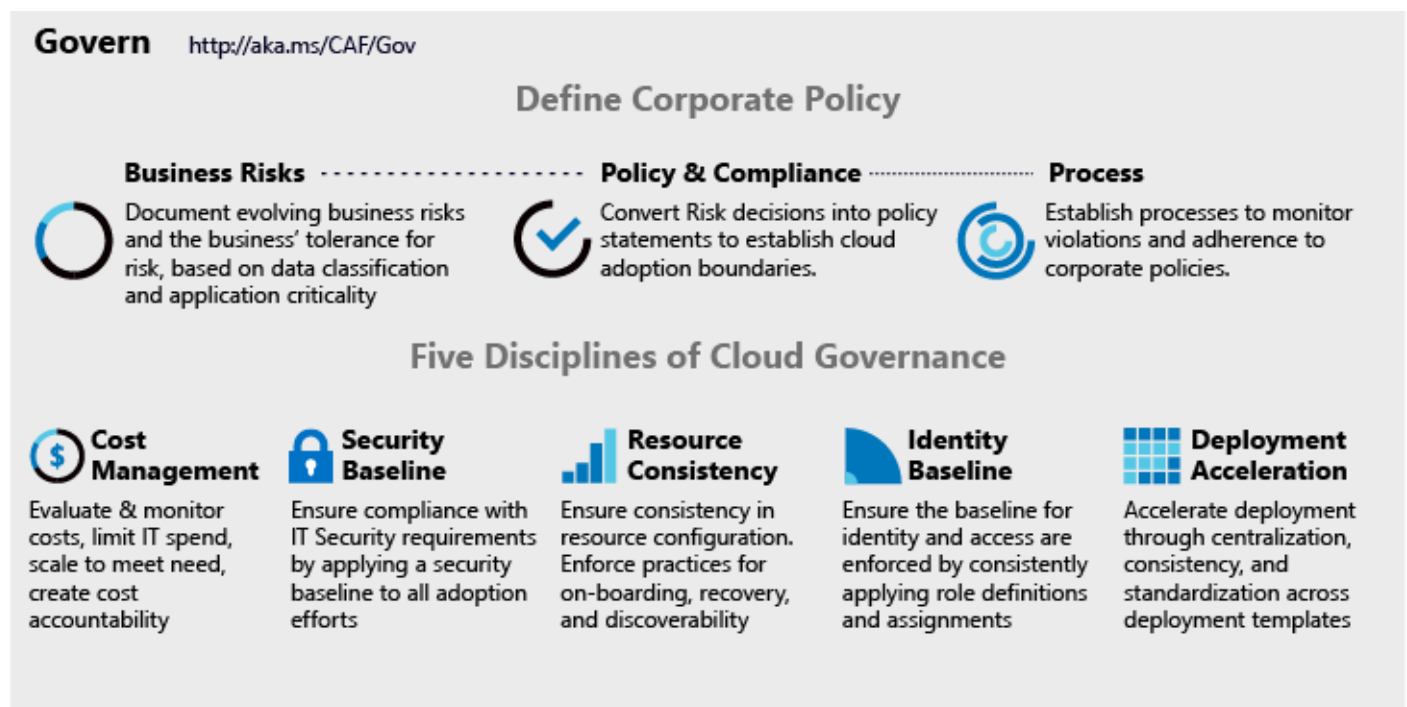
Adopting the cloud is a journey, not a destination. Along the way, there are clear milestones and tangible business benefits. However, the final state of cloud adoption is unknown when a company begins the journey. Cloud governance creates guardrails that keep the company on a safe path throughout the journey.

These governance journeys describe the experiences of fictional companies, based on the journeys of real customers. Each journey follows the customer through the governance aspects of their cloud adoption.

Establishing an end state

A journey without a target destination is just wandering. It's important to establish a rough vision of the end state before taking the first step. The following infographic provides a frame of

reference for the end state. It's not your starting point, but it shows your potential destination.



The Cloud Adoption Framework governance model identifies key areas of importance during the journey. Each area relates to different types of risks the company must address as it adopts more cloud services. Within this framework, the governance journey identifies required actions for the Cloud Governance team. Along the way, each principle of the Cloud Adoption Framework governance model is described further. Broadly, these include:

Corporate policies: Corporate policies drive cloud governance. The governance journey focuses on specific aspects of corporate policy:

- **Business risks:** Identifying and understanding corporate risks.
- **Policy and compliance:** Converting risks into policy statements that support any compliance requirements.
- **Processes:** Ensuring adherence to the stated policies.

Five Disciplines of Cloud Governance: These disciplines support the corporate policies. Each discipline protects the company from potential pitfalls:

- Cost Management
- Security Baseline
- Resource Consistency
- Identity Baseline
- Deployment Acceleration

Essentially, corporate policies serve as the early warning system to detect potential problems. The disciplines help the company manage risks and create guardrails.

Grow to the end state

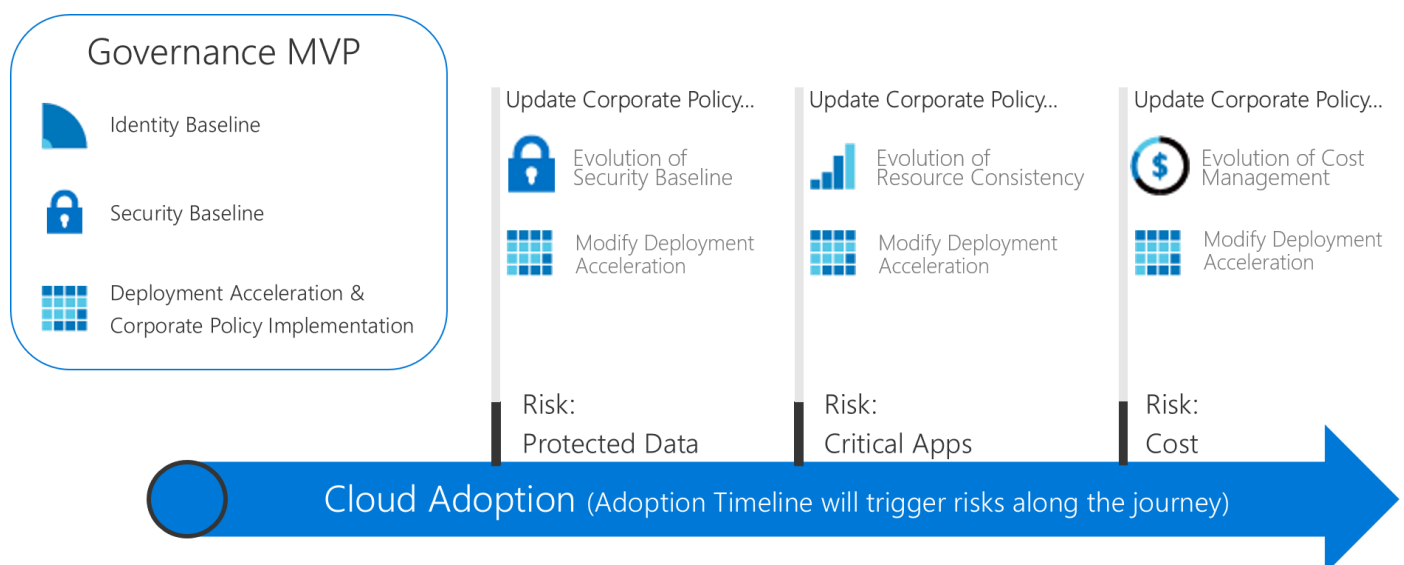
Because governance requirements will evolve throughout the cloud adoption journey, a different approach to governance is required. Companies can no longer wait for a small team to build

guardrails and roadmaps on every highway *before taking the first step*. Business results are expected more quickly and smoothly. IT governance must also move quickly and keep pace with business demands to stay relevant during cloud adoption and avoid "shadow IT."

An **incremental governance** approach empowers these traits. Incremental governance relies on a small set of corporate policies, processes, and tools to establish a foundation for adoption and governance. That foundation is called a **minimum viable product (MVP)**. An MVP allows the governance team to quickly incorporate governance into implementations throughout the adoption lifecycle. An MVP can be established at any point during the cloud adoption process. However, it's a good practice to adopt an MVP as early as possible.

The ability to respond rapidly to changing risks empowers the Cloud Governance team to engage in new ways. The Cloud Governance team can join the Cloud Strategy team as scouts, moving ahead of the cloud adoption teams, plotting routes, and quickly establishing guardrails to manage risks associated with the adoption plans. These just-in-time governance layers are known as **governance evolutions**. With this approach, governance strategy evolves one step ahead of the cloud adoption teams.

The following diagram shows a simple governance MVP and three governance evolutions. During the evolutions, additional corporate policies are defined to remediate new risks. The Deployment Acceleration discipline then applies those changes across each deployment.




ⓘ Note

Governance is not a replacement for key functions such as security, networking, identity, finance, DevOps, or operations. Along the way, there will be interactions with and dependencies on members from each function. Those members should be included on the Cloud Governance team to accelerate decisions and actions.


Choosing a governance journey

The journeys demonstrate how to implement a governance MVP. From there, each journey shows how the Cloud Governance team can work ahead of the cloud adoption teams as a partner to accelerate adoption efforts. The Cloud Adoption Framework governance model guides the application of governance from foundation through subsequent evolutions.

To begin a governance journey, choose one of the two options below. The options are based on synthesized customer experiences. The titles are based on the size of the enterprise for ease of navigation. However, the reader's decision may be more complex. The following tables outline the differences between the two options.

 **Warning**

A more robust governance starting point may be required. In such cases, consider the [Azure Virtual Datacenter](#) approach briefly described [below](#). This approach is commonly suggested during enterprise-scale adoption efforts, and especially for efforts which exceed 10,000 assets. It is also the de facto choice for complex governance scenarios when any of the following are required: extensive third-party compliance requirements, deep domain expertise, or parity with mature IT governance policies and compliance requirements.

 **Note**

It’s unlikely that either journey aligns completely to your situation. Choose whichever journey is closest and use it as a starting point. Throughout the journey, additional information is provided to help you customize decisions to meet specific criteria.

Business characteristics

Characteristic	Small-to-medium enterprise	Large enterprise
Geography (country or geopolitical region)	Customers or staff reside largely in one geography	Customers or staff reside in multiple geographies
Business units affected	Single business unit	Multiple business units
IT budget	Single IT budget	Budget allocated across business units
IT investments	Capital expense-driven investments are planned yearly and usually cover only basic maintenance.	Capital expense-driven investments are planned yearly and often include maintenance and a refresh cycle of three to five years.

Current state before adopting cloud governance

State	Small-to-medium enterprise	Large enterprise
Datacenter or third-party hosting providers	Fewer than five datacenters	More than five datacenters
Networking	No WAN, or 1 – 2 WAN providers	Complex network or global WAN
Identity	Single forest, single domain. No requirement for claims-based authentication or third-party multi-factor authentication devices.	Complex, multiple forests, multiple domains. Applications require claims-based authentication or third-party multi-factor authentication devices.

Desired future state after evolving cloud governance

State	Small-to-medium enterprise	Large enterprise
Cost Management – cloud accounting	Showback model. Billing is centralized through IT.	Chargeback model. Billing could be distributed through IT procurement.
Security Baseline – protected data	Company financial data and IP. Limited customer data. No third-party compliance requirements.	Multiple collections of customers' financial and personal data. May need to consider third-party compliance.
Resource Consistency – mission-critical applications	Outages are painful but not financially damaging. Existing IT Operations are relatively immature.	Outages have defined and monitored financial impacts. IT operations are established and mature.

These two journeys represent two extremes of experience for customers who invest in cloud governance. Most companies reflect a combination of the two scenarios above. After reviewing the journey, use the Cloud Adoption Framework governance model to start the governance conversation and modify the baseline journeys to more closely meet your needs.

Azure Virtual Datacenter

Azure Virtual Datacenter is an approach to making the most of the Azure cloud platform's capabilities while respecting an enterprise's security and governance requirements.

Compared to traditional on-premises environments, Azure allows workload development teams and their business sponsors to take advantage of the increased deployment agility that cloud platforms offer. However, as your cloud adoption efforts expand to include mission-critical data

and workloads, this agility may conflict with corporate security and policy compliance requirements established by your IT teams. This is especially true for large enterprises that have existing sophisticated governance and regulatory requirements.

The Azure Virtual Datacenter approach aims to address these concerns earlier in the adoption lifecycle by providing models, reference architectures, sample automation artifacts, and guidance to help achieve a balance between developer and IT governance requirements during enterprise cloud adoption efforts. Central to this approach is the concept of a virtual datacenter itself: the implementation of isolation boundaries around your cloud infrastructure through the application of access and security controls, network policies, and compliance monitoring.

A virtual datacenter can be thought of as your own isolated cloud within the Azure platform, integrating management processes, regulatory requirements, and security processes required by your governance policies. Within this virtual boundary, Azure Virtual Datacenter offers example models for deploying workloads while ensuring consistent compliance and provides basic guidance on implementing an organization's separation of roles and responsibilities in the cloud.

Azure Virtual Datacenter assumptions

Although smaller teams may benefit from the models and recommendations the Azure Virtual Datacenter provides, this approach is designed to guide enterprise IT groups managing large cloud environments. For organizations that meet the following criteria it's recommended that you consider consulting the Azure Virtual Datacenter guidance when designing your Azure-based cloud infrastructure:

- Your enterprise is subject to regulatory compliance requirements that require centralized monitoring and audit capabilities.
- Your cloud estate will consist of over 10,000 IaaS VMs or an equivalent scale of PaaS services.
- You need to enable agile deployment capabilities for workloads in support of developer and operations teams, while maintaining common policy and governance compliance and central IT control over core services.
- Your industry depends on a complex platform that requires deep domain expertise (for example, finance, oil and gas, or manufacturing).
- Your existing IT governance policies require tighter parity with existing features, even during early stage adoption.

For more information, visit the [Azure Virtual Datacenter](#) section of the Cloud Adoption Framework site.

Next steps

Choose one of these journeys:

Small-to-medium enterprise governance journey

