Large enterprise: Initial corporate policy behind the governance strategy

02/11/2019 • 5 minutes to read • Contributors

In this article

The following corporate policy defines the initial governance position, which is the starting point for this journey. This article defines early-stage risks, initial policy statements, and early processes to enforce policy statements.

> ⓘ **Note**
>
> The corporate policy is not a technical document, but it drives many technical decisions. The governance MVP described in the overview ultimately derives from this policy. Before implementing a governance MVP, your organization should develop a corporate policy based on your own objectives and business risks.

Cloud Governance team

The CIO recently held a meeting with the IT Governance team to understand the history of the PII and mission-critical policies and review the effect of changing those policies. She also discussed the overall potential of the cloud for IT and the company.

After the meeting, two members of the IT Governance team requested permission to research and support the cloud planning efforts. Recognizing the need for governance and an opportunity to limit shadow IT, the Director of IT Governance supported this idea. With that, the Cloud Governance team was born. Over the next several months, they will inherit the cleanup of many mistakes made during exploration in the cloud from a governance perspective. This will earn them the moniker of *cloud custodians*. In later evolutions, this journey will show how their roles change over time.

Objective

The initial objective is to establish a foundation for governance agility. An effective Governance MVP allows the governance team to stay ahead of cloud adoption and implement guardrails as the adoption plan evolves.

Business risks

The company is at an early stage of cloud adoption, experimenting and building proofs of concept. Risks are now relatively low, but future risks are likely. There is little definition around the final state of the technical solutions to be deployed to the cloud. In addition, the cloud readiness of IT employees is low. A foundation for cloud adoption will help the team safely learn and grow.

Future-proofing: There is a risk of not empowering growth, but also a risk of not providing the right protections against future risks.

An agile yet robust governance approach is needed to support the board's vision for corporate and technical growth. Failure to implement such a strategy will slow technical growth, potentially risking market share growth and future market share. The impact of such a business risk is unquestionably high. However, the role IT will play in those potential future states is unknown, making the risk associated with current IT efforts relatively high. That said, until more concrete plans are aligned, the business has a high tolerance for risk.

This business risk can be broken down tactically into several technical risks:

- Well-intended corporate policies could slow transformation efforts or break critical business processes, if not considered within a structured approval flow.
- The application of governance to deployed assets could be difficult and costly.
- Governance may not be properly applied across an application or workload, creating gaps in security.
- With so many teams working in the cloud, there is a risk of inconsistency.
- Costs may not properly align to business units, teams, or other budgetary management units.
- The use of multiple identities to manage various deployments could lead to security issues.
- Despite current policies, there is a risk that protected data could be mistakenly deployed to the cloud.

Tolerance indicators

The current risk tolerance is high and the appetite for investing in cloud governance is low. As such, the tolerance indicators act as an early warning system to trigger the investment of time and energy. If the following indicators are observed, it would be wise to evolve the governance strategy.

- Cost Management: Scale of deployment exceeds 1,000 assets to the cloud, or monthly spending exceeds $10,000 USD per month.
- Identity Baseline: Inclusion of applications with legacy or third-party multi-factor authentication requirements.
- Security Baseline: Inclusion of protected data in defined cloud adoption plans.
- Resource Consistency: Inclusion of any mission-critical applications in defined cloud adoption plans.

Policy statements

The following policy statements establish the requirements needed to remediate the defined risks. These policies define the functional requirements for the governance MVP. Each will be represented in the implementation of the governance MVP.

Cost Management:

- 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.

Security Baseline:

- Any asset deployed to the cloud must have an approved data classification.
- No assets identified with a protected level of data may be deployed to the cloud, until sufficient requirements for security and governance can be approved and implemented.
- Until minimum network security requirements can be validated and governed, cloud environments are seen as a demilitarized zone and should meet similar connection requirements to other datacenters or internal networks.

Resource Consistency:

- Because no mission-critical workloads are deployed at this stage, there are no SLA, performance, or BCDR requirements to be governed.
- When mission-critical workloads are deployed, additional governance requirements will be established with IT operations.

Identity Baseline:

- All assets deployed to the cloud should be controlled using identities and roles approved by current governance policies.
- All groups in the on-premises Active Directory infrastructure that have elevated privileges should be mapped to an approved RBAC role.

Deployment Acceleration:

- All assets must be grouped and tagged according to defined grouping and tagging strategies.
- All assets must use an approved deployment model.
- Once a governance foundation has been established for a cloud provider, any deployment tooling must be compatible with the tools defined by the governance team.

Processes

No budget has been allocated for ongoing monitoring and enforcement of these governance policies. Because of that, the Cloud Governance team has some ad hoc ways to monitor adherence to policy statements.

- **Education:** The Cloud Governance team is investing time to educate the cloud adoption teams on the governance journeys that support these policies.
- **Deployment reviews:** Before deploying any asset, the Cloud Governance team will review the governance journey with the cloud adoption teams.

Next steps

This corporate policy prepares the Cloud Governance team to implement the governance MVP, which will be the foundation for adoption. The next step is to implement this MVP.

Best practice explained