


# Define corporate policy for cloud governance

01/02/2019 • 3 minutes to read • Contributors 

## In this article

[How can corporate IT policy become cloud-ready?](#)

[Review existing policies](#)

[Create cloud policy statements](#)

[Incremental governance and integrating with existing policy](#)

[Next steps](#)

Once you've analyzed the known risks and related risk tolerances for your organization's cloud transformation journey, your next step is to establish policy that will explicitly address those risks and define the steps needed to remediate them where possible.

## How can corporate IT policy become cloud-ready?

In traditional governance and incremental governance, corporate policy creates the working definition of governance. Most IT governance actions seek to implement technology to monitor, enforce, operate, and automate those corporate policies. Cloud Governance is built on similar concepts.

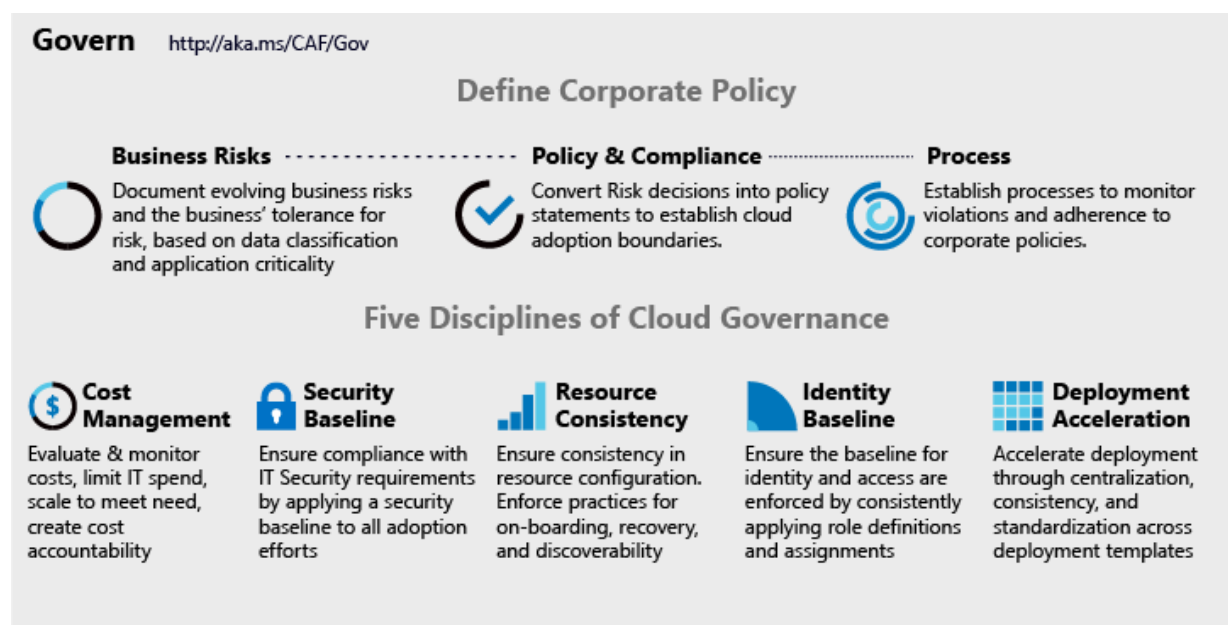


Figure 1. Corporate governance and governance disciplines.

The image above illustrates the relationship between business risk, policy and compliance, and monitoring and enforcement mechanisms that will need to interact as part of your governance strategy. The Five Disciplines of Cloud Governance allow you to manage these interactions and realize your strategy.

Cloud governance is the product of an ongoing adoption effort over time, as a true lasting transformation doesn't happen overnight. Attempting to deliver complete cloud governance before addressing key corporate policy changes using a fast aggressive method seldom produces the desired results. Instead we recommend an incremental approach.

What is different about a cloud adoption framework is the purchasing cycle and it can enable authentic transformation. Since there is not a large capital expenditure acquisition requirement, engineers can begin experimentation and adoption sooner. In most corporate cultures, elimination of the capital expense barrier to adoption can lead to tighter feedback loops, organic growth, and incremental execution.

The shift to cloud adoption requires a shift in governance. In many organizations, corporate policy transformation allows for improved governance and higher rates of adherence through incremental policy changes and automated enforcement of those changes, powered by newly defined capabilities that you configure with your cloud service provider.

## Review existing policies

As governance is an ongoing process, policy should be regularly reviewed with IT staff and stakeholders to ensure resources hosted in the cloud continue to maintain compliance with overall corporate goals and requirements. Your understanding of new risks and acceptable tolerance can fuel a [review of existing policies](#), in order to determine the required level of governance that is appropriate for your organization.

### Tip

If your organization uses vendors or other trusted business partners, one of the biggest business risks to consider may be a lack of adherence to [regulatory compliance](#) by these external organizations. This risk often cannot be remediated, and instead may require a strict adherence to requirements by all parties. Make sure you've identified and understand any third-party compliance requirements before beginning a policy review.

## Create cloud policy statements

Cloud-based IT policies establish the requirements, standards, and goals that your IT staff and automated systems will need to support. Policy decisions are a primary factor in your [cloud architecture design](#) and how you will implement your [policy adherence processes](#).

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. While these policies can be integrated into your wider corporate policy documentation, cloud policy statements discussed throughout the Cloud Adoption Framework guidance tends to be a more concise summary of the risks and plans to deal with them. Each definition should include these pieces of information:

- **Business risk:** A summary of the risk this policy will address.
- **Policy statement:** A concise explanation of the policy requirements and goals.
- **Design or technical guidance:** Actionable recommendations, specifications, or other guidance to support and enforce this policy that IT teams and developers can use when designing and building their cloud deployments.

If you need help getting started with defining policies, consult the [governance disciplines](#) introduced in the governance section overview. The articles for each of these disciplines includes examples of common business risks encountered when moving to the cloud and sample policies used to remediate those risks (for example, see the Cost Management discipline's [sample policy definitions](#)).

## Incremental governance and integrating with existing policy

Planned additions to your cloud environment should always be vetted for compliance with existing policy, and policy updated to account for any issues not already covered. You should also perform regular [cloud policy review](#) to ensure your cloud policy is up-to-date and in-sync with any new corporate policy.

The need to integrate cloud policy with your legacy IT policies depends largely on the maturity of your cloud governance processes and the size of your cloud estate. See the article on [incremental governance and the policy MVP](#) for a broader discussion on dealing with policy integration during your cloud transformation.

## Next steps

After defining your policies, draft an architecture design guide to provide IT staff and developers with actionable guidance.

Draft an architecture design guide