What is a cloud policy review?

02/11/2019 • 3 minutes to read • Contributors

In this article

A **cloud policy review** is the first step toward governance maturity in the cloud. The objective of this process is to modernize existing corporate IT policies. When completed, the updated policies provide an equivalent level of risk management for cloud-based resources. This article explains the cloud policy review process and its importance.

Why perform a cloud policy review?

Most businesses manage IT through the execution of processes which alignment with governing policies. In small businesses, these policies may anecdotal and processes loosely defined. As businesses grow into large enterprises, policies and processes tend to be more clearly documented and consistently executed.

As companies mature corporate IT policies, dependencies on past technical decisions have a tendency to seep into governing policies. For instance, its common to see disaster recovery processes include policy that mandates offsite tape backups. This inclusion assumes a dependency on one type of technology (tape backups), that may no longer be the most relevant solution.

Cloud transformations create a natural inflection point to reconsider the legacy policy decisions of the past. Technical capabilities and default processes change considerably in the cloud, as do the inherit risks. Using the prior example, the tape backup policy stemmed from the risk of a single point of failure by keeping data in one location and the business need to minimize the risk profile by mitigating this risk. In a cloud deployment, there are several options that deliver the same risk mitigation, with much lower recovery time objectives (RTO). For example:

- A cloud-native solution could enable geo-replication of the Azure SQL Database.
- A hybrid solution could use Azure Site Recovery to replicate an IaaS workload to multiple datacenters.

When executing a cloud transformation, policies often govern many of the tools, services, and processes available to the cloud adoption teams. If those policies are based on legacy technologies, they may hinder the team's efforts to drive change. In the worst case, important policies are entirely ignored by the migration team to enable workarounds. Neither is an acceptable outcome.

The cloud policy review process

Cloud policy reviews align existing IT governance and IT security policies with the Five Disciplines of Cloud Governance: Cost Management, Security Baseline, Identity Baseline, Resource Consistency, and Deployment Acceleration.

For each of these disciplines, the review process follows these steps:

1. Review existing on-premises policies related to the specific discipline, looking for two key data points: legacy dependencies and identified business risks.
2. Evaluate each business risk by asking a simple question: "Does the business risk still exist in a cloud model?"
3. If the risk still exists, rewrite the policy by documenting the necessary mitigation, not the technical solution.
4. Review the updated policy with the cloud adoption teams to understand potential solutions to the required mitigation.

Example of a policy review for a legacy policy

To provide an example of the process, let's again use the tape backup policy in the prior section:

- A corporate policy mandates offsite tape backups for all production systems. In this policy, you can see two data points of interest:
  - Legacy dependency on a tape backup solution
  - An assumed business risk associated with the storage of backups in the same physical location as the production equipment.
- Does the risk still exist? Yes. Even in the cloud, a dependence on a single facility does create some risk. There is a lower probability of this risk affecting the business than was present in the on-premises solution, but the risk still exists.
- Rewrite of the policy. In the case of a datacenter-wide disaster, there must exist a means of restoring production systems within 24 hours of the outage in a different datacenter and different geographic location.
- Review with the cloud adoption teams. Depending on the solution being implemented, there are multiple means of adhering to this Resource Consistency policy.