Resource Consistency motivations and business risks

02/11/2019 • 2 minutes to read • Contributors

In this article

This article discusses the reasons that customers typically adopt a Resource Consistency discipline within a cloud governance strategy. It also provides a few examples of potential business risks that can drive policy statements.

Is Resource Consistency relevant?

When it comes to deploying resources and workloads, the cloud offers increased agility and flexibility over most traditional on-premises datacenters. However, these potential cloud-based advantages also come paired with potential management drawbacks that can seriously jeopardize the success of your cloud adoption. What assets have you deployed? What teams own what assets? Do you have enough resources supporting a workload? How do you know if workloads are healthy?

Resource Consistency is crucial to ensure that resources are deployed, updated, and configured consistently and repeatably, and that service disruptions are minimized and remedied in as little time as possible.

The Resource Consistency discipline is concerned with identifying and mitigating business risks related to the operational aspects of your cloud deployment. Resource Consistency includes monitoring of applications, workloads, and asset performance. It also includes the tasks required to meet scale demands, provide disaster recovery capabilities, mitigate performance Service Level Agreement (SLA) violations, and proactively avoid those SLA violations through automated remediation.

Initial test deployments may not require much beyond adopting some cursory naming and tagging standards to support your Resource Consistency needs. As your cloud adoption matures and you deploy more complicated and mission-critical assets, the need to invest in the Resource Consistency discipline increases rapidly.

Business risk

The Resource Consistency discipline attempts to address core operational business risks. Work with your business and IT teams to identify these risks and monitor each of them for relevance as you plan for and implement your cloud deployments.

Risks will differ between organization, but the following serve as common risks that you can use as a starting point for discussions within your Cloud Governance team:

- **Unnecessary operational cost.** Obsolete or unused resources, or resources that are overprovisioned during times of low demand, add unnecessary operational costs.
- **Underprovisioned resources.** Resources that experience higher than anticipated demand can result in business disruption as cloud resources are overwhelmed by demand.
- **Management inefficiencies.** Lack of consistent naming and tagging metadata associated with resources can lead to IT staff having difficulty finding resources for management tasks or identifying ownership and accounting

information related to assets. This results in management inefficiencies that can increase cost and slow IT responsiveness to service disruption or other operational issues.

- **Business interruption.** Service disruptions that result in violations of your organization's established Service Level Agreements (SLAs) can result in loss of business or other financial impacts to your company.

Next steps

Using the Cloud Management template, document business risks that are likely to be introduced by the current cloud adoption plan.

Once an understanding of realistic business risks is established, the next step is to document the business's tolerance for risk and the indicators and key metrics to monitor that tolerance.

Understand indicators, metrics, and risk tolerance