How does business risk change in the cloud?

04/04/2019 • 4 minutes to read • Contributors

In this article

An understanding of business risk is one of the most important elements of any cloud transformation. Risk drives policy, and it influences monitoring and enforcement requirements. Risk heavily influences how we manage the digital estate, on-premises or in the cloud.

Relativity of risk

Risk is relative. A small company with a few IT assets, in a closed building has little risk. Add users and an internet connection with access to those assets, the risk is intensified. When that small company grows to Fortune 500 status, the risks are exponentially greater. As revenue, business process, employee counts, and IT assets accumulate, risks increase and coalesce. IT assets that aid in generating revenue are at tangible risk of stopping that revenue stream in the event of an outage. Every moment of downtime equates to losses. Likewise, as data accumulates, the risk of harming customers grows.

In the traditional on-premises world, IT governance teams focus on assessing risks, creating processes to manage those risks, and deploying systems to ensure remediation measures are successfully implemented. These efforts work to balance risks required to operate in a connected, modern business environment.

Understanding business risks in the cloud

During a transformation, the same relative risks exist.

- During early experimentation, a few assets are deployed with little to no relevant data. The risk is small.
- When the first workload is deployed, risk goes up a little. This risk is easily remediated by choosing an inherently low risk application with a small user base.
- As more workloads come online, risks change at each release. New apps go live, risks change.
- When a company brings the first 10-20 applications online, the risk profile is much different that it is when the 1000th applications go into production in the cloud.

The assets that accumulated in the traditional, on-premises estate likely accumulated over time. The maturity of the business and IT teams was likely growing in a similar fashion. That parallel growth can tend to create some unnecessary policy baggage.

During a cloud transformation, both the business and IT teams have an opportunity to reset those policies and build new with a matured mindset.

What is a business risk MVP?

A **minimum viable product** is commonly used to define to define the smallest unit of something that can produce tangible value. In a business risk MVP, the Cloud Governance team starts with the assumption that some assets will be deployed to a cloud environment at some point in time. It's unknown what those assets are at the time, and the team may be unsure what types of data will be stored on those assets.

When planning for business risk, the Cloud Governance team could build for the worst case scenario and map every possible policy to the cloud. However, identifying all potential business risks for all cloud usage scenarios can take considerable time and effort, potentially delaying the implementation of governance to your cloud workloads. This is not advised, but is an option.

Conversely, an MVP approach can allow the team to define an initial starting point and set of assumptions that would be true for most/all assets. This business risk MVP will support initial small scale or test cloud deployments, and then be used as a base for gradually identifying and remediating new risks as business needs arise or additional workloads are added to your cloud environment. This process allows you to apply governance throughout the cloud adoption process.

The following are a few basic examples of business risks that can be included as part of an MVP:

- All assets are at risk of being terminated (through error, mistake or maintenance).
- All assets are at risk of generating too much spending.
- All assets could be compromised by weak passwords.
- Any asset with all open ports exposed to the internet are at risk of compromise.

The above examples are meant to establish MVP business risks as a theory. The actual list will be unique to every environment. Once the Business Risk MVP is established, they can be converted to policies to remediate each risk.

Incremental risk mitigation

As your organization deploys more workloads to the cloud, development teams will make use of increasing amounts of cloud resources. At each iteration, new assets are created and staged. At each release, workloads are readied for production promotion. Each of these cycles has the potential to introduce previously unidentified business risks.

Assuming a business risk MVP is the starting point for your initial cloud adoption efforts, governance can mature in parallel to your increasing use of cloud resources. When the Cloud Governance team operates in parallel to cloud adoption teams, the growth of business risks can be addressed as they are identified, providing a stable ongoing model for developing governance maturity.

Each asset staged can easily be classified according to risk. Data classification documents can be built or created in parallel to staging cycles. Risk profile and exposure points can likewise be documented. Over time an extremely clear view of business risk will come into focus across the organization.

With each iteration, the Cloud Governance team can work with the Cloud Strategy team to quickly communicate new risks, mitigation strategies, tradeoffs, and potential costs. This empowers business participants and IT leaders to partner in mature, well-informed decisions. Those decisions then inform policy maturity. When required, the policy changes produce new work items for the maturity of core infrastructure systems. When changes to staged systems are required, the cloud adoption teams have ample time to make changes, while the business tests the staged systems and develops a user adoption plan.

This approach minimizes risks, while empowering the team to move quickly. It also ensures that risks are promptly addressed and resolved before deployment.

Next steps

Evaluate risk tolerance