Security Baseline motivations and business risks

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

In this article

Is a Security Baseline relevant?
Business risk
Next steps

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

Is a Security Baseline relevant?

Security is a key concern for any IT organization. Cloud deployments face many of the same security risks as workloads hosted in traditional on-premises datacenters. However, the nature of public cloud platforms, with a lack of direct ownership of the physical hardware storing and running your workloads, means cloud security requires its own policy and processes.

One of the primary things that sets cloud security governance apart from traditional security policy is the ease with which resources can be created, potentially adding vulnerabilities if security isn't considered before deployment. The flexibility that technologies like software defined networking (SDN) provide for rapidly changing your cloud-based network topology can also easily modify your overall network attack surface in unforeseen ways. Cloud platforms also provide tools and features that can improve your security capabilities in ways not always possible in on-premises environments.

The amount you invest into security policy and processes will depend a great deal on the nature of your cloud deployment. Initial test deployments may only need the most basic of security policies in place, while a mission-critical workload will entail addressing complex and extensive security needs. All deployments will need to engage with the discipline at some level.

The Security Baseline discipline covers the corporate policies and manual processes that you can put in place to protect your cloud deployment against security risks.

> **Note**
>
> While it is important to understand Identity Baseline in the context of Security Baseline and how that relates to Access Control, the Five Disciplines of Cloud Governance calls out Identity Baseline as its own discipline, separate from Security Baseline.

Business risk

The Security Baseline discipline attempts to address core security-related business risks. Work with your business 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 security-related risks that you can use as a starting point for discussions within your Cloud Governance team:

- **Data breach:** Inadvertent exposure or loss of sensitive cloud-hosted data can lead to losing customers, contractual issues, or legal consequences.
- **Service disruption:** Outages and other performance issues due to insecure infrastructure interrupts normal operations and can result in lost productivity or lost business.

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