Identity Baseline motivations and business risks

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

In this article

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

Is Identity Baseline relevant?

Traditional on-premises directories are designed to allow businesses to strictly control permissions and policies for users, groups, and roles within their internal networks and datacenters. This is usually intended to support single tenant implementations, with services applicable only within the on-premises environment.

Cloud identity services are intended to expand an organization's authentication and access control capabilities to the internet. They support multitenancy and can be used to manage users and access policy across cloud applications and deployments. Public cloud platforms have some form of cloud-native identity services supporting management and deployment tasks and are capable of varying levels of integration with your existing on-premises identity solutions. All of these features can result in cloud identity policy being more complicated than your traditional on-premises solutions require.

The importance of the Identity Baseline discipline to your cloud deployment will depend on the size of your team and need to integrate your cloud-based identity solution with an existing on-premises identity service. Initial test deployments may not require much in the way of user organization or management, but as your cloud estate matures, you will likely need to support more complicated organizational integration and centralized management.

Business risk

The Identity Baseline discipline attempts to address core business risks related to identity services and access control. 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 identity-related risks that you can use as a starting point for discussions within your Cloud Governance team:

- **Unauthorized access.** Sensitive data and resources that can be accessed by unauthorized users can lead to data leaks or service disruptions, violating your organization's security perimeter and risking business or legal liabilities.
- **Inefficiency due to multiple identity solutions.** Organizations with multiple identity services tenants can require multiple accounts for users. This can lead to inefficiency for users who need to remember multiple sets of credentials and for IT in managing accounts across multiple systems. If user access assignments are not updated across identity solutions as staff, teams, and business goals change, your cloud resources may be vulnerable to unauthorized access or users unable to access required resources.
- **Inability to share resources with external partners.** Difficulty adding external business partners to your existing identity solutions can prevent efficient resource sharing and business communication.

- **On-premises identity dependencies.** Legacy authentication mechanisms or third-party multi-factor authentication might not be available in the cloud, requiring either migrating workloads to be retooled, or additional identity services to be deployed to the cloud. Either requirement could delay or prevent migration, and increase costs.

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