Identity Baseline discipline overview

Identity Baseline is one of the Five Disciplines of Cloud Governance within the Cloud Adoption Framework governance model. Identity is increasingly considered the primary security perimeter in the cloud, which is a shift from the traditional focus on network security. Identity services provide the core mechanisms supporting access control and organization within IT environments, and the Identity Baseline discipline complements the Security Baseline discipline by consistently applying authentication and authorization requirements across cloud adoption efforts.

> **Note**
>
> Identity Baseline governance does not replace the existing IT teams, processes, and procedures that allow your organization to manage and secure identity services. The primary purpose of this discipline is to identify potential identity-related business risks and provide risk-mitigation guidance to IT staff that are responsible for implementing, maintaining, and operating your identity management infrastructure. As you develop governance policies and processes make sure to involve relevant IT teams in your planning and review processes.

This section of the Cloud Adoption Framework outlines the approach to developing an Identity Baseline discipline as part of your cloud governance strategy. The primary audience for this guidance is your organization's cloud architects and other members of your Cloud Governance team. However, the decisions, policies, and processes that emerge from this discipline should involve engagement and discussions with relevant members of the IT teams responsible for implementing and managing your organization's identity management solutions.

If your organization lacks in-house expertise in Identity Baseline and security, consider engaging external consultants as a part of this discipline. Also consider engaging Microsoft Consulting Services, the Microsoft FastTrack cloud adoption service, or other external cloud adoption experts to discuss concerns related to this discipline.

Policy statements

Actionable policy statements and the resulting architecture requirements serve as the foundation of an Identity Baseline discipline. To see policy statement samples, see the article on Identity Baseline Policy Statements. These samples can serve as a starting point for your organization's governance policies.

> **Caution**
>
> The sample policies come from common customer experiences. To better align these policies to specific cloud governance needs, execute the following steps to create policy statements

that meet your unique business needs.

Developing Identity Baseline governance policy statements

The following six steps offer examples and potential options to consider when developing Identity Baseline governance. Use each step as a starting point for discussions within your Cloud Governance team and with affected business, and IT teams across your organization to establish the policies and processes needed to manage identity-related risks.

Identity Baseline Template
Download the template for documenting an Identity Baseline discipline

Business Risks
Understand the motives and risks commonly associated with the Identity Baseline discipline.

Indicators and Metrics
Indicators to understand if it is the right time to invest in the Identity Baseline discipline.

Policy adherence processes
Suggested processes for supporting policy compliance in the Identity Baseline discipline.

Maturity

Aligning Cloud Management maturity with phases of cloud adoption.

Toolchain

Azure services that can be implemented to support the Identity Baseline discipline.

Next steps

Get started by evaluating business risks in a specific environment.

Understand business risks