Security Baseline discipline overview

Security Baseline is one of the Five Disciplines of Cloud Governance within the Cloud Adoption Framework governance model. Security is a component of any IT deployment, and the cloud introduces unique security concerns. Many businesses are subject to regulatory requirements that make protecting sensitive data a major organizational priority when considering a cloud transformation. Identifying potential security threats to your cloud environment and establishing processes and procedures for addressing these threats should be a priority for any IT Security or Cybersecurity team. The Security Baseline discipline ensures technical requirements and security constraints are consistently applied to cloud environments, as those requirements mature.

> **Note**
>
> Security Baseline governance does not replace the existing IT teams, processes, and procedures that your organization uses to secure cloud-deployed resources. The primary purpose of this discipline is to identify security-related business risks and provide risk-mitigation guidance to the IT staff responsible for security infrastructure. As you develop governance policies and processes make sure to involve relevant IT teams in your planning and review processes.

This article outlines the approach to developing a Security 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 your IT and security teams, especially those technical leaders responsible for implementing networking, encryption, and identity services.

Making the correct security decisions is critical to the success of your cloud deployments and wider business success. If your organization lacks in-house expertise in cybersecurity, consider engaging external security consultants as a component 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 a Security Baseline discipline. To see policy statement samples, see the article on Security 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 Security Baseline governance policy statements

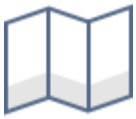
The following six steps offer examples and potential options to consider when developing Security Baseline governance. Use each step as a starting point for discussions within your Cloud Governance team and with affected business, IT, and security teams across your organization to establish the policies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

Security Baseline Template
Download the template for documenting a Security Baseline discipline

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

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

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



Maturity

Aligning Cloud Management maturity with phases of cloud adoption.

Toolchain

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

Next steps

Get started by evaluating business risks in a specific environment.

Understand business risks