


Identity Baseline sample policy statements

02/11/2019 • 3 minutes to read • Contributors 

In this article

[Lack of access controls](#)

[Overprovisioned access](#)

[Lack of shared management accounts between on-premises and the cloud](#)

[Weak authentication mechanisms](#)

[Isolated identity providers](#)

[Identity reviews](#)

[Next steps](#)

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. These statements should provide a concise summary of risks and plans to deal with them. Each statement definition should include these pieces of information:

- **Technical risk:** A summary of the risk this policy will address.
- **Policy statement:** A clear summary explanation of the policy requirements.
- **Design options:** Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The following sample policy statements address common identity-related business risks. These statements are examples you can reference when drafting policy statements to address your organization's needs. These examples are not meant to be proscriptive, and there are potentially several policy options for dealing with each identified risk. Work closely with business and IT teams to identify the best policies for your unique set of risks.

Lack of access controls

Technical risk: Insufficient or ad-hoc access control settings can introduce risk of unauthorized access to sensitive or mission-critical resources.

Policy statement: All assets deployed to the cloud should be controlled using identities and roles approved by current governance policies.

Potential design options: [Azure Active Directory conditional access](#) is the default access control mechanism in Azure.

Overprovisioned access

Technical risk: Users and groups with control over resources beyond their area of responsibility can result in unauthorized modifications leading to outages or security vulnerabilities.

Policy statement: The following policies will be implemented:

- A least-privilege access model will be applied to any resources involved in mission-critical applications or protected data.
- Elevated permissions should be an exception, and any such exceptions must be recorded with the Cloud Governance team. Exceptions will be audited regularly.

Potential design options: Consult the [Azure Identity Management best practices](#) to implement a role-based access control (RBAC) strategy that restricts access based on the [need to know](#) and [least-privilege security](#) principles.

Lack of shared management accounts between on-premises and the cloud

Technical risk: IT management or administrative staff with accounts on your on-premises Active Directory may not have sufficient access to cloud resources may not be able to efficiently resolve operational or security issues.

Policy statement: All groups in the on-premises Active Directory infrastructure that have elevated privileges should be mapped to an approved RBAC role.

Potential design options: Implement a hybrid identity solution between your cloud-based Azure Active Directory and your on-premises Active Directory, and add the required on-premises groups to the RBAC roles necessary to do their work.

Weak authentication mechanisms

Technical risk: Identity management systems with insufficiently secure user authentication methods, such as basic user/password combinations, can lead to compromised or hacked passwords, providing a major risk of unauthorized access to secure cloud systems.

Policy statement: All accounts are required to sign in to secured resources using a multi-factor authentication method.

Potential design options: For Azure Active Directory, implement [Azure Multi-Factor Authentication](#) as part of your user authorization process.

Isolated identity providers

Technical risk: Incompatible identity providers can result in the inability to share resources or services with customers or other business partners.

Policy statement: Deployment of any applications that require customer authentication must use an approved identity provider that is compatible with the primary identity provider for internal users.

Potential design options: Implement [Federation with Azure Active Directory](#) between your internal and customer identity providers.

Identity reviews

Technical risk: Over time business change, the addition of new cloud deployments or other security concerns can increase the risks of unauthorized access to secure resources.

Policy statement: Cloud Governance processes must include quarterly review with identity management teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

Potential design options: Establish a quarterly security review meeting that includes both governance team members and IT staff responsible for managing identity services. Review existing security data and metrics to establish gaps in current identity management policy and tooling, and update policy to remediate any new risks.

Next steps

Use the samples mentioned in this article as a starting point for developing policies to address specific business risks that align with your cloud adoption plans.

To begin developing your own custom policy statements related to Identity Baseline, download the [Identity Baseline template](#).

To accelerate adoption of this discipline, choose the [actionable governance journey](#) that most closely aligns with your environment. Then modify the design to incorporate your specific corporate policy decisions.

Actionable governance journeys