# How to use this template

This sample template is designed to help you define the policy statements and design guidance that allow you to mature the [Five Disciplines of Cloud Governance](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/governance-disciplines) within your organization. The examples in this template are focused on the [Identity Baseline](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/identity-baseline/overview) discipline. Use these examples as a starting point for discussions within your organization around this discipline.

The following instructions will guide usage of this template:

* Update the template's title page with your author information, publish date and the governance discipline this document supports.
* Update this template to reflect risks, tolerance, indictors, toolchains, etc., that align to your business and technology needs.
* Update this template to reflect your policy statements.
* Update this template's executive summary to reflect your updated content.
* Before publication remove the “sample” watermark.
* Delete this page and update the table of contents before publishing your customized policy statements.

**Microsoft Cloud Adoption Framework for Azure**

**Cloud Governance**

Identity Baseline Discipline

Policy Statements and Design Guidance

The document outlines the policy statements, design guidance, and processes required to support the Identity Baseline governance discipline during cloud adoption. Associated risks, tolerance, and remediation strategies are included for reference.

**Author(s):** <Update Author>

**Date Published:** 03/3/2019

Contents

[How to use this template 1](#_Toc2782560)

[Executive Summary 3](#_Toc2782561)

[Policy Statements 3](#_Toc2782562)

[Business Risks 4](#_Toc2782563)

[Metrics and Indicators 4](#_Toc2782564)

[Metrics 4](#_Toc2782565)

[Indicators 5](#_Toc2782566)

[Policy compliance processes 6](#_Toc2782567)

[Planning, review, and reporting processes 6](#_Toc2782568)

[Ongoing monitoring 7](#_Toc2782569)

[Violation Triggers and Enforcement Actions 7](#_Toc2782570)

[Toolchain 8](#_Toc2782571)

[Azure Specific Tooling 8](#_Toc2782572)

[Tooling for other Cloud Providers 8](#_Toc2782573)

# Executive Summary

Cloud identity services are intended to expand an organization's authentication and access control capabilities to the internet and are used to manage users and access policy across cloud applications and deployments. Cloud-native identity services are capable of varying levels of integration with existing on-premises identity solutions, which can result in cloud identity policy being more complicated than traditional on-premises solutions require. This document identifies and determines the business’s tolerance for risks, and outlines efforts to remediate these risks. The result is a series of policy statements that should guide the architecture of any solutions deployed to the cloud.

This policies and guidance in this document has been developed in conjunction with the governance best practices documented in the [Microsoft Cloud Adoption Framework for Azure (CAF)](http://aka.ms/caf).

# Policy Statements

The following statements should guide cloud adoption architecture decisions to ensure compliance with governance efforts related to the Identity Baseline discipline. For additional examples of relevant policy statements, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/identity-baseline/policy-statements).

**Lack of access controls**: All assets deployed to the cloud should be controlled using identities and RBAC roles approved by current governance policies.

**Weak authentication mechanisms**: All accounts are required to login to secured resources using a multi-factor authentication (MFA) method.

**Lack of shared management accounts between on-premises and the cloud**: All groups in the on-premises Active Directory infrastructure that have elevated privileges should be mapped to an approved Microsoft Entra ID RBAC role.

# Business Risks

The following Identity related business risks have been identified as concerns based on the current plans for cloud adoption. For additional examples of relevant business risks, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/identity-baseline/business-risks).

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Description | Indicators | Resolution |
| **Unauthorized access** | Sensitive data and resources that can be accessed by unauthorized users can lead to data leaks or service disruptions, violating security perimeters and risking business or legal liabilities. | Current | Policy Statements enforced |
| **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. | Cloud workloads dependent on legacy authentication mechanisms | Policy statements drafted but not enforced |
| **Inefficiency due to multiple identity solutions** | Organizations with multiple directories 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. | More than 3 deployed Active Directory Domains | Policy statements drafted but not enforced |

# Metrics and Indicators

The following are key metrics and indicators that will guide the resolution or mitigation of business risks. For additional examples of relevant metrics or indicators, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/identity-baseline/metrics-tolerance).

## Metrics

This governance discipline attempts to govern or improve the following key metrics.

* Overall size of directory services infrastructure: Number of directory forests, domains, and tenants used by the organization.
* Dependency on legacy or on-premises authentication mechanisms: Cloud deployed workloads are dependent on legacy authentication mechanisms or third-party multi-factor authentication (MFA) services.
* Elevated users: Number of user accounts with elevated access to resources or management tools.
* Use of RBAC: Number of subscriptions, resource groups, or individual resources not managed through role-based access control (RBAC).
* Compromised accounts: Number of user accounts that have been compromised.

## Indicators

The following indicators will trigger changes in policy statements based on changes in metrics and other conditions.

* Current: Current state of metrics. Any policy statements listed as current should be actively enforced.
* Elevated access: If more than 15% of users have elevated permissions to management tools and resources will require policies to limit overprovisioning of access.
* RBAC: If fewer than 75% of resources are using role-based access control methods, policy statements requiring RBAC on all resources will be created.
* Authentication failures: If authentication failures represent more than 15% of attempts, policies are required to ensure IT investigates that authentication methods are not under external attack, and that users are able to use authentication methods correctly.
* Directory services complexity: If more than 3 forests, domains, or directory tenants are used to provide cloud-based directory services, policies are required to ensure directory synchronization allowing for common credentials between directories.

# Policy compliance processes

The following section outlines the processes that will ensure cloud deployments remain in compliance with Identity Baseline policies. This includes an overview of the planning, review and reporting processes performed by the Cloud Governance team, as well as the ongoing monitoring and enforcement processes that can be automated or supplemented with tooling to allow for faster response to policy deviation.

For additional examples of relevant policy compliance processes, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/identity-baseline/compliance-processes).

## Planning, review, and reporting processes

Initial risk assessment and planning: As part of the initial adoption of the Identity Baseline discipline, the Cloud Governance team will identify the core business risks and tolerances related to cloud identity management. The team will use this information to discuss specific technical risks with members of the IT teams responsible for managing identity services and develop a baseline set of security policies for mitigating these risks as part of establishing an initial governance strategy.

Deployment planning: Before any workload deployments, the Cloud Governance team will review the access needs of the workloads and develop an access control strategy that aligns with established corporate identity policy. The team will document any gaps between these needs and current policy to determine if policy updates are required, and modify policy as needed.

Deployment testing: As part of the deployment, the Cloud Governance team, in cooperation with IT teams responsible for identity services, will be responsible for reviewing the deployment to validate identity policy compliance.

Annual planning: On an annual basis, the Cloud Governance team will perform a high-level review of identity management strategy. This review will explore planned changes to the identity services environment and updated cloud adoption strategies to identify the potential for increased risk or the need to modify current identity infrastructure patterns. Also, the team will use this process to review the latest identity management best practices and integrate these into policies and review processes.

Quarterly planning: On a quarterly basis the Cloud Governance team will perform a general review of identity and access control audit data. The team will meet with cloud adoption teams to identify any potential new risks or operational requirements that would require updates to identity policy or changes in access control strategy.

The quarterly planning process will also include an evaluation of the Cloud Governance team's current membership to identify knowledge gaps related to new or evolving policy and risks related to identity. The Cloud Governance team will invite relevant IT staff to participate in reviews and planning as either temporary technical advisors or permanent members of the team.

Education and Training: On a bi-monthly basis, the Cloud Governance team will offer training sessions to make sure IT staff and developers are up-to-date on the latest identity policy requirements. As part of this process the team will also review and update any documentation, guidance, or other training assets to ensure they are in sync with the latest corporate policy statements.

Monthly audit and reporting reviews: The Cloud Governance team will conduct an audit on all cloud deployments on a monthly basis to assure their continued alignment with identity policy. This review will check user access against business change to ensure users have correct access to cloud resources and ensure access strategies such as RBAC are being followed consistently. Privileged accounts will be identified, and their purpose documented. This review process will result in a report for the Cloud Strategy team and each cloud adoption team detailing overall adherence to policy. The report is also stored for auditing and legal purposes.

## Ongoing monitoring

IT teams will implement automated monitoring systems for the organization's identity infrastructure, capturing relevant log data needed to evaluate risks related to identity services. They will also establish reporting and alerting systems to ensure prompt detection and mitigation of potential security policy violations.

## Violation Triggers and Enforcement Actions

Suspicious activity detected: User logins detected from anonymous proxy IP addresses, unfamiliar locations, or successive logins from impossibly distant geographical locations may indicate a potential account breach or malicious access attempt. Login will be blocked until user identity can be verified and password reset.

Leaked user credentials: Accounts that have their username and password leaked to the internet will be disabled until user identity can be verified and password reset.

Insufficient access controls detected: Any protected assets where access restrictions do not meet security requirements will have access blocked until the resource is brought into compliance.

# Toolchain

The following cloud provider specific tools will be implemented to automate the policy statements in this document. For additional examples of relevant tooling specific to Azure, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/identity-baseline/toolchain).

## Azure Specific Tooling

Cloud-based authentication and access control: [Microsoft Entra ID](https://learn.microsoft.com/entra/fundamentals/whatis)

Directory synchronization between on-premises and cloud: [Microsoft Entra Cloud Sync](https://learn.microsoft.com/entra/identity/hybrid/connect/whatis-azure-ad-connect-v2)

Cloud hosted support for directory services and legacy authentication: [Active Directory Domain Services](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview)

Federated authentication between trusted directories: [Microsoft Entra Connect and federation](https://learn.microsoft.com/entra/identity/hybrid/connect/how-to-connect-fed-whatis)

## Tooling for other Cloud Providers

List similar tools for other cloud providers, as needed.