


# Identity Baseline metrics, indicators, and risk tolerance

02/11/2019 • 4 minutes to read • Contributors 

## In this article

[Metrics](#)

[Risk tolerance indicators](#)

[Next steps](#)

This article is intended to help you quantify business risk tolerance as it relates to Identity Baseline. Defining metrics and indicators helps you create a business case for making an investment in maturing the Identity Baseline discipline.

## Metrics

Identity Baseline focuses on identifying, authenticating, and authorizing individuals, groups of users, or automated processes, and providing them appropriate access to resources in your cloud deployments. As part of your risk analysis you'll want to gather data related to your identity services to determine how much risk you face, and how important investment in Identity Baseline governance is to your planned cloud deployments.

The following are examples of useful metrics that you should gather to help evaluate risk tolerance within the Identity Baseline discipline:

- **Identity systems size.** Total number of users, groups, or other objects managed through your identity systems.
- **Overall size of directory services infrastructure.** Number of directory forests, domains, and tenants used by your organization.
- **Dependency on legacy or on-premises authentication mechanisms.** Number of workloads that depend on legacy authentication mechanisms or third-party multi-factor authentication services.
- **Extent of cloud-deployed directory services.** Number of directory forests, domains, and tenants you've deployed to the cloud.
- **Cloud-deployed Active Directory servers.** Number of Active Directory servers deployed to the cloud.
- **Cloud-deployed organizational units.** Number of Active Directory organizational units (OUs) deployed to the cloud.
- **Extent of federation.** Number of Identity Baseline systems federated with your organization's systems.
- **Elevated users.** Number of user accounts with elevated access to resources or management tools.
- **Use of role-based access control.** Number of subscriptions, resource groups, or individual resources not managed through role-based access control (RBAC).
- **Authentication claims.** Number of successful and failed user authentication attempts.
- **Authorization claims.** Number of successful and failed attempts by users to access resources.
- **Compromised accounts.** Number of user accounts that have been compromised.

## Risk tolerance indicators

Risks related to Identity Baseline are largely related to the complexity of your organization's identity infrastructure. If all your users and groups are managed using a single directory or cloud-native identity provider using minimal integration with other services, your risk level will likely be small. However, as your business needs grow your Identity Baseline systems may need to support more complicated scenarios, such as multiple directories to support your internal organization or federation with external identity providers. As these systems become more complex, risk increases.

In the early stages of cloud adoption, work with your IT security team and business stakeholders to identify [business risks](#) related to identity, then determine an acceptable baseline for identity risk tolerance. This section of the Cloud Adoption Framework provides examples, but the detailed risks and baselines for your company or deployments may be different.

Once you have a baseline, establish minimum benchmarks representing an unacceptable increase in your identified risks. These benchmarks act as triggers for when you need to take action to address these risks. The following are a few examples of how identity related metrics, such as those discussed above, can justify an increased investment in the Identity Baseline discipline.

- **User account number trigger.** A company with more than  $x$  users, groups, or other objects managed in your identity systems could benefit from investment in the Identity Baseline discipline to ensure efficient governance over a large number of accounts.
- **On-premises identity dependency trigger.** A company planning to migrate workloads to the cloud that require legacy authentication capabilities or third-party multi-factor authentication should invest in the Identity Baseline discipline to reduce risks related to refactoring or additional cloud infrastructure deployment.
- **Directory services complexity trigger.** A company maintaining more than  $x$  number of individual forests, domains, or directory tenants should invest in the Identity Baseline discipline to reduce risks related with account management and the efficiency issues related to multiple user credentials spread across multiple systems.
- **Cloud-hosted directory services trigger.** A company hosting  $x$  Active Directory server virtual machines (VMs) hosted in the cloud, or having  $x$  organizational units (OUs) managed on these cloud-based servers, can benefit from investment in the Identity Baseline discipline to optimize integration with any on-premises or other external identity services.
- **Federation trigger.** A company implementing identity federation with  $x$  external Identity Baseline systems can benefit from investing in the Identity Baseline discipline to ensure consistent organizational policy across federation members.
- **Elevated access trigger.** A company with more than  $x\%$  of users with elevated permissions to management tools and resources should consider investing in the Identity Baseline discipline to minimize the risk of inadvertent overprovisioning of access to users.
- **RBAC trigger.** A company with under  $x\%$  of resources using role-based access control methods should consider investing in the Identity Baseline discipline to identify optimized ways to assign user access to resources.
- **Authentication failure trigger.** A company where authentication failures represent more than  $x\%$  of attempts should invest in the Identity Baseline discipline to ensure that authentication methods are not under external attack, and that users are able to use the authentication methods correctly.
- **Authorization failure trigger.** A company where access attempts are rejected more than  $x\%$  of the time should invest in the Identity Baseline discipline to improve the application and updating of access controls, and identify potentially malicious access attempts.
- **Compromised account trigger.** A company with more than  $x$  compromised accounts should invest in the Identity Baseline discipline to improve the strength and security of authentication mechanisms and improve mechanisms to remediate risks related to compromised accounts.

The exact metrics and triggers you use to gauge risk tolerance and the level of investment in the Identity Baseline discipline will be specific to your organization, but the examples above should serve as a useful base for discussion within your Cloud Governance team.

## Next steps

Using the [Cloud Management template](#), document metrics and tolerance indicators that align to the current cloud adoption plan.

Building on risks and tolerance, establish a process for governing and communicating Identity Baseline policy adherence.

Establish policy adherence processes

