# Identity Baseline discipline improvement

02/11/2019 • 5 minutes to read • Contributors

**In this article**



The Identity Baseline discipline focuses on ways of establishing policies that ensure consistency and continuity of user identities regardless of the cloud provider that hosts the application or workload. Within the Five Disciplines of Cloud Governance, Identity Baseline includes decisions regarding the Hybrid Identity Strategy, evaluation and extension of identity repositories, implementation of single sign-on (same sign-on), auditing and monitoring for unauthorized use or malicious actors. In some cases, it may also involve decisions to modernize, consolidate, or integrate multiple identity providers.

This article outlines some potential tasks your company can engage in to better develop and mature the Identity Baseline discipline. These tasks can be broken down into planning, building, adopting, and operating phases of implementing a cloud solution, which are then iterated on allowing the development of an incremental approach to cloud governance.

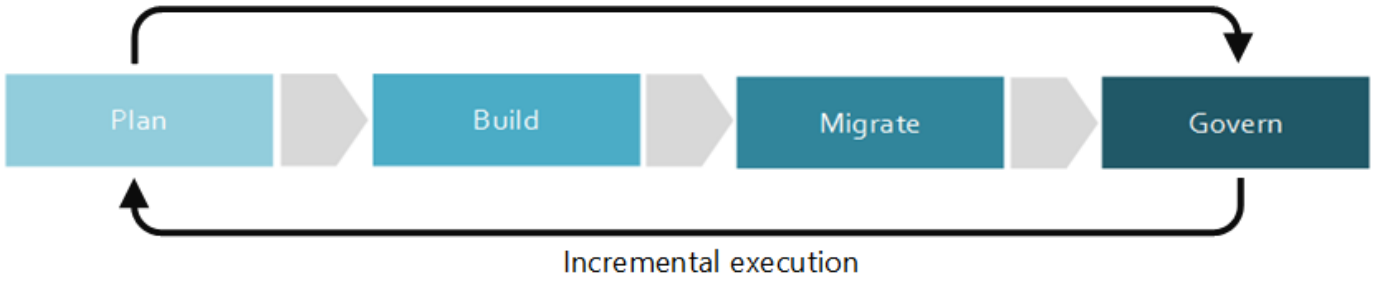


*Figure 1. Adoption phases of the incremental approach to cloud governance.*

It's impossible for any one document to account for the requirements of all businesses. As such, this article outlines suggested minimum and potential example activities for each phase of the governance maturation process. The initial objective of these activities is to help you build a Policy MVP and establish a framework for incremental policy evolution. Your Cloud Governance team will need to decide how much to invest in these activities to improve your Identity Baseline governance capabilities.

> **⊗ Caution**
>
> Neither the minimum or potential activities outlined in this article are aligned to specific corporate policies or third-party compliance requirements. This guidance is designed to help facilitate the conversations that will lead to alignment of both requirements with a cloud governance model.

## Planning and readiness

This phase of governance maturity bridges the divide between business outcomes and actionable strategies. During this process, the leadership team defines specific metrics, maps those metrics to the digital estate, and begins planning

the overall migration effort.

**Minimum suggested activities:**

- Evaluate your Identity toolchain options and implement a hybrid strategy that is appropriate to your organization.
- Develop a draft Architecture Guidelines document and distribute to key stakeholders.
- Educate and involve the people and teams affected by the development of architecture guidelines.

**Potential activities:**

- Define roles and assignments that will govern identity and access management in the cloud.
- Define your on-premises groups and map to corresponding cloud-based roles.
- Inventory identity providers (including database-driven identities used by custom applications).
- Consider options for consolidation or integration of identity providers where duplication exists, to simplify the overall identity solution.
- Evaluate hybrid compatibility of existing identity providers.
- For identity providers that are not hybrid compatible, evaluate consolidation or replacement options.

# Build and predeployment

Several technical and nontechnical prerequisites are required to successfully migrate an environment. This process focuses on the decisions, readiness, and core infrastructure that proceeds a migration.

**Minimum suggested activities:**

- Consider a pilot test before implementing your Identity toolchain, making sure it simplifies the user experience as much as possible.
- Apply feedback from pilot tests into the predeployment. Repeat until results are acceptable.
- Update the Architecture Guidelines document to include deployment and user adoption plans, and distribute to key stakeholders.
- Consider establishing an early adopter program and rolling out to a limited number of users.
- Continue to educate the people and teams most affected by the architecture guidelines.

**Potential activities:**

- Evaluate your logical and physical architecture and determine a Hybrid Identity Strategy.
- Map identity access management policies, such as login ID assignments, and choose the appropriate authentication method for Azure AD.
  - If federated, enable tenant restrictions for administrative accounts.
- Integrate your on-premises and cloud directories.
- Consider using the following access models:
  - Least-privilege access model.
  - Privileged Identity Baseline access model.
- Finalize all preintegration details and review Identity Best Practices.
  - Enable single identity, single sign-on (SSO), or seamless SSO.
  - Configure multi-factor authentication for administrators.
  - Consolidate or integrate identity providers, where necessary.
  - Implement tooling necessary to centralize management of identities.
  - Enable just-in-time (JIT) access and role change alerting.
  - Conduct a risk analysis of key admin activities for assigning to built-in roles.
  - Consider an updated rollout of stronger authentication for all users.
  - Enable Privileged Identity Baseline (PIM) for JIT (using time-limited activation) for additional administrative roles.
  - Separate user accounts from global admin accounts (to make sure that administrators do not inadvertently open emails or run programs associated with their global admin accounts).

# Adopt and migrate

Migration is an incremental process that focuses on the movement, testing, and adoption of applications or workloads in an existing digital estate.

**Minimum suggested activities:**

- Migrate your Identity toolchain from development to production.
- Update the Architecture Guidelines document and distribute to key stakeholders.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive user adoption.

**Potential activities:**

- Validate that the best practices defined during the build predeployment phases are properly executed.
- Validate and refine your Hybrid Identity Strategy.
- Ensure that each application or workload continues to align with the identity strategy before release.
- Validate that single sign-on (SSO) and seamless SSO is working as expected for your applications.
- Reduce or eliminate the number of alternative identity stores, when possible.
- Scrutinize the need for any in-app or in-database identity stores. Identities that fall outside of a proper identity provider (first-party or third-party) can represent risk to the application and the users.
- Enable conditional access for on-premises federated applications.
- Distribute identity across global regions in multiple hubs with synchronization between regions.
- Establish central role-based access control (RBAC) federation.

# Operate and post-implementation

Once the transformation is complete, governance and operations must live on for the natural lifecycle of an application or workload. This phase of governance maturity focuses on the activities that commonly come after the solution is implemented and the transformation cycle begins to stabilize.

**Minimum suggested activities:**

- Customize your Identity Baseline toolchain based on changes to your organization's changing identity needs.
- Automate notifications and reports to alert you of potential malicious threats.
- Monitor and report on system usage and user adoption progress.
- Report on post-deployment metrics and distribute to stakeholders.
- Refine the Architecture Guidelines to guide future adoption processes.
- Communicate and continually educate the affected teams on a periodic basis to ensure ongoing adherence to architecture guidelines.

**Potential activities:**

- Conduct periodic audits of identity policies and adherence practices.
- Scan for malicious actors and data breaches regularly, particularly those related to identity fraud, such as potential admin account takeovers.
- Configure a monitoring and reporting tool.
- Consider integrating more closely with security and fraud-prevention systems.
- Regularly review access rights for elevated users or roles.
  - Identify every user who is eligible to activate admin privilege.
- Review on-boarding, off-boarding, and credential update processes.
- Investigate increasing levels of automation and communication between identity access management (IAM) modules.
- Consider implementing a development security operations (DevSecOps) approach.
- Carry out an impact analysis to gauge results on costs, security, and user adoption.

- Periodically produce an impact report that shows the changes in metrics created by the system and estimate the business impacts of the Hybrid Identity Strategy.
- Establish integrated monitoring recommended by the Azure Security Center.

## Next steps

Now that you understand the concept of cloud identity governance, examine the Identity Baseline toolchain to identify Azure tools and features that you'll need when developing the Identity Baseline governance discipline on the Azure platform.

Identity Baseline toolchain for Azure