


Identity Baseline policy compliance processes

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

In this article

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

[Ongoing monitoring processes](#)

[Violation triggers and enforcement actions](#)

[Next steps](#)

This article discusses an approach to policy adherence processes that govern [Identity Baseline](#). Effective governance of identity starts with recurring manual processes that guide identity policy adoption and revisions. This requires regular involvement of the Cloud Governance team and interested business and IT stakeholders to review and update policy and ensure policy compliance. In addition, many ongoing monitoring and enforcement processes can be automated or supplemented with tooling to reduce the overhead of governance and allow for faster response to policy deviation.

Planning, review, and reporting processes

Identity management tools offer capabilities and features that greatly assist user management and access control within a cloud deployment. However, they also require well thought out processes and policies to support your organization's goals. The following is a set of example processes commonly involved in the Identity Baseline discipline. Use these examples as a starting point when planning the processes that will allow you to continue to update identity policy based on business change and feedback from the IT teams tasked with turning governance guidance into action.

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

Deployment planning: Before any deployment, review the access needs for any workloads and develop an access control strategy that aligns with established corporate identity policy. Document any gaps between 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, perform a high-level review of identity management strategy. Explore planned changes to the identity services environment and updated cloud adoption strategies to identify potential risk increase or need to modify current identity infrastructure patterns. Also use this time to review the latest identity management best practices and integrate these into your policies and review processes.

Quarterly planning: On a quarterly basis perform a general review of identity and access control audit data, and meet with the 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.

This planning process is also a good time to evaluate the current membership of your Cloud Governance team for knowledge gaps related to new or evolving policy and risks related to identity. Invite relevant IT staff to participate in reviews and planning as either temporary technical advisors or permanent members of your team.

Education and training: On a bimonthly basis, 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 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: On a monthly basis, perform an audit on all cloud deployments to assure their continued alignment with identity policy. Use this review to 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. Identify any privileged accounts and document their purpose. This review process produces 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 processes

Determining if your identity governance strategy is successful depends on visibility into the current and past state of your identity systems. Without the ability to analyze your cloud deployment's relevant metrics and related data, you cannot identify changes in your risks or detect violations of your risk tolerances. The ongoing governance processes discussed above require quality data to ensure policy can be modified to support the changing needs of your business.

Ensure that your IT teams have implemented automated monitoring systems for your identity services that capture the logs and audit information you need to evaluate risk. Be proactive in monitoring these systems to ensure prompt detection and mitigation of potential policy violation, and ensure any changes to your identity infrastructure are reflected in your monitoring strategy.

Violation triggers and enforcement actions

Violations of identity policy can result in unauthorized access to sensitive data and lead to serious disruption of mission-critical application and services. When violations are detected, you should take actions to realign with policy as soon as possible. Your IT team can automate most violation triggers using the tools outlined in the [Identity Baseline toolchain](#).

The following triggers and enforcement actions provide examples you can reference when planning how to use monitoring data to resolve policy violations:

- 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.

Next steps

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

For guidance on executing cloud management policies in alignment with adoption plans, see the article on discipline improvement.

Identity Baseline discipline improvement