


# Large enterprise: Identity Baseline evolution

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

## In this article

[Evolution of the narrative](#)

[Evolution of tangible risks](#)

[Evolution of the policy statements](#)

[Evolution of the best practices](#)

[Conclusion](#)

[Next steps](#)

This article evolves the narrative by adding Identity Baseline controls to the governance MVP.

## Evolution of the narrative

The business justification for the cloud migration of the two datacenters was approved by the CFO. During the technical feasibility study, several roadblocks were discovered:

- Protected data and mission-critical applications represent 25% of the workloads in the two datacenters. Neither can be eliminated until the current governance policies regarding PII and mission-critical applications have been modernized.
- 7% of the assets in those datacenters are not cloud-compatible. They will be moved to an alternate datacenter before termination of the datacenter contract.
- 15% of the assets in the datacenter (750 virtual machines) have a dependency on legacy authentication or third-party multi-factor authentication.
- The VPN connection that connects existing datacenters and Azure does not offer sufficient data transmission speeds or latency to migrate the volume of assets within the two-year timeline to retire the datacenter.

The first two roadblocks are being managed in parallel. This article will address the resolution of the third and fourth roadblocks.

## Evolution of the Cloud Governance team

The Cloud Governance team is expanding. Given the need for additional support regarding identity management, a systems administrator from the Identity Baseline team now participates in a weekly meeting to keep the existing team members aware of changes.

## Evolution of the current state

The IT team has approval to move forward with the CIO and CFO's plans to retire two datacenters. However, IT is concerned that 750 (15%) of the assets in those datacenters will have to be moved somewhere other than the cloud.

## Evolution of the future state

The new future state plans require a more robust Identity Baseline solution to migrate the 750 virtual machines with legacy authentication requirements. Beyond these two datacenters, similar percentages of assets in other datacenters are expected to be affected by this challenge. The future state now also requires a connection from the cloud provider to the company's MPLS/leased-line solution.

The changes to current and future state expose new risks that will require new policy statements.

# Evolution of tangible risks

**Business interruption during migration.** Migration to the cloud creates a controlled, time-bound risk that can be managed. Moving aging hardware to another part of the world is much higher risk. A mitigation strategy is needed to avoid interruptions to business operations.

**Existing identity dependencies.** Dependencies on existing authentication and identity services may delay or prevent the migration of some workloads to the cloud. Failure to return the two datacenters on time will incur millions of dollars in datacenter lease fees.

This business risk can be expanded into a few technical risks:

- Legacy authentication might not be available in the cloud, limiting deployment of some applications.
- The current third-party multi-factor authentication solution might not be available in the cloud, limiting deployment of some applications.
- Retooling or moving either could create outages and add costs.
- The speed and stability of the VPN might impede migration.
- Traffic entering the cloud could cause security issues in other parts of the global network.

## Evolution of the policy statements

The following changes to policy will help remediate the new risks and guide implementation.

1. The chosen cloud provider must offer a means of authenticating via legacy methods.
2. The chosen cloud provider must offer a means of authentication with the current third-party multi-factor authentication solution.
3. A high-speed private connection should be established between the cloud provider and the company's telco provider, connecting the cloud provider to the global network of datacenters.
4. Until sufficient security requirements are established, no inbound public traffic may access company assets hosted in the cloud. All ports are blocked from any source outside of the global WAN.

## Evolution of the best practices

The governance MVP design evolves to include new Azure policies and an implementation of Active Directory on a virtual machine. Together, these two design changes fulfill the new corporate policy statements.

Here are the new best practices:

1. DMZ blueprint: The on-premises side of the DMZ should be configured to allow communication between the following solution and the on-premises Active Directory servers. This best practice requires a DMZ to enable Active Directory Domain Services across network boundaries.
2. Azure Resource Manager templates:
  - a. Define an NSG to block external traffic and whitelist internal traffic.
  - b. Deploy two Active Directory virtual machines in a load-balanced pair based on a golden image. On first boot, that image runs a PowerShell script to join the domain and register with domain services. For more information, see [Extend Active Directory Domain Services \(AD DS\) to Azure](#).
3. Azure Policy: Apply the NSG to all resources.
4. Azure blueprint:
  - a. Create a blueprint named `active-directory-virtual-machines`.
  - b. Add each of the Active Directory templates and policies to the blueprint.
  - c. Publish the blueprint to any applicable management group.
  - d. Apply the blueprint to any subscription requiring legacy or third-party multi-factor authentication.
  - e. The instance of Active Directory running in Azure can now be used as an extension of the on-premises Active Directory solution, allowing it to integrate with the existing multi-factor authentication tool and provide

claims-based authentication, both through existing Active Directory functionality.

## Conclusion

Adding these changes to the governance MVP helps remediate many of the risks in this article, allowing each cloud adoption team to quickly move past this roadblock.

## Next steps

As cloud adoption evolves and delivers additional business value, risks and cloud governance needs will also evolve. The following are a few evolutions that may occur. For the fictional company in this journey, the next trigger is the inclusion of protected data in the cloud adoption plan. This change will require additional security controls.

Security Baseline evolution