# Small-to-medium enterprise: Security Baseline evolution

02/11/2019 • 8 minutes to read • Contributors

**In this article**

This article evolves the narrative by adding security controls that support moving protected data to the cloud.

## Evolution of the narrative

IT and business leadership have been happy with results from early stage experimentation by the IT, App Development, and BI teams. To realize tangible business values from these experiments, those teams must be allowed to integrate protected data into solutions. This triggers changes to corporate policy, but also requires an evolution of the cloud governance implementations before protected data can land in the cloud.

### Evolution of the Cloud Governance team

Given the effect of the changing narrative and support provided so far, the Cloud Governance team is now viewed differently. The two system administrators who started the team are now viewed as experienced cloud architects. As this narrative develops, the perception of them will shift from being Cloud Custodians to more of a Cloud Guardian role.

While the difference is subtle, it’s an important distinction when building a governance- focused IT culture. A Cloud Custodian cleans up the messes made by innovative cloud architects. The two roles have natural friction and opposing objectives. On the other hand, a Cloud Guardian helps keep the cloud safe, so other cloud architects can move more quickly, with less messes. Additionally, a Cloud Guardian is involved in creating templates that accelerate deployment and adoption, making them an innovation accelerator as well as a defender of the Five Disciplines of Cloud Governance.

### Evolution of the current state

At the start of this narrative, the application development teams were still working in a dev/test capacity, and the BI team was still in the experimental phase. IT operated two hosted infrastructure environments, named Prod and DR.

Since then, some things have changed that will affect governance:

- The application development team has implemented a CI/CD pipeline to deploy a cloud-native application with an improved user experience. That app doesn’t yet interact with protected data, so it is not production ready.
- The Business Intelligence team within IT actively curates data in the cloud from logistics, inventory, and third-party sources. This data is being used to drive new predictions, which could shape business processes. However, those predictions and insights are not actionable until customer and financial data can be integrated into the data platform.

- The IT team is progressing on the CIO and CFO's plans to retire the DR datacenter. More than 1,000 of the 2,000 assets in the DR datacenter have been retired or migrated.
- The loosely defined policies regarding PII and financial data have been modernized. However, the new corporate policies are contingent on the implementation of related security and governance policies. Teams are still stalled.

### Evolution of the future state

Early experiments by the App Dev and BI teams show potential improvements in customer experiences and data-driven decisions. Both teams want to expand adoption of the cloud over the next 18 months by deploying those solutions to production.

During the remaining six months, the Cloud Governance team will implement security and governance requirements to allow the cloud adoption teams to migrate the protected data in those datacenters.

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

## Evolution of tangible risks

**Data breach:** When adopting any new data platform, there is an inherent increase in liabilities related to potential data breaches. Technicians adopting cloud technologies have increased responsibilities to implement solutions that can decrease this risk. A robust security and governance strategy must be implemented to ensure those technicians fulfill those responsibilities.

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

- Mission-critical applications or protected data might be deployed unintentionally.
- Protected data might be exposed during storage due to poor encryption decisions.
- Unauthorized users might access protected data.
- External intrusion might result in access to protected data.
- External intrusion or denial of service attacks might cause a business interruption.
- Organization or employment changes might allow for unauthorized access to protected data.
- New exploits could create new intrusion or access opportunities.
- Inconsistent deployment processes might result in security gaps, which could lead to data leaks or interruptions.
- Configuration drift or missed patches might result in unintended security gaps, which could lead to data leaks or interruptions.

## Evolution of the policy statements

The following changes to policy will help remediate the new risks and guide implementation. The list looks long, but adopting these policies may be easier than it appears.

1. All deployed assets must be categorized by criticality and data classification. Classifications are to be reviewed by the Cloud Governance team and the application owner before deployment to the cloud.
2. Applications that store or access protected data are to be managed differently than those that don’t. At a minimum, they should be segmented to avoid unintended access of protected data.
3. All protected data must be encrypted when at rest.
4. Elevated permissions in any segment containing protected data should be an exception. Any such exceptions will be recorded with the Cloud Governance team and audited regularly.
5. Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets will be audited regularly.
6. No subnet containing protected data can be directly accessed over the public internet or across datacenters. Access to those subnets must be routed through intermediate subnets. All access into those subnets must come through a firewall solution that can perform packet scanning and blocking functions.

7. Governance tooling must audit and enforce network configuration requirements defined by the security management team.
8. Governance tooling must limit VM deployment to approved images only.
9. Whenever possible, node configuration management should apply policy requirements to the configuration of any guest operating system.
10. Governance tooling must enforce that automatic updates are enabled on all deployed assets. Violations must be reviewed with operational management teams and remediated in accordance with operations policies. Assets that are not automatically updated must be included in processes owned by IT Operations.
11. Creation of new subscriptions or management groups for any mission-critical applications or protected data will require a review from the Cloud Governance team, to ensure that the proper blueprint is assigned.
12. A least-privilege access model will be applied to any management group or subscription that contains mission-critical apps or protected data.
13. Trends and exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to security management tooling used in the cloud.
14. Deployment tooling must be approved by the Cloud Governance team to ensure ongoing governance of deployed assets.
15. Deployment scripts must be maintained in a central repository accessible by the Cloud Governance team for periodic review and auditing.
16. Governance processes must include audits at the point of deployment and at regular cycles to ensure consistency across all assets.
17. Deployment of any applications that require customer authentication must use an approved identity provider that is compatible with the primary identity provider for internal users.
18. Cloud governance processes must include quarterly reviews with identity management teams. These reviews can help identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

## Evolution of the best practices

The governance MVP design will evolve to include new Azure policies and an implementation of Azure Cost Management. Together, these two design changes will fulfill the new corporate policy statements.

1. The Networking and IT Security teams will define network requirements. The Cloud Governance team will support the conversation.
2. The Identity and IT Security teams will define identity requirements and make any necessary changes to local Active Directory implementation. The Cloud Governance team will review changes.
3. Create a repository in Azure DevOps to store and version all relevant Azure Resource Manager templates and scripted configurations.
4. Azure Security Center implementation:
   a. Configure Azure Security Center for any management group that contains protected data classifications.
   b. Set automatic provisioning to on by default to ensure patching compliance.
   c. Establish OS security configurations. The IT Security team will define the configuration.
   d. Support the IT Security team in the initial use of Security Center. Transition the use of Security Center to the IT Security team, but maintain access for the purpose of continually improving governance.
   e. Create a Resource Manager template that reflects the changes required for Security Center configuration within a subscription.
5. Update Azure policies for all subscriptions:
   a. Audit and enforce the criticality and data classification across all management groups and subscriptions, to identify any subscriptions with protected data classifications.
   b. Audit and enforce the use of approved images only.
6. Update Azure policies for all subscriptions that contains protected data classifications:
   a. Audit and enforce the use of standard Azure RBAC roles only.
   b. Audit and enforce encryption for all storage accounts and files at rest on individual nodes.
   c. Audit and enforce the application of an NSG to all NICs and subnets. The Networking and IT Security teams will define the NSG.

    d. Audit and enforce the use of approved network subnet and vNet per network interface.
    e. Audit and enforce the limitation of user-defined routing tables.
    f. Apply the Built-in Policies for Guest Configuration as follows:
        i. Audit that Windows web servers are using secure communication protocols.
        ii. Audit that password security settings are set correctly inside Linux and Windows machines.

7. Firewall configuration:
    a. Identify a configuration of Azure Firewall that meets necessary security requirements. Alternatively, identify a compatible third-party appliance that is compatible with Azure.
    b. Create a Resource Manager template to deploy the firewall with required configurations.
8. Azure blueprint:
    a. Create a new blueprint named `protected-data`.
    b. Add the firewall and Azure Security Center templates to the blueprint.
    c. Add the new policies for protected data subscriptions.
    d. Publish the blueprint to any management group that currently plans on hosting protected data.
    e. Apply the new blueprint to each affected subscription, in addition to existing blueprints.

## Conclusion

Adding the above processes and changes to the governance MVP will help to remediate many of the risks associated with security governance. Together, they add the network, identity, and security monitoring tools needed to protect data.

## Next Steps

As cloud adoption continues to evolve and deliver additional business value, risks and cloud governance needs also evolve. For the fictional company in this journey, the next step is to support mission-critical workloads. This is the point when Resource Consistency controls are needed.

Resource Consistency evolution