


# Security Baseline discipline improvement

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

## In this article

[Planning and readiness](#)

[Build and predeployment](#)

[Adopt and migrate](#)

[Operate and post-implementation](#)

[Next steps](#)

The Security Baseline discipline focuses on ways of establishing policies that protect the network, assets, and most importantly the data that will reside on a cloud provider's solution. Within the Five Disciplines of Cloud Governance, Security Baseline includes classification of the digital estate and data. It also includes documentation of risks, business tolerance, and mitigation strategies associated with the security of the data, assets, and network. From a technical perspective, this also includes involvement in decisions regarding [encryption](#), [network requirements](#), [hybrid identity strategies](#), and the [processes](#) used to develop cloud Security Baseline policies.

This article outlines some potential tasks your company can engage in to better develop and mature the Security 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](#).

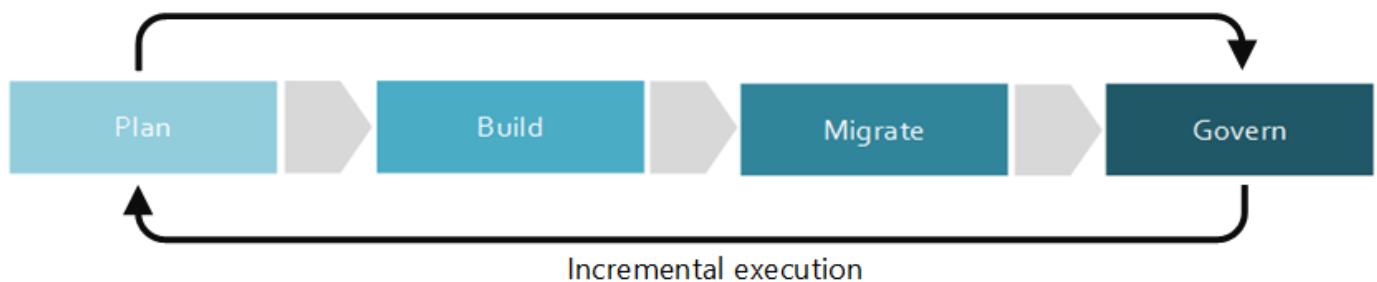


Figure 1. Adoption phases of the incremental approach to cloud governance.

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 Security 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 [Security Baseline toolchain](#) options.
- 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.
- Add prioritized security tasks to your migration backlog.

#### Potential activities:

- Define a data classification schema.
- Conduct a digital estate planning process to inventory the current IT assets powering your business processes and supporting operations.
- Conduct a [policy review](#) to begin the process of modernizing existing corporate IT security policies, and define MVP policies addressing known risks.
- Review your cloud platform's security guidelines. For Azure these can be found in the [Microsoft Service Trust Platform](#).
- Determine whether your Security Baseline policy includes a [Security Development Lifecycle](#).
- Evaluate network, data, and asset-related business risks based on the next one to three releases, and gauge your organization's tolerance for those risks.
- Review Microsoft's [top trends in cybersecurity](#) report to get an overview of the current security landscape.
- Consider developing a [Security DevOps](#) role in your organization.

## 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:

- Implement your [Security Baseline toolchain](#) by rolling out in a predeployment phase.
- Update the Architecture Guidelines document and distribute to key stakeholders.
- Implement security tasks on your prioritized migration backlog.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive user adoption.

#### Potential activities:

- Determine your organization's [encryption](#) strategy for cloud-hosted data.
- Evaluate your cloud deployment's [identity](#) strategy. Determine how your cloud-based identity solution will coexist or integrate with on-premises identity providers.
- Determine network boundary policies for your [Software Defined Networking \(SDN\)](#) design to ensure secure virtualized networking capabilities.
- Evaluate your organization's [least-privilege access](#) policies, and use task-based roles to provide access to specific resources.
- Apply security and monitoring mechanisms to for all cloud services and virtual machines.
- Automate [security policies](#) where possible.
- Review your Security Baseline policy and determine if you need to modify your plans according to best practices guidance such as those outlined in the [Security Development Lifecycle](#).

## 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 [Security Baseline toolchain](#) from predeployment 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:

- Review the latest Security Baseline and threat information to identify any new business risks.
- Gauge your organization's tolerance to handle new security risks that may arise.
- Identify deviations from policy, and enforce corrections.
- Adjust security and access control automation to ensure maximum policy compliance.
- Validate that the best practices defined during the build and predeployment phases are properly executed.
- Review your least-privilege access policies and adjust access controls to maximize security.
- Test your Security Baseline toolchain against your workloads to identify and resolve any vulnerabilities.

## 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:

- Validate and refine your [Security Baseline toolchain](#).
- Customize notifications and reports to alert you of potential security issues.
- Refine the Architecture Guidelines to guide future adoption processes.
- Communicate and educate the affected teams periodically to ensure ongoing adherence to architecture guidelines.

#### Potential activities:

- Discover patterns and behavior for your workloads and configure your monitoring and reporting tools to identify and notify you of any abnormal activity, access, or resource usage.
- Continuously update your monitoring and reporting policies to detect the latest vulnerabilities, exploits, and attacks.
- Have procedures in place to quickly stop unauthorized access and disable resources that may have been compromised by an attacker.
- Regularly review the latest security best practices and apply recommendations to your security policy, automation, and monitoring capabilities where possible.

## Next steps

Now that you understand the concept of cloud security governance, move on to learn more about [what security and best practices guidance Microsoft provides](#) for Azure.

[Learn about security guidance for Azure](#)

[Introduction to Azure security](#)

[Learn about logging, reporting, and monitoring](#)