# How to use this template

This sample template is designed to help you define the policy statements and design guidance that allow you to mature the [Five Disciplines of Cloud Governance](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/governance-disciplines) within your organization. The examples in this template are focused on the [Security Baseline](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/security-baseline/overview) discipline. Use these examples as a starting point for discussions within your organization around this discipline.

The following instructions will guide usage of this template:

* Update the template's title page with your author information, publish date and the governance discipline this document supports.
* Update this template to reflect risks, tolerance, indictors, toolchains, etc., that align to your business and technology needs.
* Update this template to reflect your policy statements.
* Update this template's executive summary to reflect your updated content.
* Before publication remove the “sample” watermark.
* Delete this page and update the table of contents before publishing your customized policy statements.

**Microsoft Cloud Adoption Framework for Azure**

**Cloud Governance**

Security Baseline Discipline

Policy Statements and Design Guidance

The document outlines the policy statements and design guidance required to support the Security Baseline governance discipline during cloud adoption. Associated risks, tolerance, and remediation strategies are included for reference.

**Author(s):** <Update Author>

**Date Published:** 03/3/2019

Contents

[How to use this template 1](#_Toc2782588)

[Executive Summary 3](#_Toc2782589)

[Policy Statements 3](#_Toc2782590)

[Business Risks 4](#_Toc2782591)

[Metrics and Indicators 4](#_Toc2782592)

[Metrics 4](#_Toc2782593)

[Indicators 4](#_Toc2782594)

[Policy compliance processes 5](#_Toc2782595)

[Planning, review, and reporting processes 5](#_Toc2782596)

[Ongoing monitoring 6](#_Toc2782597)

[Violation Triggers and Enforcement Actions 6](#_Toc2782598)

[Toolchain 7](#_Toc2782599)

[Azure Specific Tooling 7](#_Toc2782600)

[Tooling for other Cloud Providers 7](#_Toc2782601)

# Executive Summary

Cloud deployments face many of the same security risks as workloads hosted in traditional on-premises datacenters. However, one of the primary things that set cloud security governance apart from traditional security policy is the ease with which resources can be created, potentially adding vulnerabilities if security isn't considered before deployment. This document identifies and determines the business’s tolerance for risks, and outlines efforts to remediate these risks. The result is a series of policy statements that should guide the architecture of any solutions deployed to the cloud.

This policies and guidance in this document has been developed in conjunction with the governance best practices documented in the [Microsoft Cloud Adoption Framework for Azure (CAF)](http://aka.ms/caf).

# Policy Statements

The following statements should guide cloud adoption architecture decisions to ensure compliance with governance efforts related to the Security Baseline discipline. For additional examples of relevant policy statements, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/security-baseline/policy-statements).

**Asset classification**: All deployed assets must be categorized by criticality and data classification. Classifications must be reviewed by the Cloud Governance team and the application owner before deployment to the cloud.

**Network isolation**: Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.

**Secure on-premises connectivity**: All connections between the on-premises and cloud networks must take place either through a secure encrypted VPN connection or a dedicated private WAN link.

# Business Risks

The following security related business risks have been identified as concerns based on the current plans for cloud adoption. For additional examples of relevant business risks, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/security-baseline/business-risks).

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Description | Indicators | Resolution |
| Data breach | Inadvertent exposure or loss of sensitive cloud-hosted data can lead to losing customers, contractual issues, or legal consequences. | Current | Policy statements enforced |
| Service disruption | Outages and other performance issues due to insecure infrastructure interrupts normal operations and can result in lost productivity or lost business. | Mission-critical workloads deployed | Policy statements drafted but not enforced |

# Metrics and Indicators

The following are key metrics and indicators that will guide the resolution or mitigation of business risks. For additional examples of relevant metrics or indicators, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/security-baseline/metrics-tolerance).

## Metrics

Current Security Management efforts attempt to govern or improve the following key metrics.

* Data classification: Number of cloud-stored data and services that are unclassified according to on your organization's privacy, compliance, or business impact standards.
* Attack surface: Number total data sources, services, and applications that are cloud-hosted and accessible over the internet.
* Number of unencrypted data stores: Number of sensitive data stores that are not encrypted.
* Overall Standards Compliance: Ratio of compliance adherence to security standards.

## Indicators

The following indicators will trigger changes in policy statements based on changes in metrics and other conditions.

* Current: Current state of metrics. Any policy statements listed as current should be actively enforced.
* Mission-critical workloads trigger: Deploying mission-critical workloads to the cloud will require creation and enforcement of policy statements to remediate risks related to service disruption.
* Protected data trigger: Hosting data on the cloud that can be classified as confidential, private, or otherwise subject to regulatory concerns will require policies in place to prevent the risk of data breach.

# Policy compliance processes

The following section outlines the processes that will ensure cloud deployments remain in compliance with Security Baseline policies. This includes an overview of the planning, review and reporting processes performed by the Cloud Governance team, as well as the ongoing monitoring and enforcement processes that can be automated or supplemented with tooling to allow for faster response to policy deviation.

For additional examples of relevant policy compliance processes, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/security-baseline/compliance-processes).

## Planning, review, and reporting processes

Initial risk assessment and planning: As part of the initial adoption of the Security Baseline discipline, the Cloud Governance team will identify core business risks and tolerances related to cloud security. The team will use this information to begin discussions on specific technical risks with IT and security staff, and to develop a baseline set of security policies as part of developing an initial governance strategy.

Deployment planning: Before deploying any workload or asset, the IT and Cloud Governance teams will perform a security review to identify any new risks and ensure all access and data security policy requirements are met.

Deployment testing: As part of the deployment process for any workload or asset, the Cloud Governance team, in cooperation with corporate security teams, will review the deployment to validate security policy compliance.

Annual planning: On an annual basis, Cloud Governance team will perform a high-level review of security strategy. Future corporate priorities and updated cloud adoption strategies will be explored to identify potential risk increase or other emerging security needs. This process will also involve a review of the latest security best practices and integrate these into policies and review processes.

Quarterly review and planning: On a quarterly basis, the Cloud Governance team will review security audit data and incident reports to identify any changes required in security policy. As part of this process, the current cybersecurity landscape will be explored to proactively anticipate emerging threats and update policy as appropriate. After the review is complete, design guidance will be aligned with updated policy.

This review will also evaluate the Cloud Governance team's current membership for knowledge gaps related to new or evolving policy and risks related to security. The team will invite relevant security and IT staff to participate in reviews and planning as either temporary technical advisors or permanent members of the team.

Education and Training: On a bi-monthly basis, the Cloud Governance team will offer training sessions to ensure IT staff and developers are up-to-date on the latest security policy requirements. As part of this process, the team will review all documentation, guidance, or other training assets and updated to ensure they are in sync with the latest corporate policy statements.

Monthly audit and reporting reviews: On a monthly basis, security and Cloud Governance teams will perform an audit on all cloud deployments to ensure their continued alignment with security policy. Security related activities will be reviewed with IT staff and the team will identify any compliance issues not already handled as part of the ongoing monitoring and enforcement process. This process will result in a report for the Cloud Strategy team and each cloud adoption team to communicate overall adherence to policy. The report is also stored for auditing and legal purposes.

## Ongoing monitoring

Security and IT teams will implement automated monitoring systems for the organization's cloud infrastructure, capturing relevant log data needed to evaluate security related risks. They will also establish reporting and alerting systems to ensure prompt detection and mitigation of potential security policy violations.

## Violation Triggers and Enforcement Actions

Increase in attacks detected: If any resource experiences a 25% increase in brute force or DDoS attacks, discuss with IT security staff and workload owner to determine remedies. Track issue and update guidance if policy revision is necessary to prevent future incidents.

Unclassified data detected: Any data source without an appropriate privacy, security, or business impact classification will have external access denied until the classification is applied by the data owner and the appropriate level of data protection applied.

Network vulnerability detected: Access to any resource not explicitly allowed by the network access policies should trigger an alert to IT security staff and the relevant workload owner. Track issue and update guidance if policy revision is necessary to mitigate future incidents.

# Toolchain

The following cloud provider specific tools will be implemented to automate the policy statements in this document. For additional examples of relevant tooling specific to Azure, see the [governance theory section of CAF](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/security-baseline/toolchain).

## Azure Specific Tooling

Apply access controls to resources and resource creation: [Azure Active Directory](https://review.docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis)

Secure virtual networks: [Azure Resource Manager](https://review.docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview)

Detect malicious activity: [Azure Monitor](https://review.docs.microsoft.com/en-us/azure/azure-monitor/overview)

Preemptively detect vulnerabilities: [Azure Security Center](https://review.docs.microsoft.com/en-us/azure/security-center/security-center-intro)

## Tooling for other Cloud Providers

List similar tools for other cloud providers, as needed.