# 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 [Deployment Acceleration](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/deployment-acceleration/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**

Deployment Acceleration Discipline

Policy Statements and Design Guidance

The document outlines the policy statements, design guidance, and processes required to support the Deployment Acceleration 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](#_Toc2791857)

[Executive Summary 3](#_Toc2791858)

[Policy Statements 3](#_Toc2791859)

[Business Risks 4](#_Toc2791860)

[Metrics and Indicators 4](#_Toc2791861)

[Metrics 4](#_Toc2791862)

[Indicators 5](#_Toc2791863)

[Policy compliance processes 6](#_Toc2791864)

[Planning, review, and reporting processes 6](#_Toc2791865)

[Ongoing monitoring 7](#_Toc2791866)

[Violation Triggers and Enforcement Actions 7](#_Toc2791867)

[Toolchain 8](#_Toc2791868)

[Azure Specific Tooling 8](#_Toc2791869)

[Tooling for other Cloud Providers 8](#_Toc2791870)

# Executive Summary

As cloud adoption grows, the scaling, failover, and disaster recovery capabilities that cloud provides can best be taken advantage of using standards and automation. Adopting a DevOps or DevSecOps approach is often the best way to manage deployments. The Deployment Acceleration discipline is focused on supporting these approaches by stablishing policies to govern asset configuration or deployment. This document identifies and determines the business’s tolerance for risks related to Deployment Acceleration, 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 Deployment Acceleration 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/deployment-acceleration/policy-statements).

**Lack of visibility into system issues**: Key metrics and diagnostics measures will be identified for all production systems and components. Monitoring and diagnostic tools will be applied to these systems and monitored regularly by operations personnel.

**Reliance on manual deployment or configuration of systems**: All assets deployed to the cloud should be deployed using templates or automation scripts whenever possible.

**Configuration security reviews**: Cloud Governance processes must include quarterly review with configuration management teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

# Business Risks

The following Deployment Acceleration 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/deployment-acceleration/business-risks).

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Description | Indicators | Resolution |
| Service disruption | Lack of predictable repeatable deployment processes or unmanaged changes to system configurations can disrupt normal operations and can result in lost productivity or lost business. | Current | Policy Statements enforced |
| Cost overruns | Unexpected changes in configuration of system resources can make identifying root cause of issues more difficult, raising the costs of development, operations, and maintenance. | Configuration drift | Policy statements drafted but not enforced |
| Organizational inefficiencies | Barriers between development, operations, and security teams can cause numerous challenges to effective adoption of cloud technologies and the development of a unified cloud governance model. | Project schedule / Out of compliance | 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/deployment-acceleration/metrics-tolerance).

## Metrics

This governance discipline attempts to govern and improve the following key metrics.

* Service level agreements (SLA). This can include both Microsoft’s commitments for uptime and connectivity of Azure services, as well as commitments made by the business to its external and internal customers.
* Time to deployment. The amount of time needed to deploy updates to an existing system.
* Assets out-of-compliance. The number or percentage of resources that are out of compliance with defined policies.

## 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.
* Service-level agreement (SLA): A company that cannot meet its SLAs to its external customers or internal partners should invest in the Deployment Acceleration discipline to reduce system downtime.
* Configuration drift: A company that is experiencing unexpected changes in the configuration of key system components, or failures in the deployment of or updates to its systems, should invest in the Deployment Acceleration discipline to identify root causes and steps for remediation.
* Out of compliance: If the number of out-of-compliance resources exceeds a defined threshold (either as a total number of resources or a percentage of total resources), a company should invest in Deployment Acceleration discipline improvements to ensure each resource's configuration remains in compliance throughout that resource's lifecycle.
* Project schedule: If the time to deploy a company's resources and applications often exceed a define threshold, a company should invest in its Deployment Acceleration processes to introduce or improve automated deployments for consistency and predictability. Deployment times measured in days or even weeks usually indicate a suboptimal Deployment Acceleration strategy.

# Policy compliance processes

The following section outlines the processes that will ensure cloud deployments remain in compliance with Deployment Acceleration 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/deployment-acceleration/compliance-processes).

## Planning, review, and reporting processes

Initial risk assessment and planning: As part of the initial adoption of the Deployment Acceleration discipline, the Cloud Governance team will identify core business risks and tolerances related to the deployment of business applications. The team will use this information to discuss specific technical risks with IT Operations staff, and develop a baseline set of deployment and configuration policies for mitigating these risks to establish an initial governance strategy.

Deployment planning: Before deploying any asset, the Cloud Governance team will perform a security and operations review to identify any new risks and ensure all deployment related policy requirements are met.

Deployment testing: As part of the deployment process for any asset, the Cloud Governance team, in cooperation with development teams, is responsible for reviewing a deployment's policy compliance.

Annual planning: The Cloud Governance team will conduct an annual high-level review of Deployment Acceleration strategy. This review will explore future corporate priorities and updated cloud adoption strategies to identify potential risk increase and other emerging configuration needs and opportunities. The team will also use this time to review the latest Deployment Acceleration best practices and integrate these into policies and review processes.

Quarterly review and planning: The Cloud Governance team will conduct a quarterly review of operational audit data and incident reports to identify any changes required in Deployment Acceleration policy. As part of this process, the team will review current DevOps best practices, and update policy as appropriate. After the review is complete, the team will align application and systems design guidance 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 DevOps and Deployment Acceleration. The team will invite relevant 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 make sure IT staff and developers are up-to-date on the latest Deployment Acceleration strategy and requirements. As part of this process the team will 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: The Cloud Governance team will perform a monthly audit on all cloud deployments to assure their continued alignment with configuration policy. As part of this process the team will review deployment-related activities with IT staff and identify any compliance issues not already handled as part of the ongoing monitoring and enforcement process. The result of this review is 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

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

## Violation Triggers and Enforcement Actions

Unexpected changes in configuration detected: If the configuration of a resource changes unexpectedly, work with IT staff and workload owners to identify root cause and develop a remediation plan.

Configuration of new resources does not adhere to policy: Work with DevOps teams and workload owners to review Deployment Acceleration policies during project startup so everyone involved understands the relevant policy requirements.

Deployment failures or configuration issues cause delays in project schedules: Work with development teams and workload owners to ensure the team understands how to automate the deployment of cloud-based resources for consistency and repeatability. Fully automated deployments should be required early in the development cycle — trying to accomplish this late in the development cycle usually leads to unexpected issues and delays.

# 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/deployment-acceleration/toolchain).

## Azure Specific Tooling

Implement Corporate Policies: [Azure Policy](https://docs.microsoft.com/en-us/azure/governance/policy/overview)

Apply Policies across subscriptions: [Azure Management Groups](https://docs.microsoft.com/en-us/azure/governance/management-groups/)

Create fully compliant environments: [Azure Blueprints](https://docs.microsoft.com/en-us/azure/governance/blueprints/overview)

Create an automated pipeline to deploy code and configure assets (DevOps): [Azure DevOps](https://docs.microsoft.com/en-us/azure/devops/index?view=azure-devops&viewFallbackFrom=vsts)

## Tooling for other Cloud Providers

List similar tools for other cloud providers, as needed.