# 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 [Resource Consistency](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/resource-consistency/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**

Resource Consistency Discipline

Policy Statements and Design Guidance

The document outlines the policy statements, design guidance, and processes required to support the Resource Consistency 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](#_Toc2787069)

[Executive Summary 3](#_Toc2787070)

[Policy Statements 3](#_Toc2787071)

[Business Risks 4](#_Toc2787072)

[Metrics and Indicators 4](#_Toc2787073)

[Metrics 4](#_Toc2787074)

[Indicators 5](#_Toc2787075)

[Policy compliance processes 6](#_Toc2787076)

[Planning, review, and reporting processes 6](#_Toc2787077)

[Ongoing monitoring 7](#_Toc2787078)

[Violation Triggers and Enforcement Actions 7](#_Toc2787079)

[Toolchain 8](#_Toc2787080)

[Azure Specific Tooling 8](#_Toc2787081)

[Tooling for other Cloud Providers 8](#_Toc2787082)

# Executive Summary

The cloud offers increased agility and flexibility over most traditional on-premises datacenters, but this flexibility can also add potential management drawbacks that can jeopardize the success of your cloud adoption efforts. The Resource Consistency governance discipline is concerned with ensuring resources are deployed, updated, and configured consistently and repeatably, and that service disruptions are minimized and remedied in as little time as possible. This document identifies and determines the business’s tolerance for risks related to Resource Consistency, 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 Resource Consistency 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/resource-consistency/policy-statements).

**Obsolete assets:** Cloud-hosted assets that are no longer actively used must be retired within 3 months.

**Tagging**: Deployed assets should be tagged with the following values: cost, criticality, SLA, and environment. Governance tooling must validate these values against predefined values managed by the governance team.

**Disaster recovery**: All mission-critical applications and protected data must have backup and recovery solutions implemented to minimize business impact of outages or system failures.

**Monitoring**: Governance tooling must validate that the appropriate level of logging data is being collected for all mission-critical applications or protected data.

# Business Risks

The following Resource Consistency 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/resource-consistency/business-risks).

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Description | Indicators | Resolution |
| Unnecessary operational cost | Obsolete or unused resources, or resources that are overprovisioned during times of low demand, add unnecessary operational costs. | Current | Policy Statements enforced |
| Management inefficiencies | Lack of consistent naming and tagging metadata associated with resources can lead to IT staff having difficulty finding resources for management tasks or identifying ownership and accounting information related to assets. This results in management inefficiencies that can increase cost and slow IT responsiveness to service disruption or other operational issues. | 10% of resources lack required tagging metadata | Policy statements drafted but not enforced |
| Business Interruption | Service disruptions that result in violations of your organization's established Service Level Agreements (SLAs) can result in loss of business or other financial impacts to your company. | Mission critical services are experiencing less than 99.9% uptime | 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/resource-consistency/metrics-tolerance).

## Metrics

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

* Cloud assets: Total number of cloud-deployed resources.
* Untagged resources: Number of resources without required accounting, business impact, or organizational tags.
* Underused assets: Number of resources where memory, CPU, or network capabilities are all consistently under-used.
* Resource depletion: Number of resources where memory, CPU, or network capabilities are exhausted by load.
* Service availability: Percentage of actual uptime cloud-hosted workloads compared to the expected uptime.
* Backup Health: Number of backups actively being synchronized.

## 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.
* Tagging and naming: A company with more than 5% of resources lacking required tagging information or not obeying naming standards requires policies to ensure consistent application of them to cloud-deployed assets.
* Service availability: If mission-critical services are experiencing under 99.9% uptime, policies are required to ensure backup, recovery, and service continuity requirements are met.
* Over-provisioned resources trigger: If more than 25% of assets regularly using very small amounts of their available memory, CPU, or network capabilities, policies are required to optimize resources usage.
* Under-provisioned resources: If more than 5% of assets are regularly exhausting most of their available memory, CPU, or network capabilities, policies are required to help ensure these assets have the resources necessary to prevent service interruptions.
* Backup health: More than 5% failure of restore operations will with backup and ensure important resources are protected.

# Policy compliance processes

The following section outlines the processes that will ensure cloud deployments remain in compliance with Resource Consistency 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/resource-consistency/compliance-processes).

## Planning, review, and reporting processes

Initial risk assessment and planning: As part of the initial adoption of the Resource Consistency discipline, the Cloud Governance team will identify core business risks and tolerances related to operations and IT management. The team will use this information to discuss specific technical risks with members of IT staff and workload owners to develop a baseline set of Resource Consistency policies designed to mitigate these risks, establishing an initial governance strategy.

Deployment planning: Before deploying any asset, with IT and security staff will perform a review to identify any new operational risks. The team will establish resource requirements and expected demand patterns, and identify scalability needs and potential usage optimization opportunities. This process will also ensure backup and recovery plans are in place.

Deployment testing: As part of deployment, the Cloud Governance team, in cooperation with operations teams, will be responsible for reviewing the deployment to validate Resource Consistency policy compliance.

Annual planning: On an annual basis, the Cloud Governance team will perform a high-level review of Resource Consistency strategy. This review will explore future corporate expansion plans or priorities and update cloud adoption strategies to identify potential risk increase or other emerging Resource Consistency needs. The team will also use this time to review the latest best practices for cloud Resource Consistency and integrate these into policies and review processes.

Quarterly review and planning: On a quarterly basis the Cloud Governance team will perform a review of operational data and incident reports to identify any changes required in Resource Consistency policy. As part of this process, the team will review changes in resource usage and performance to identify assets that require increases or decreases in resource allocation and identify any workloads or assets that are candidates for retirement.

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 Resource Consistency as a discipline. 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 Resource Consistency policy requirements and guidance. As part of this process the team will review and update any documentation or other training assets to ensure they are in sync with the latest corporate policy statements.

Monthly audit and reporting reviews: On a monthly basis, the Cloud Governance team will perform an audit on all cloud deployments to assure their continued alignment with Resource Consistency policy. The team will review related activities with IT staff and identify any compliance issues not already handled as part of the ongoing monitoring and enforcement process. This review process will result in a report for the Cloud Strategy team and each cloud adoption team to communicate overall performance and 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 Resource Deployment related risks. They will also establish reporting and alerting systems to ensure prompt detection and mitigation of potential resource policy violations.

## Violation Triggers and Enforcement Actions

Over-provisioned resource detected: Resources detected using less than 60% of CPU or memory capacity should automatically scale down or deprovisioning resources to reduce costs.

Under-provisioned resource detected: Resources detected using more than 80% of CPU or memory capacity should automatically scale up or provisioning additional resources to provide additional capacity.

Untagged resource creation: Any request to create a resource without required meta tags will be rejected automatically.

Critical resource outage detected: IT staff are notified on all detected outages of mission-critical outages. If outage is not immediately resolvable, staff will escalate the issue and notify workload owners and the Cloud Governance team. The Cloud Governance team will track the issue until resolution and update guidance if policy revision is necessary to prevent 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/resource-consistency/toolchain).

## Azure Specific Tooling

Deploy resources using templates and apply metadata tagging: [Azure Resources Manager](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview)

Plan and Orchestrate deployments: [Azure Blueprints](https://docs.microsoft.com/en-us/azure/governance/blueprints/overview)

Configure operational reports and alerts: [Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/overview)

## Tooling for other Cloud Providers

List similar tools for other cloud providers, as needed.