Resource Consistency sample policy statements

02/11/2019 • 4 minutes to read • Contributors

In this article

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. These statements should provide a concise summary of risks and plans to deal with them. Each statement definition should include these pieces of information:

- **Technical risk:** A summary of the risk this policy will address.
- **Policy statement:** A clear summary explanation of the policy requirements.
- **Design options:** Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The following sample policy statements address common business risks related to resource consistency. These statements are examples you can reference when drafting policy statements to address your organization's needs. These examples are not meant to be proscriptive, and there are potentially several policy options for dealing with each identified risk. Work closely with business and IT teams to identify the best policies for your unique set of risks.

Tagging

Technical risk: Without proper metadata tagging associated with deployed resources, IT Operations cannot prioritize support or optimization of resources based on required SLA, importance to business operations, or operational cost. This can result in mis-allocation of IT resources and potential delays in incident resolution.

Policy statement: The following policies will be implemented:

- Deployed assets should be tagged with the following values: cost, criticality, SLA, and environment.
- Governance tooling must validate tagging related to cost, criticality, SLA, application, and environment. All values must align to predefined values managed by the governance team.

Potential design options: In Azure, standard name-value metadata tags are supported on most resource types. Azure Policy is used to enforce specific tags as part of resource creation.

Ungoverned subscriptions

Technical risk: Arbitrary creation of subscriptions and management groups can lead to isolated sections of your cloud estate that are not properly subject to your governance policies.

Policy statement: Creation of new subscriptions or management groups for any mission-critical applications or protected data will require a review from the Cloud Governance team. Approved changes will be integrated into a proper blueprint assignment.

Potential design options: Lock down administrative access to your organizations Azure management groups to only approved governance team members who will control the subscription creation and access control process.

Manage updates to virtual machines

Technical risk: Virtual machines (VMs) that are not up-to-date with the latest updates and software patches are vulnerable to security or performance issues, which can result in service disruptions.

Policy statement: Governance tooling must enforce that automatic updates are enabled on all deployed VMs. 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.

Potential design options: For Azure hosted VMs, you can provide consistent update management using the Update Management solution in Azure Automation.

Deployment compliance

Technical risk: Deployment scripts and automation tooling that is not fully vetted by the Cloud Governance team can result in resource deployments that violate policy.

Policy statement: The following policies will be implemented:

- Deployment tooling must be approved by the Cloud Governance team to ensure ongoing governance of deployed assets.
- Deployment scripts must be maintained in central repository accessible by the Cloud Governance team for periodic review and auditing.

Potential design options: Consistent use of Azure Blueprints to manage automated deployments allows consistent deployments of Azure resources that adhere to your organization's governance standards and policies.

Monitoring

Technical risk: Improperly implemented or inconsistently instrumented monitoring can prevent the detection of workload health issues or other policy compliance violations.

Policy statement: The following policies will be implemented:

- Governance tooling must validate that all assets related to mission-critical applications or protected data are included in monitoring for resource depletion and optimization.
- Governance tooling must validate that the appropriate level of logging data is being collected for all mission-critical applications or protected data.

Potential design options: Azure Monitor is the default monitoring service in Azure, and consistent monitoring can be enforced via Azure Blueprints when deploying resources.

Disaster recovery

Technical risk: Resource failure, deletions, or corruption can result in disruption of mission-critical applications or services and the loss of sensitive data.

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

Potential design options: The [Azure Site Recovery] service provides backup, recovery, and replication capabilities intended to minimize outage duration in business continuity and disaster recovery (BCDR) scenarios.

Next steps

Use the samples mentioned in this article as a starting point to develop policies that address specific business risks that align with your cloud adoption plans.

To begin developing your own custom policy statements related to Resource Consistency, download the Resource Consistency template.

To accelerate adoption of this discipline, choose the actionable governance journey that most closely aligns with your environment. Then modify the design to incorporate your specific corporate policy decisions.

Actionable governance journeys