


Resource Consistency policy compliance processes

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

In this article

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

[Ongoing monitoring processes](#)

[Violation triggers and enforcement actions](#)

[Next steps](#)

This article discusses an approach to policy adherence processes that govern [Resource Consistency](#). Effective cloud Resource Consistency governance starts with recurring manual processes designed to identify operational inefficiency, improve management of deployed resources, and ensure mission-critical workloads have minimal disruptions. These manual processes are supplemented with monitoring, automation, and tooling to help reduce the overhead of governance and allow for faster response to policy deviation.

Planning, review, and reporting processes

Cloud platforms provide an array of management tools and features that you can use to organize, provision, scale, and minimize downtime. Using these tools to effectively structure and operate your cloud deployments in ways that remediate potential risks requires well thought out processes and policies in addition to close cooperation with IT Operations teams and business stakeholders.

The following is a set of example processes commonly involved in the Resource Consistency discipline. Use these examples as a starting point when planning the processes that will allow you to continue to update Resource Consistency policy based on business change and feedback from the development and IT teams tasked with turning guidance into action.

Initial risk assessment and planning: As part of your initial adoption of the Resource Consistency discipline, identify your core business risks and tolerances related to operations and IT management. Use this information to discuss specific technical risks with members of your IT teams and workload owners to develop a baseline set of Resource Consistency policies designed to remediate these risks, establishing your initial governance strategy.

Deployment planning: Before deploying any asset, perform a review to identify any new operational risks. Establish resource requirements and expected demand patterns, and identify scalability needs and potential usage optimization opportunities. Also ensure backup and recovery plans are in place.

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

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

Quarterly review and planning: On a quarterly basis perform a review of operational data and incident reports to identify any changes required in Resource Consistency policy. As part of this process, 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 planning process is also a good time to evaluate the current membership of your Cloud Governance team for knowledge gaps related to new or evolving policy and risks related to Resource Consistency as a discipline. Invite relevant IT staff to participate in reviews and planning as either temporary technical advisors or permanent members of your team.

Education and training: On a bimonthly basis, 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 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, perform an audit on all cloud deployments to assure their continued alignment with Resource Consistency policy. Review 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 performance and adherence to policy. The report is also stored for auditing and legal purposes.

Ongoing monitoring processes

Determining if your Resource Consistency governance strategy is successful depends on visibility into the current and past state of your cloud infrastructure. Without the ability to analyze the relevant metrics and data of your cloud environment's health and activity, you cannot identify changes in your risks or detect violations of your risk tolerances. The ongoing governance processes discussed above require quality data to ensure policy can be modified to optimize your cloud resource usage and improve overall performance of cloud-hosted workloads.

Ensure that your IT teams have implemented automated monitoring systems for your cloud infrastructure that capture the relevant logs data you need to evaluate risks. Be proactive in monitoring these systems to ensure prompt detection and mitigation of potential policy violation, and ensure your monitoring strategy is in line with your operational needs.

Violation triggers and enforcement actions

Because Resource Consistency policy compliance can lead to critical service disruption or significant cost overruns risks, the Cloud Governance team should have visibility into noncompliance incidents. Ensure IT staff have clear escalation paths for reporting these issues to the governance team members best suited to identify and verify that policy issues are mitigated once detected.

When violations are detected, you should take actions to realign with policy as soon as possible. Your IT team can automate most violation triggers using the tools outlined in the [Resource Consistency toolchain for Azure](#).

The following triggers and enforcement actions provide examples you can reference when planning how to use monitoring data to resolve policy violations:

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

Next steps

Using the [Cloud Management template](#), document the processes and triggers that align to the current cloud adoption plan.

For guidance on executing cloud management policies in alignment with adoption plans, see the article on discipline improvement.

Resource Consistency discipline improvement