


Large enterprise: Resource Consistency evolution

02/11/2019 • 6 minutes to read • Contributors 

In this article

[Evolution of the narrative](#)

[Evolution of tangible risks](#)

[Evolution of the policy statements](#)

[Evolution of the best practices](#)

[Conclusion](#)

[Next steps](#)

This article evolves the narrative by adding Resource Consistency controls to the governance MVP to support mission-critical applications.

Evolution of the narrative

The cloud adoption teams have met all requirements to move protected data. With those applications come SLA commitments to the business and need for support from IT Operations. Right behind the team migrating the two datacenters, multiple application development and BI teams are ready to begin launching new solutions into production. IT Operations is new to cloud operations and needs to quickly integrate existing operational processes.

Evolution of current state

- IT is actively moving production workloads with protected data into Azure. Some low-priority workloads are serving production traffic. More can be cut over as soon as IT Operations signs off on readiness to support the workloads.
- The application development teams are ready for production traffic.
- The BI team is ready to integrate predictions and insights into the systems that run operations for the three business units.

Evolution of the future state

- IT operations is new to cloud operations and needs to quickly integrate existing operational processes.

The changes to current and future state expose new risks that will require new policy statements.

Evolution of tangible risks

Business interruption: There is an inherent risk of any new platform causing interruptions to mission-critical business processes. The IT Operations team and the teams executing on various cloud adoptions are relatively inexperienced with cloud operations. This increases the risk of interruption and must be remediated and governed.

This business risk can be expanded into several technical risks:

- Misaligned operational processes might lead to outages that can't be detected or mitigated quickly.
- External intrusion or denial of service attacks might cause a business interruption.
- Mission-critical assets might not be properly discovered and therefore not properly operated.

- Undiscovered or mislabeled assets might not be supported by existing operational management processes.
- Configuration of deployed assets might not meet performance expectations.
- Logging might not be properly recorded and centralized to allow for remediation of performance issues.
- Recovery policies may fail or take longer than expected.
- Inconsistent deployment processes might result in security gaps that could lead to data leaks or interruptions.
- Configuration drift or missed patches might result in unintended security gaps that could lead to data leaks or interruptions.
- Configuration might not enforce the requirements of defined SLAs or committed recovery requirements.
- Deployed operating systems or applications might not meet OS and application hardening requirements.
- There is a risk of inconsistency due to multiple teams working in the cloud.

Evolution of the policy statements

The following changes to policy will help remediate the new risks and guide implementation. The list looks long, but the adoption of these policies may be easier than it would appear.

1. All deployed assets must be categorized by criticality and data classification. Classifications are to be reviewed by the Cloud Governance team and the application owner before deployment to the cloud.
2. Subnets containing mission-critical applications must be protected by a firewall solution capable of detecting intrusions and responding to attacks.
3. Governance tooling must audit and enforce network configuration requirements defined by the Security Baseline team.
4. Governance tooling must validate that all assets related to mission-critical applications or protected data are included in monitoring for resource depletion and optimization.
5. Governance tooling must validate that the appropriate level of logging data is being collected for all mission-critical applications or protected data.
6. Governance process must validate that backup, recovery, and SLA adherence are properly implemented for mission-critical applications and protected data.
7. Governance tooling must limit virtual machine deployment to approved images only.
8. Governance tooling must enforce that automatic updates are **prevented** on all deployed assets that support mission-critical applications. 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.
9. Governance tooling must validate tagging related to cost, criticality, SLA, application, and data classification. All values must align to predefined values managed by the Cloud Governance team.
10. Governance processes must include audits at the point of deployment and at regular cycles to ensure consistency across all assets.
11. Trends and exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tooling used in the cloud.
12. Before release into production, all mission-critical applications and protected data must be added to the designated operational monitoring solution. Assets that cannot be discovered by the chosen IT operations tooling cannot be released for production use. Any changes required to make the assets discoverable must be made to the relevant deployment processes to ensure assets will be discoverable in future deployments.
13. When discovered, asset sizing is to be validated by operational management teams to validate that the asset meets performance requirements.
14. Deployment tooling must be approved by the Cloud Governance team to ensure ongoing governance of deployed assets.
15. Deployment scripts must be maintained in central repository accessible by the Cloud Governance team for periodic review and auditing.
16. Governance review processes must validate that deployed assets are properly configured in alignment with SLA and recovery requirements.

Evolution of the best practices

This section of the article will evolve the governance MVP design to include new Azure policies and an implementation of Azure Cost Management. Together, these two design changes will fulfill the new corporate policy statements.

Following the experience of this fictional example, it is assumed that the Protected Data evolution has already happened. Building on that best practice, the following will add operational monitoring requirements, readying a subscription for mission-critical applications.

Corporate IT subscription: Add the following to the Corporate IT subscription, which acts as a hub.

1. As an external dependency, the Cloud Operations team will need to define operational monitoring tooling, business continuity and disaster recovery (BCDR) tooling, and automated remediation tooling. The Cloud Governance team can then support necessary discovery processes.
 - a. In this use case, the Cloud Operations team chose Azure Monitor as the primary tool for monitoring mission-critical applications.
 - b. The team also chose Azure Site Recovery as the primary BCDR tooling.
2. Azure Site Recovery implementation.
 - a. Define and deploy Azure Vault for backup and recovery processes.
 - b. Create an Azure Resource Management template for creation of a vault in each subscription.
3. Azure Monitor implementation.
 - a. Once a mission-critical subscription is identified, a log analytics workspace can be created using PowerShell. This is a predeployment process.

Individual cloud adoption subscription: The following will ensure that each subscription is discoverable by the monitoring solution and ready to be included in BCDR practices.

1. Azure Policy for mission-critical nodes
 - a. Audit and enforce use of standard roles only.
 - b. Audit and enforce application of encryption for all storage accounts.
 - c. Audit and enforce use of approved network subnet and VNet per network interface.
 - d. Audit and enforce the limitation of user-defined routing tables.
 - e. Audit and enforce the deployment of Log Analytics agents for Windows and Linux virtual machines.
2. Azure blueprint
 - a. Create a blueprint named `mission-critical-workloads-and-protected-data`. This blueprint will apply assets in addition to the protected data blueprint.
 - b. Add the new Azure policies to the blueprint.
 - c. Apply the blueprint to any subscription that is expected to host a mission-critical application.

Conclusion

Adding these processes and changes to the governance MVP helps remediate many of the risks associated with resource governance. Together, they add the recovery, sizing, and monitoring controls necessary to empower cloud-aware operations.

Next steps

As cloud adoption continues to evolve and deliver additional business value, the risks and cloud governance needs will also evolve. For the fictional company in this journey, the next trigger is when the scale of deployment exceeds 1,000 assets to the cloud or monthly spending exceeds \$10,000 USD per month. At this point, the Cloud Governance team adds Cost Management controls.

