


Deployment Acceleration policy compliance processes

02/11/2019 • 4 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 [Deployment Acceleration](#). Effective governance of cloud configuration starts with recurring manual processes designed to detect issues and impose policies to remediate those risks. However, you can automate these processes and supplement with tooling to reduce the overhead of governance and allow for faster response to deviation.

Planning, review, and reporting processes

The best Deployment Acceleration tools in the cloud are only as good as the processes and policies that they support. The following is a set of example processes commonly used as part of a Deployment Acceleration discipline. Use these examples as a starting point when planning the processes that will allow you to continue to update deployment and configuration policy based on business change and feedback from the development and IT teams responsible for turning governance guidance into action.

Initial risk assessment and planning: As part of your initial adoption of the Deployment Acceleration discipline, identify your core business risks and tolerances related to deployment of your business applications. Use this information to discuss specific technical risks with members of the IT operations team, and develop a baseline set of deployment and configuration policies for remediating these risks to establish your initial governance strategy.

Deployment planning: Before deploying any asset, 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 your IT operations teams, is responsible for reviewing the deployment policy compliance.

Annual planning: Conduct an annual high-level review of Deployment Acceleration strategy. Explore future corporate priorities and updated cloud adoption strategies to identify potential risk increase and other emerging configuration needs and opportunities. Also use this time to review the latest DevOps best practices and integrate these into your policies and review processes.

Quarterly review and planning: 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, review current DevOps and DevTechOps best practices, and update policy as appropriate. After the review is complete, align application and systems design guidance with updated policy.

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 DevOps and Deployment Acceleration. 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 Deployment Acceleration strategy and requirements. As part of this process 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: Perform a monthly audit on all cloud deployments to assure their continued alignment with configuration policy. 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 processes

Determining if your Deployment Acceleration 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 resources operational health and activity, you cannot identify changes in your risks or detect violations of your risk tolerances. The ongoing governance processes discussed above requires quality data to ensure policy can be modified to protect your infrastructure against changing threats and risks from misconfigured resources.

Ensure that your IT operations teams have implemented automated monitoring systems for your cloud infrastructure that capture the relevant logs data you need to evaluate risk. 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 deployment and configuration needs.

Violation triggers and enforcement actions

Because noncompliance with configuration policies can lead to critical service disruption risks, the Cloud Governance team should have visibility into serious policy violations. Ensure IT staff have clear escalation paths for reporting configuration compliance 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 [Deployment Acceleration toolchain for Azure](#).

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

- **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.

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.

Deployment Acceleration discipline improvement