


Deployment Acceleration motivations and business risks

02/11/2019 • 2 minutes to read • Contributors 

In this article

[Is Deployment Acceleration relevant?](#)

[Business risk](#)

[Next steps](#)

This article discusses the reasons that customers typically adopt a Deployment Acceleration discipline within a cloud governance strategy. It also provides a few examples of business risks that drive policy statements.

Is Deployment Acceleration relevant?

On-premises systems are often deployed using baseline images or installation scripts. Additional configuration is usually necessary, which may involve multiple steps or human intervention. These manual processes are error-prone and often result in "configuration drift", requiring time-consuming troubleshooting and remediation tasks.

Most Azure resources can be deployed and configured manually via the Azure portal. This approach may be sufficient for your needs when only have a few resources to manage. However, as your cloud estate grows, your organization should begin to integrate automation into your deployment processes to ensure your cloud resources avoid configuration drift or other problems introduced by manual processes. Adopting a DevOps or [DevSecOps](#) approach is often the best way to manage your deployments as you cloud adoption efforts mature.

A robust Deployment Acceleration plan ensures that your cloud resources are deployed, updated, and configured correctly and consistently, and remain that way. The maturity of your Deployment Acceleration strategy can also be a significant factor in your [Cost Management strategy](#). Automated provisioning and configuration of your cloud resources allows you to scale down or deallocate resources when demand is low or time-bound, so you only pay for resources as you need them.

Business risk

The Deployment Acceleration discipline attempts to address the following business risks. During cloud adoption, monitor each of the following for relevance:

- **Service disruption:** Lack of predictable repeatable deployment processes or unmanaged changes to system configurations can disrupt normal operations and can result in lost productivity or lost business.
- **Cost overruns:** Unexpected changes in configuration of system resources can make identifying root cause of issues more difficult, raising the costs of development, operations, and maintenance.
- **Organizational inefficiencies:** Barriers between development, operations, and security teams can cause numerous challenges to effective adoption of cloud technologies and the development of a unified cloud governance model.

Next steps

Using the [Cloud Management template](#), document business risks that are likely to be introduced by the current cloud adoption plan.

Once an understanding of realistic business risks is established, the next step is to document the business's tolerance for risk and the indicators and key metrics to monitor that tolerance.

Metrics, indicators, and risk tolerance