


Deployment Acceleration sample policy statements

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

In this article

[Reliance on manual deployment or configuration of systems](#)

[Lack of visibility into system issues](#)

[Configuration security reviews](#)

[Next steps](#)

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 configuration-related business risks. 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.

Reliance on manual deployment or configuration of systems

Technical risk: Relying on human intervention during deployment or configuration increases the likelihood of human error and reduces the repeatability and predictability of system deployments and configuration. It also typically leads to slower deployment of system resources.

Policy statement: All assets deployed to the cloud should be deployed using templates or automation scripts whenever possible.

Potential design options: [Azure Resource Manager templates](#) provides an infrastructure-as-code approach to deploying your resources to Azure. The [Azure Building Blocks](#) provide a command-line tool and set of Resource Manager templates designed to simplify deployment of Azure resources.

Lack of visibility into system issues

Technical risk: Insufficient monitoring and diagnostics for business systems prevent operations personnel from identifying and remediating issues before a system outage occurs, and can significantly increase the time needed to properly resolve an outage.

Policy statement: The following policies will be implemented:

- Key metrics and diagnostics measures will be identified for all production systems and components, and monitoring and diagnostic tools will be applied to these systems and monitored regularly by operations personnel.

- Operations will consider using monitoring and diagnostic tools in nonproduction environments such as Staging and QA to identify system issues before they occur in the production environment.

Potential design options: [Azure Monitor](#), which also includes Log Analytics and Application Insights, provides tools for collecting and analyzing telemetry to help you understand how your applications are performing and proactively identify issues affecting them and the resources they depend on.

Configuration security reviews

Technical risk: Over time, new security threats or concerns can increase the risks of unauthorized access to secure resources.

Policy statement: Cloud Governance processes must include quarterly review with configuration management teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

Potential design options: Establish a quarterly security review meeting that includes both governance team members and IT staff responsible for configuration cloud applications and resources. Review existing security data and metrics to establish gaps in current Deployment Acceleration policy and tooling, and update policy to remediate any new risks.

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 identity management, download the [Identity Baseline 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