Governance, security, and compliance in Azure

04/09/2019 • 2 minutes to read • Contributors

In this article

Use **Azure Policy** and **Azure Security Center** to help enforce and automate your governance decisions. As you plan your compliance strategy, we recommend you work with people in your organizations with the roles: security, compliance, and enterprise architect.

Azure Policy | Azure Security Center

Azure Policy is a service that you use to create, assign, and manage policies. These policies enforce rules on your resources so those resources stay compliant with your corporate standards and service level agreements. Azure Policy scans your resources to identify resources that aren't compliant with the policies you implement. For example, you can have a policy to allow only a specific virtual machine (VM) size to run in your environment. When you implement this policy, it evaluates existing VMs in your environment and any new VMs that are deployed. The policy evaluation generates compliance events for you to use for monitoring and reporting.

Common policies you should consider:

- Enforce tagging for resources and resource groups.
- Restrict regions for deployed resources.
- Restrict expensive SKUs for specific resources.
- Audit use of important optional features like Azure managed disks.

Apply a policy

To apply a policy to a resource group:

1. Go to Azure Policy.
2. Select **Assign a policy**.

Learn more

To learn more, see Azure Policy.