


# What processes can help ensure policy adherence?

02/11/2019 • 4 minutes to read • Contributors 

## In this article

[Prioritize policy adherence processes](#)

[Establish Cloud Governance team processes](#)

[Violation triggers and actions](#)

[Monitoring and compliance automation](#)

After establishing your cloud policy statements and drafting a design guide, you'll need to create a strategy for ensuring your cloud deployment stays in compliance with your policy requirements. This strategy will need to encompass your Cloud Governance team's ongoing review and communication processes, establish criteria for when policy violations require action, and defining the requirements for automated monitoring and compliance systems that will detect violations and trigger remediation actions.

See the corporate policy sections of the [actionable governance journeys](#) for examples of how policy adherence process fit into a cloud governance plan.

## Prioritize policy adherence processes

How much investment in developing processes is required to support your policy goals? Depending on the size and maturity of your cloud deployment, the effort required to establish processes that support compliance, and the costs associated with this effort, can vary widely.

For small deployments consisting of development and test resources, policy requirements may be simple and require few dedicated resources to address. On the other hand, a mature mission-critical cloud deployment with high-priority security and performance needs may require a team of staff, extensive internal processes, and custom monitoring tooling to support your policy goals.

As a first step in defining your policy adherence strategy, evaluate how the processes discussed below can support your policy requirements. Determine how much effort is worth investing in these processes, and then use this information to establish realistic budget and staffing plans to meet these needs.

## Establish Cloud Governance team processes

Before defining triggers for policy compliance remediation, you need establish the overall processes that your team will use and how information will be shared and escalated between IT staff and the Cloud Governance team.

### Assign Cloud Governance team members

Your Cloud Governance team will provide ongoing guidance on policy compliance and handle policy-related issues that emerge when deploying and operating your cloud assets. When building this team, invite staff from your organization that have expertise in areas covered by your defined policy statements and identified risks.

For initial test deployments this can be limited to a few system administrators responsible for establishing the basics of governance. As your governance processes mature, review the cloud guidance team's membership regularly to ensure that you can properly address new potential risks and policy requirements. Identify members of your IT and business

staff with relevant experience or interest in specific areas of governance and include them in your teams on a permanent or ad-hoc basis as-needed.

## Reviews and policy iteration

As additional resources and workloads are deployed, the Cloud Governance team will need to ensure that new workloads or assets comply with policy requirements. Evaluate new requirements from workload development teams to ensure their planned deployments will align with your design guides, and update your policies to support these requirements when appropriate.

Plan to evaluate new potential risks and update policy statements and design guides as needed. Work with IT staff and workload teams to evaluate new Azure features and services on an ongoing basis. Also schedule regular review cycles each of the five governance disciplines to ensure policy is up-to-date and being met.

## Education

Policy compliance requires IT staff and developers to understand the policy requirements that affect their areas of responsibility. Plan to devote resources to document decisions and requirements, and educate all relevant teams on the design guides that support your policy requirements.

As policy changes, regularly update documentation and training materials, and ensure education efforts communicate updated requirements and guidance to relevant IT staff.

## Establish escalation paths

If a resource goes out of compliance, who gets notified? If IT staff detect a policy compliance issue, who do they contact? Make sure the escalation process to the Cloud Governance team is clearly defined. Ensure these communication channels are kept updated to reflect staff and organization changes.

# Violation triggers and actions

After defining your Cloud Governance team and its processes, you need to explicitly define what qualifies as compliance violations that will trigger actions, and what those actions should be.

## Define triggers

For each of your policy statements, review requirements to determine what constitutes a policy violation. Generate your triggers using the information you've already established as part of the policy definition process.

- **Risk tolerance:** Create violation triggers based on the metrics and risk indicators you established as part of your [risk tolerance analysis](#).
- **Defined policy requirements:** Policy statements may provide service level agreement (SLA), business continuity and disaster recovery (BCDR), or performance requirements that should be used as the basis for compliance triggers.

## Define actions

Each violation trigger should have a corresponding action. Triggered actions should always notify an appropriate IT staff or Cloud Governance team member when a violation occurs. This notification can lead to a manual review of the compliance issue or kickoff a predefined remediation process depending on the type and severity of the detected violation.

Some examples of violation triggers and actions:

Cloud governance discipline	Sample trigger	Sample action
Cost Management	Monthly cloud spending is more than 20% higher than expected.	Notify billing unit leader who will begin a review of resource usage.
Security Baseline	Detect suspicious user login activity.	Notify IT security team and disable suspect user account.
Resource Consistency	CPU utilization for workload is greater than 90%.	Notify the IT Operations team and scale out additional resources to handle load.

## Monitoring and compliance automation

After you've defined your compliance violation triggers and actions, you can start planning how best to use the logging and reporting tools and other features of the cloud platform to help automate your monitoring and policy compliance strategy.

Consult the Cloud Adoption Framework [logging and reporting decision guide](#) topic for guidance on choosing the best monitoring pattern for your deployment.