


# Security Baseline policy compliance processes

02/11/2019 • 5 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 [Security Baseline](#). Effective governance of cloud security starts with recurring manual processes designed to detect vulnerabilities and impose policies to remediate those security risks. This requires regular involvement of the Cloud Governance team and interested business and IT stakeholders to review and update policy and ensure policy compliance. In addition, many ongoing monitoring and enforcement processes can be automated or supplemented with tooling to reduce the overhead of governance and allow for faster response to policy deviation.

## Planning, review, and reporting processes

The best Security Baseline 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 involved in the Security Baseline discipline. Use these examples as a starting point when planning the processes that will allow you to continue to update security policy based on business change and feedback from the security and IT teams tasked with turning governance guidance into action.

**Initial risk assessment and planning:** As part of your initial adoption of the Security Baseline discipline, identify your core business risks and tolerances related to cloud security. Use this information to discuss specific technical risks with members of your IT and security teams and develop a baseline set of security policies for mitigating these risks to establish your initial governance strategy.

**Deployment planning:** Before deploying any workload or asset, perform a security review to identify any new risks and ensure all access and data security policy requirements are met.

**Deployment testing:** As part of the deployment process for any workload or asset, the Cloud Governance team, in cooperation with your corporate security teams, will be responsible for reviewing the deployment to validate security policy compliance.

**Annual planning:** On an annual basis, perform a high-level review of Security Baseline strategy. Explore future corporate priorities and updated cloud adoption strategies to identify potential risk increase and other emerging security needs. Also use this time to review the latest Security Baseline best practices and integrate these into your policies and review processes.

**Quarterly review and planning:** On a quarterly basis perform a review of security audit data and incident reports to identify any changes required in security policy. As part of this process, review the current cybersecurity landscape to proactively anticipate emerging threats, and update policy as appropriate. After the review is complete, align 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 security. 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 security policy 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:** On a monthly basis, perform an audit on all cloud deployments to assure their continued alignment with security policy. Review security 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 security 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 security health and activity, you cannot identify changes in your risks or detect violations of your risk tolerances. The ongoing governance processes discussed above require quality data to ensure policy can be modified to better protect your infrastructure against changing threats and security requirements.

Ensure that your security and IT 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 security needs.

## Violation triggers and enforcement actions

Because security noncompliance can lead to critical and data exposure and service disruption risks, the Cloud Governance team should have visibility into serious policy violations. Ensure IT staff have clear escalation paths for reporting security issues to the governance team members best suited to identify and verify that policy issues are mitigated.

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 [Security Baseline toolchain for Azure](#).

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

- **Increase in attacks detected.** If any resource experiences a 25% increase in brute force or DDoS attacks, discuss with IT security staff and workload owner to determine remedies. Track issue and update guidance if policy revision is necessary to prevent future incidents.
- **Unclassified data detected.** Any data source without an appropriate privacy, security, or business impact classification will have external access denied until the classification is applied by the data owner and the appropriate level of data protection applied.
- **Security health issue detected.** Disable access to any virtual machines (VMs) that have known access or malware vulnerabilities identified until appropriate patches or security software can be installed. Update policy guidance to account for any newly detected threats.
- **Network vulnerability detected.** Access to any resource not explicitly allowed by the network access policies should trigger an alert to IT security staff and the relevant workload owner. Track issue and update guidance if policy revision is necessary to mitigate future incidents.

## 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.

