Google Cloud

Audits and security assessments

So far, you've learned that audits demonstrate to others that an organization has specific security standards in place for governance and control, making them trustworthy.

In this reading, you'll learn more about auditors and how they conduct audits. You'll also explore the different types of assessments that are commonly used before and during audits. Please note, the following reading should not be considered legal advice.

Who are the auditors?

There are several different types of auditors. For example, an internal auditor ensures that controls are followed by inspecting those controls. Internal audits are often conducted by the organization's Chief Financial Officer (CFO) instead of the IT team. CFOs have this responsibility because if the internal audit team also reports to the IT team, there may be an influence from leadership to ignore identified issues. But, if the audit team reports directly to the finance team, they can work independently without leadership influence.

There are also external auditors who are accredited by organizations that have developed specific audit standards. For example, the American Institute of Certified Public Accountants (AICPA) audits for SOC 2® certification, and external assessors audit for HITRUST® certification. Auditors use a set of common criteria to inspect all the controls and issue findings. They then make a determination if the audit standard has been adequately met.

For example, an audit standard might require specific controls be in place and working to properly pass the audit and be certified. The auditor would then evaluate whether the requirements for the audit were met, and issue a recommendation to the accrediting body. The accrediting body then certifies the organization and issues a report. Auditors receive regular training so they can uphold high standards that are applied equally across organizations.

How do they conduct audits?

Auditors or auditing organizations create control expectations and a rubric for assessment. The control expectations may change depending on the type of company being audited, and the specific ongoing governance requirements that company must meet. For example, public companies usually meet Sarbanes-Oxley, and SOC 1 and 2® audit standards. Also, companies doing business in regulated industries, like healthcare, may need to meet audit standards for HITRUST®.

A security audit report is a comprehensive document that contains the results of a security assessment for a business or organization. It identifies control gaps and outlines the strengths and weaknesses of the organization's security. It lists all of the auditors' findings, which are descriptions of missing controls. For example, an organization might be required to have controls like a vulnerability management process and incident management. Auditors document if the organization is non-compliant with these requirements. The audit's findings would then focus on the lack of a system or control, but not the specific vulnerability.

Also, findings may be prioritized according to severity and specific organizational needs. For example, the absence of controls to protect against distributed denial of service (DDoS) attacks is more severe for a company with a public-facing app, like an internet store, but less severe for a company that concentrates on software development, and doesn't expose its resources to public networks.

Security assessments

During an audit, an auditor might assess or ask for proof of security assessments such as vulnerability scans, cloud services configuration hardening, and cloud infrastructure security.

While an audit is an internal or external evaluation of an organization's compliance against specific standards or regulations, an assessment is an internal evaluation of the security posture of an organization. An assessment helps identify potential security weaknesses, and determines the effectiveness of security controls that are already in place. This type of information is valuable to an auditor evaluating security controls.

Vulnerability scanning

Vulnerability scans are one type of assessment that organizations can provide auditors. Vulnerability scans use automation to identify and analyze known vulnerabilities in a system. And, they check several types of resources, including systems, networks, cloud infrastructures, web applications, network service apps, and containers.

Cloud services configuration hardening

Auditors might also request an assessment of how organizations harden their cloud service configurations. The essential goal of cloud services configuration hardening is to prevent potential vulnerabilities. An internal assessment validates that services have the minimum necessary permissions and capabilities, and that any unneeded communication capabilities, like ports, are closed and can't communicate. Security operations teams assess service configurations to ensure that the configuration is updated to stay aligned with new security best practices and guidelines, and to ensure this process runs seamlessly. These teams typically use vulnerability scanning tools, like Security Command Center to perform the assessment.

A configuration hardening audit assesses these services, among others:

- Cloud systems
- Containers
- Clusters
- Virtual machines
- Network devices

Cloud infrastructure security assessment

A cloud infrastructure security assessment is an automated check to determine if the controls are working as expected to meet standards, like CIS® benchmarks. Auditors request this type of assessment because it evaluates infrastructures against benchmarks to detect compliance gaps within the cloud environment. It can also check for sufficient monitoring, identity capabilities, and verify that the access and security policies are in place to mitigate risk.

Pro tip: Leverage automation to continually assess the environment for security deficiencies. While this doesn't eliminate the need for a scheduled annual, bi-annual, or quarterly audit, automated checks help ensure that risks and vulnerabilities are detected, identified, and remediated before the audit takes place.

Note: Audits can vary based on industry and organizational needs.

Key takeaways

Audits are essential to help ensure compliance and to build user trust. While auditors can be internal or external to an organization, they all inspect controls and their application in an organization's system. An important outcome of an audit is the audit report that highlights security gaps and strengths. Also, organizations should be prepared to provide auditors with proof of security assessments that demonstrate the effectiveness of security controls. Overall, audits provide enhanced visibility into the security posture of cloud assets.

Resources for more information

These resources can help you learn more about audits and assessments:

- SOC 2® suite of services provides more information on SOC2® audits that are carried by AICPA
- Click the link to learn the difference between an audit and an assessment