

Audits vs. Assessments: Who's Asking, and How Formal It Gets

Mon, Aug 31, 10:00 AM EDT · <https://scottslab.io/posts/audits-and-assessments>



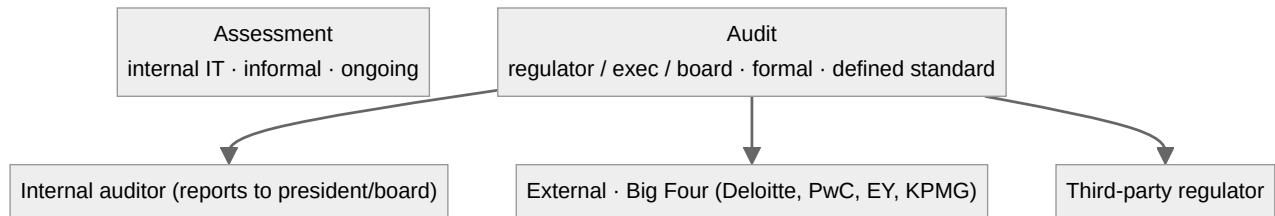
TL;DR

An assessment is the informal, ongoing self-check your own IT team runs. An audit is the formal one: demanded by a regulator, executive, or board, against a defined standard, by one of three auditor types (internal, external "Big Four," or a third-party regulator). Define the scope upfront (on-prem, cloud, hybrid) so nobody's surprised, and expect two deliverables: a gap analysis (your remediation roadmap) and an attestation (the formal "controls are adequate and working").

The words get used interchangeably and they shouldn't be, because the difference is who's asking and how much it binds you. An assessment is requested by your own internal IT staff. It's less formal, and it's an ongoing evaluation tool you run on yourselves to find problems before anyone official does. An audit is a formal examination requested by an outside authority: a regulator, an executive, the board. It follows a defined standard, not your own judgment. Assessments are how you stay ready; audits are how you get graded.

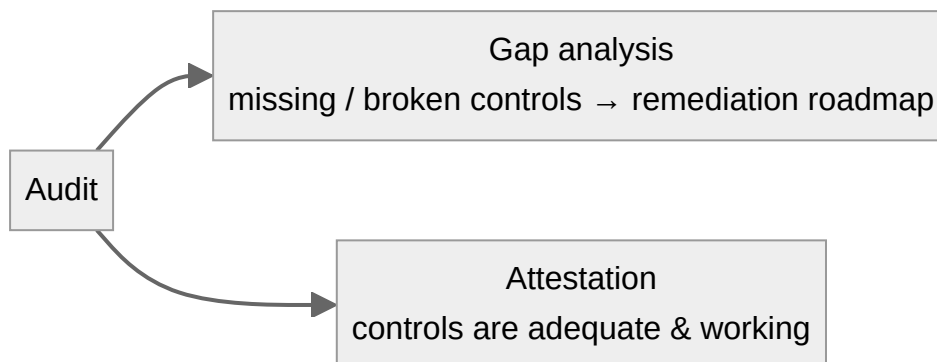
Audits come from three types of auditor, and the independence increases as you go down the list. Internal auditors work for the organization but report up to the president or board (not to IT), so they can call it straight. External auditors are the independent firms: the "Big Four" being Deloitte,

PwC, EY, and KPMG. And third-party regulators audit you against the rules they enforce. The pattern is deliberate: the more the result matters to outsiders, the more independent the person signing it needs to be.



Audits vs. Assessments: Who's Asking, and How Formal It Gets

Real audit standards are far more concrete than "are you secure?" PCI DSS ships a roughly 360-page audit procedures document, where each requirement carries specific test procedures the auditor must perform. Requirement 3.5.1 (rendering card numbers unreadable) alone breaks into three distinct steps the auditor walks through. Which is why scope has to be nailed down upfront: on-premises, cloud, hybrid, or all three. Defining scope before the audit starts prevents nasty surprises for everyone. The auditor doesn't wander into systems nobody meant to include, and you don't get graded on infrastructure that was never in play.



Audits vs. Assessments: Who's Asking, and How Formal It Gets

Two deliverables come out the other end, and you want to know which you're getting. A gap analysis lists the controls that are missing or not working properly. It's unglamorous and it's the most useful thing an audit produces, because it's a ready-made remediation roadmap. An attestation is the formal statement that your controls are adequate and functioning: the clean bill of health you can hand to a customer or regulator. Aim for the attestation; treasure the gap analysis, because it's the one that actually makes you better.