Avoiding Common Third Party Attestation Pitfalls

A GUIDE TO AUDIT READINESS

Third-party attestation (TPA) reports are **increasingly important for the tech industry**. They verify that a company has internal controls in place, and that those controls are functioning properly. Attestation services help verify that safeguards are in place at the company over valuable customer data, like financial or other personally identifiable information.

Many tech companies, such as software-as-a-service (SaaS) or anything-as-a-service (XaaS) businesses, frequently provide services to other companies that increase connectivity between two or more organizations. Because these organizations make attractive targets for threat actors, they must be proactive in mitigating the risk of breaches or other events that could disrupt operations or expose personal information. If a XaaS company does not prioritize completeness, accuracy, and timeliness in processing activities or transactions for its customer base, it could negatively impact customer organizations' internal control environments, as well.

Because of these and other potential hurdles, tech companies are facing increased demand from stakeholders to assess their internal controls environments. For example, potential customers or investors may require a company to obtain a **System and Organization Controls (SOC) Report** to demonstrate and document the strength of its controls. Attestation services enable companies to do just that.

But even if they recognize the importance of attestation services, are tech companies prepared for the scope and rigor of an audit? Some companies — especially startups — may not be tracking their audit readiness and may not have the right documentation, experience, or mindset for a successful audit.

Here are some of the most common TPA pitfalls, as well as tips for how tech companies can avoid them.

Common TPA Pitfalls

A PASSIVE MINDSET

Audits measure outputs, and the mindset at the top of an organization affects its inputs. Audit-ready leaders should set an example by emphasizing corporate governance in their day-to-day interactions. Are the right protocols in place and did they function properly over a given period? Is any information incomplete or missing? Most critically: Is there a clear trail of accountability in key areas — i.e., was it documented? Without documentation, it is not provable. Without the right mindset, that documentation might not exist.

If company leaders do not actively establish and follow protocols, that passive tone can spread. It can filter throughout the company, harming day-to-day activities and reducing audit readiness. Tone at the top matters. Other employees take their cues from leadership and may not prioritize active corporate governance through implementation of formal policies, procedures, and controls in their own work. Ready or documented information that shows a well governed environment may not be available, making it difficult to pass an audit and greatly increasing the amount of work necessary to prepare for one.

ORGANIZATIONAL IMMATURITY

Many early-stage companies, such as founder-led or bootstrapped startups, may lack mechanisms to iterate and improve on their systems and processes. These companies often lack formal processes and tend to be heavily dependent on a small number of personnel who are already stretched thin with the day to day rigor of a start-up. While this is understandable, as many of these companies are focused on survival or on getting their product to market, organizational immaturity can negatively impact audit readiness.

For example, imagine a small tech startup with a lean staff and an "everyone-knows-everyone" office culture. This startup may have a policy whereby a director must give verbal approval before any checks exceeding a certain amount are issued. The policy may be convenient and timesaving, but it does not leave a paper trail. There is no way to verify that the director gave approval in any particular instance. Audits require hard evidence, not word-of-mouth. When processes are informal, there is no audit trail to trace where things went wrong, if something does go wrong, and no clear trail of accountability.

LACK OF IN-HOUSE EXPERTISE

Just as they often may operate without well-defined process and controls, younger companies or startups likely may not have a leadership team with prior attestation experience, which can make it more difficult to address barriers to audit readiness.

If leaders don't have a clear understanding of an audit's scope, process, and requirements, it will be harder for them to develop and implement effective policies and procedures to ready the company for an audit.

INADEQUATE DOCUMENTATION

Documentation is the most essential part of audit readiness — but not all documentation is created equal. Even if a tech company has a record keeping policy in place, is it robust enough to pass an audit? Audit-ready documentation must be organized and accessible, standardized across an organization, and preserved over a sufficient period.

Imagine another version of the tech startup above, where the company policy requires written approval from an executive for each check issued over a certain threshold. In theory, this policy would leave a paper trail for an auditor to follow, but only if the paper trail is still there when the auditor is looking for it. Long-term data storage can be expensive, especially for an early-stage startup. To offset the costs, the startup might decide to cap its document storage at three months. That practice may suffice for the company's internal needs, but it will not be enough if a new customer asks the company to pursue a SOC 2 Type 2 examination. SOC 2 Type 2 examination can cover up to one year of activity, meaning it would take months to build up enough documentation for an audit, even after the company implements the changes necessary to ensure that documentation is preserved for longer.

Audit Readiness Tips

It's virtually impossible to cram for an audit because audits generally measure past performance. But tech companies can give themselves a head start in preparing by prioritizing best practices and employing useful tools.

HIRING FOR AUDIT EXPERIENCE

Some tech startups are fortunate enough to have venture capital or private equity backers, who can lend previous audit experience to the growing business or may have founders that come with previous audit experience. But many do not have such support or may not have such experience. During early stages, tech startups may consider hiring consultants on an as-needed basis to provide the audit guidance needed. As they fill their leadership team, tech leaders should consider requiring key roles, like the CFO, CISO, to have audit experience. These professionals can help set the right tone at the top and take proactive steps toward audit readiness. They can also help companies avoid common pitfalls that they may otherwise overlook.

PROACTIVELY INVESTIGATING FUTURE REQUIREMENTS

Tech companies tend to grow and expand fast — adding new products or services or entering new markets to reach more customers. But that growth can also come with new laws, requirements, and stakeholder expectations. Companies may be subject to increasing requests to evaluate their controls and demonstrate compliance with new rules or standards. Leaders should prepare ahead to meet these demands by incorporating potential control updates into their strategic discussions around product, service, or location expansions.

CONDUCTING A READINESS ASSESSMENT

Companies that want to put their policies, procedures, or control environments to the test should consider enlisting a third party to conduct a readiness assessment. A readiness assessment is like an audit rehearsal, providing a snapshot of a company's current state. It can identify gaps in documentation, data security, or other areas — allowing the company to build a strategy that addresses its weaknesses or deficiencies.

PRIORITIZING COMPLIANCE BY DESIGN

Building tools and processes to be compliant from day one is both easier and cheaper than changing or retrofitting them later. Tech companies are increasingly recognizing the importance of incorporating data protection by design into their systems, products, and services. That awareness should extend to audit readiness, with a "compliance by design" mindset for process and controls by implementing "security by design," "privacy by design" approach. For example, companies should implement data governance best practices from the outset to ensure their data is clean, standardized, and accessible for when the time comes to seek an audit.

How BDO Can Help

Just because a company does not need a certain report right now, that doesn't mean it won't in the future. Getting the right attestation support early can empower companies to break down barriers to entry, opening the way to new markets and new customers.

BDO can help companies of all maturity levels assess and bolster their audit readiness and provide attestation experience that tech companies may lack in-house. We can work with less mature companies to educate them about the often year-long process of receiving valuable reports like SOC 1 or SOC 2. We can also support fast-growing companies, whose obligations can evolve just as quickly, by forecasting what reports they may need in the future.

CONTACT

HANK GALLIGAN
National Technology Industry Leader
hgalligan@bdo.com

BINITA PRADHAN
Third Party Attestation Principal
bpradhan@bdo.com

Whether you are a first-timer or already advanced in audit, BDO can help you prepare for your next assessment. **Contact us to learn more ▶**

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.