Beyond compliance: Navigating the critical choice for high-quality SOC audits

In today's rapidly evolving business environment, companies increasingly outsource critical technology and business operations to third-party service providers. While this enables companies to focus on mission-critical activities, it also amplifies the need for the robust third-party assurance and transparency that high-quality System and Organization Controls® (SOC)[1] reports provide.

SOC 1 and SOC 2 reports are globally recognized as vital tools that provide reasonable assurance that third parties maintain robust internal controls, support financial reporting integrity, and safeguard sensitive data.

Industry trends and audit quality

Multi-disciplinary public accounting firms have been the primary issuers of SOC-type reports since their introduction in the 1970s. Recently, however, there has been a growing presence of new entrants, including individual certified public accountants, offering these reports at high discounts. These newer entrants often lack the perspective of an established multi-disciplinary public accounting firm; a perspective developed through years of not only issuing these reports, but relying on them as the external auditor for public company financial statement audits.

This trend invites us to consider important questions about audit quality, depth of analysis, and the long-term implications for businesses that depend on these reports to effectively manage their third-party risks.

Obtaining a SOC report should never be merely a check the box compliance exercise. Instead – the selection of a SOC service auditor and the resulting report should be handled with diligence and as a mechanism to ensure quality governance and operations. Below we cover key elements to look for when choosing a service provider.

[1] System and Organization Controls and SOC are registered marks of the American Institute of Certified Public Accountants (AICPA), which reserves all rights.

The role of SOC reports

As defined by the American Institute of Certified Public Accountants (AICPA), SOC 1 reports are intended to provide assurance over a service organization's controls that are relevant to the user entity's internal control over financial reporting (ICFR), while SOC 2 reports focus on operational controls related to security, availability, processing integrity, confidentiality, and privacy.[2]

Organizations rely on SOC reports to gain insights into the control environment of their service providers and, in some cases, to determine whether they are willing to commence or continue doing business with a service provider. Financial auditors specifically rely on SOC reports for their financial statement audits, which highlights the important role a SOC report has in protecting the capital markets. Notably, with the rise of SaaS-based ERP systems, SOC 1 reports are often replacing the comprehensive risk assessment and testing financial auditors have performed over on-prem ERP systems. Both financial auditors and user organizations expect high-quality SOC reports that are comprehensive, supported by thorough testing, and backed by the credibility of the accounting firm.

Implications of low-quality SOC reports

For businesses that rely on SOC reports, the consequences of a low-quality report can be severe, including:

- Contractual Non-Compliance: Inadequate SOC reports may fail to identify and address critical gaps in controls, leading to compliance breaches and contractual penalties.
- Audit Challenges: User entity auditors may reject or require additional substantiation for SOC reports deemed unreliable, which increases audit costs and delays. When external audit firms decline to rely on SOC 1s due to quality issues, the organizations that provide these reports have to find alternative methods for providing assurance over their controls, which is a trend that is becoming more common in the market.
- Operational and Reputational Risks: Overreliance on inadequate SOC reports can leave businesses exposed to undetected risks, which, if realized, could damage customer trust, disrupt operations, and result in financial losses.
- Emerging Risks: An auditor with a checklist mentality may not identify changes, such as the introduction of AI, that require a thoughtful governance and controls response.

[2] SOC 2® - SOC for Service Organizations: Trust Services Criteria | AICPA & CIMA

Hallmarks of a high-quality report and what to consider when choosing an auditor

A SOC report is only as trustworthy as the firm that issues it. Key factors to consider include:

- Depth of Testing Procedures: Established public accounting firms often bring a multidisciplinary team with deep expertise in IT systems, financial controls, and contractual compliance. Newer entrants to the SOC market may rely more on standard checklists that could miss details that matter and may also lack the resources and experience needed for thorough testing of controls.

  One way to evaluate the depth of testing procedures is by reviewing the sufficiency and specificity of the tests described in Section 4 of the SOC report. Although most services provided by service organizations vary, some SOC service auditors will use generic language to describe their test procedures. This may indicate that the testing procedures performed by the SOC auditor are not in depth or accurately tailored. Additionally, tests performed by inspection or by re-performing a sample of transactions are generally more persuasive than tests performed via observation or inquiry. An overreliance on inquiry may indicate the auditor has not sufficiently verified controls and governance.

- Quality Control & Public Company Accounting Oversight Board (PCAOB) review experience: Some less mature organizations or sole proprietors do not have the same rigorous internal quality controls and peer review processes that are hallmarks of established firms, which increases the risk of inconsistencies, errors and omissions. Additionally, while the SOC standards are not currently under PCAOB oversight, firms that audit public companies are regulated by the PCAOB and follow their strict audit standards, and so they may be better attuned to their requirements. These requirements typically flow into the SOC firm's guidance, which results in higher quality SOC reports.[3]

- Experience of auditors: Established firms typically invest heavily in training, continuous professional development, and knowledge-sharing. Less mature organizations, by contrast, may rely on smaller teams with limited experience, especially when dealing with complex environments involving cloud computing, multi-vendor ecosystems and advanced cybersecurity measures. The emergence of AI and agentic systems also introduces new risks that a multi-disciplinary auditor with cutting-edge training and experience is better able to address.

Conclusion

As digital transformation and outsourcing become integral to business success, the reliance on SOC reports and the associated risks addressed by these reports are growing exponentially. Low quality SOC reports are at odds with this rising risk. Companies should prioritize quality and reputation over price when selecting SOC auditors. A vigilant, informed approach to SOC report quality—supported by engagement with reputable firms and thorough internal review—is essential for safeguarding organizational trust and resilience.

For more information on SOC reporting

The value of SOC reports in monitoring third-party risks

Click here to read ▶

Authors

Nina Currigan
Partner, Tech Assurance Audit
National SOC Solution Leader
T: 1 303 519 2190
E: ncurrigan@kpmg.com

Raghav Ahuja
Director,
Tech AssuranceAudit
T: 1 571 382 9809
E: rahuja@kpmg.com

Some or all of the services described herein may not be permissable for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**