The Value of SOC Reports in Monitoring Third-Party Risks

The proliferation of digital transformation and outsourcing increases the need for third-party assurance

Expansion of business process and system outsourcing continues to raise the need for third-party assurance. When outsourced processes and/or systems relate to internal controls over financial reporting, a SOC 1 report is a third-party assurance option that can provide transparency about the third-party's control environment. Alternatively, if security, availability, processing integrity, confidentiality, or privacy is a concern, a SOC 2 report can provide assurance over one or more of those areas. Now more than ever, SOC reports issued by reputable public accounting firms are paramount to effectively monitor and mitigate the unique risks that arise from digital transformation.

In the current environment, as digital transformation programs are accelerating, organizations are outsourcing entire business functions, rather than past practices when outsourcing was often limited to discrete pieces of an operation.

Consequently, financial reporting risks are evolving, and in some cases, increasing. The result is a need for more assurance from third parties to their customers in order to establish and maintain trust and provide transparency. That trust can be increased through a robust SOC 1 report that not only includes a description of how the outsource party is protecting client data and completely and accurately processing their transactions through the execution of controls, but also testing procedures executed by a public accounting firm to examine the design and operating effectiveness of those controls.

Erin Huston (Technology Assurance Principal), an IT audit specialist, suggests that it is essential to understand that "when a business outsources its processes, it is not outsourcing its responsibility to manage risks. However, we find that is how some businesses tend to think."

An in-depth review of a SOC 1 report is essential for a business to monitor the risks that exist in employing a third party. "Too often we learn they don't review the depth and scope of the SOC report, and they don't know enough about the SOC auditor's experience.Since a SOC 1 report is meant to support financial statement audits, organizations should request that their third-party vendors obtain SOC 1 reports from accounting firms experienced with performing public company financial statement audits," said Nina Currigan (Technology Assurance Partner). "Audit firms experienced with performing public company financial statement audits are uniquely positioned to ensure that a third-party vendor's SOC 1 report is going to meet the needs of their customers in depth, scope, and quality."

SOC 1 and SOC 2 reports are similar, yet distinct:

- SOC 1 reports are designed to report on controls that address risks associated with internal controls over financial reporting.
- SOC 2 reports are designed to report on controls that address risks associated with security, availability, processing integrity, confidentiality, or privacy.

This article focuses on SOC 1 reports.

Shared Responsibility Model

"Both companies and the service organizations to which they outsource processes should understand the shared responsibility model, which delineates each party's responsibilities for managing risks. A thorough understanding can help reduce the risk of deficient controls, which can jeopardize financial-reporting integrity, amongst other risks," said Akshit Khanna (Technology Assurance, System Implementation Assurance Principal).

As digital transformation expands and creates more outsourcing needs for businesses, a new landscape has evolved —multiple systems and processes shared among a business and its multiple service providers. A company should understand how its risk posture has changed when it outsources large scale operations by creating a shared responsibility model, which places higher emphasis on the concept of risk, a business's role in managing risk, as well as the business's understanding of the expectations of its service providers.

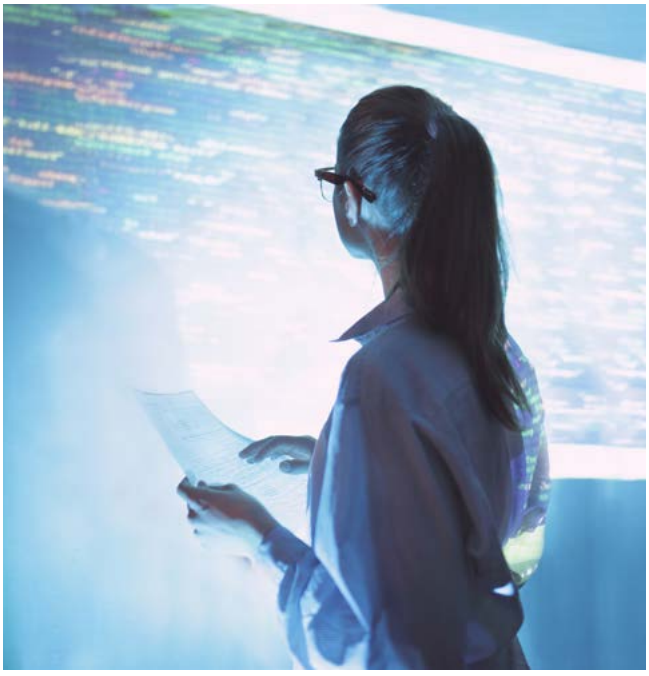
At KPMG our technology assurance specialists routinely witness situations where financial reporting risks have escalated because key individuals in a business do not have a clear view of the extent of the business's third-party outsourcing. Some individuals may know their organization's ERP system has been moved to the cloud, but they may not know if all or parts are with one third party or several of them. In some cases, they may not even know the identity of the third parties.

It is critical for businesses to inventory all third parties they use, and obtain and review SOC 1 reports from each of those third parties to ensure they provide sufficient details of the effectiveness of controls that address financial reporting risks. The review of SOC 1 reports is essential to effectively monitor risks and evaluate compliance with regulations.

Key SOC 1 Risks and Suggested Action Steps

Keep in mind that there are several straightforward ways by which companies can gain comfort that vendors are effectively managing their risks. Our suggestions include identifying these risks and considering these action steps:

- Companies that receive SOC 1 reports from organizations to which they've outsourced business processing and systems may have inadequate communications and training programs that can help identify financial reporting risks associated with outsourcing. Consequently, it is critical for those companies to raise awareness inside the business through regular communication and training about how to review SOC 1 reports and identify risks, controls, and reporting complexities created by digital transformation programs.
- While it is essential to establish a Vendor Risk Management program inside the business to review SOC 1 reports, knowing which people to populate it could be a challenge for some businesses. We suggest that a team should comprise people from such areas as internal audit, procurement, legal, information technology, finance, regulatory reporting, and others.



- Clarity about the potential risks contained in a SOC 1 report often can be elusive, which is a key reason to establish rigorous review practices that identify and address potential risks. Make it a common practice to ask penetrating questions that require detailed and clear answers from third parties, and the SOC 1 audit firm, if necessary, about statements and conclusions contained in the reports.
- A vulnerability we often see is that the people responsible for reviewing their company's outsourcing risk profile do not know the identity of all third parties doing business with their company. Making certain that individuals who have responsibilities to manage Vendor Risk Management programs have broad knowledge of all third-party relationships therefore is a must. They need to know about all outsourced services/functions/processes, which third parties are doing the work, understand how SOC 1 reports are used, and how to read SOC 1 reports.
- Last-minute requests for a review of a SOC 1 report by a company's internal audit team should be avoided. It is a good practice to set up schedules with lead-times that alert the internal audit department about pending reviews of SOC 1 reports. Such a practice can help with a thorough examination of the description of the test procedures performed by the SOC 1 auditor that can determine whether procedures align with how internal audit would test those controls.

Documentation and thorough testing of controls are the foundation of an effective SOC 1 report, providing a sense of affirmation to a business that its data—and data of its clients—is controlled, and that the processes employed by a third party are producing complete and accurate information relevant to financial reporting.

Further a SOC 1 report can be a valuable tool for third parties to establish trust with their customers. It requires third parties to build a program of responsibilities across functions. Companies are using outsourcing more heavily now than ever, raising the stakes, and the bar, for both the companies that outsource their critical business processes and systems, as well as the third parties to which they outsource.

Authors

Nina Currigan
Partner, Technology Assurance Audit
T: 303-382-7808
E: ncurrigan@kpmg.com

Akshit Khanna
Principal, Technology Assurance Audit
T: 617-988-5984
E: akshitkhanna@kpmg.com

Erin Huston
Principal, Technology Assurance Audit
T: 480-459-3607
E: ehuston@kpmg.com

Learn about us: **kpmg.com**