Vendor Controls Assurance (SOC 2+)

A cost effective approach to building customer trust

PwC presents a new assurance solution which is designed to meet the increasing needs of managing third party risks, saving vendors and their customers time and money in achieving controls assurance over vendor operations.

pwc

The need for enhanced reporting on vendor risk management – The driver for SOC 2+

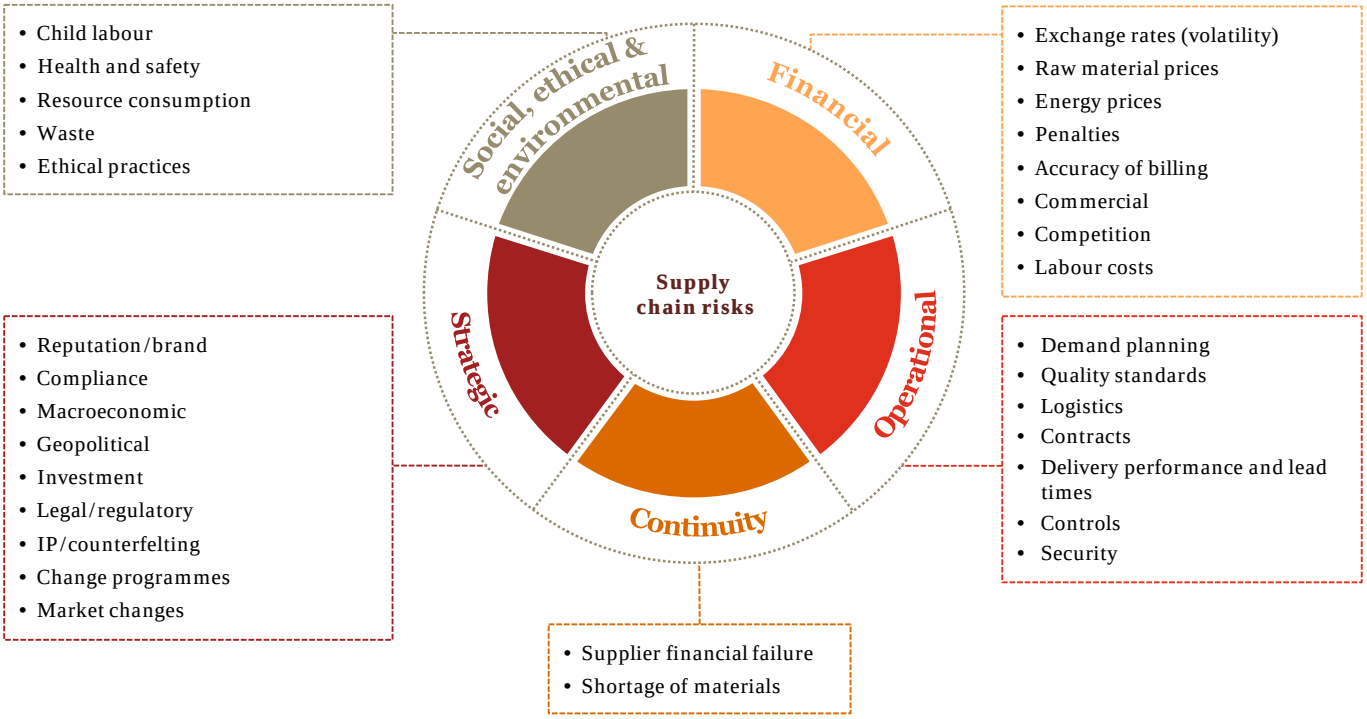
Spotlight on the current outsourcing environment

Today's service economy has put third party vendors front and center. By 2017, the US business-process outsourcing market is expected to be 23.3% larger than it was in 2012[1].

It's no secret outsourcing can reduce costs and increase business agility. Thanks to the data hosting, cloud, and business-process services of vendors, companies can redirect in-house resources back to the business and focus on core competencies.

Of course, employing third party vendors opens a company to additional risks, ranging from data errors to supply chain disruptions. Outsourcing arrangements can also involve multiple supplier relationships that are invisible to the end client, giving rise to additional risk exposures.

Key risks faced by vendors and customers from outsourcing arrangements



Despite these risks, vendors are enjoying a strong demand for their services. However, they are experiencing more stringent oversight from customers and increasing requests for on-site audits and other assessments, based on risk management and regulatory requirements. The increased time required to oversee outsourced arrangements diverts valuable resources away from running the business and these efforts may only yield a limited level of comfort that financial, operational, and reputational risks are being mitigated.

[1] Source: IDC, *Worldwide and U.S. Business Process Outsourcing Services 2013-2017 Forecast*, May 2013, and PwC analysis.

Meanwhile, regulators including the Federal Reserve, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau are casting a watchful eye on vendors and their customers, driving the need for a more effective and efficient solution to providing assurance over vendor operations.

The risks of outsourcing can be significant, and proper management of these risks calls for an independent, efficient, and effective approach to provide assurance over vendor operations.

Why the current approach to achieving assurance over vendor operations is no longer sufficient

Many vendors are receiving multiple and varied questionnaires from a significant number (hundreds, in some cases) of customers, at unpredictable times, which can significantly strain resources and may result in an inconsistent level of quality in their responses. To meet the demand, vendors are finding themselves investing additional time and resources. PwC estimates that the cost to respond to the various questionnaires and inquiries from customers can cost vendors in excess of $5m annually, while also taking core resources away from delivering on the core competency of the company.

Some vendors have tried using SOC (Service Organization Controls) 1 or 2 reports to respond to questionnaires but have found them inadequate as they don't sufficiently cover the areas of interest to the customers.

On-site assessments performed by customers also seem deficient because they are performed at a specific point in time, and fail to provide an overall view of a vendor's operations or environment.

All-in-all, the current environment is one where both service providers and customers are investing significant time and effort, and neither one is reaping the full benefits of reliable controls assurance.

Vendors are seeking a way to take control of this challenging situation: to find cost-effective, consistent, and controllable ways to give their customers the assurance they need while maintaining their ability to conduct business as usual without disruption.

The vendor questionnaire approach diverts both time and money away from existing operations and does not provide assurance. In addition, the SOC 1 and 2 reports do not always provide customers with the required level of comfort.

A better solution on controls assurance

Recognizing this growing need, PwC has developed a time-saving framework that alleviates much of the burden on vendors while giving customers the assurances they seek. This framework has been led by PwC, and developed in collaboration with other professional services firms to create a framework accepted by the industry.

PwC's Vendor Controls Attestation Report (SOC 2+), a report built upon AICPA SOC 2 reporting principles, allows an independent, standardized assessment to be performed over vendor operations and eliminates the need for the time consuming and costly vendor questionnaire process. The report format is similar to SOC 1 and SOC 2 reports, making it easy for both vendors and their customers to digest. In addition to the principles covered in SOC 2 reports (security, availability and confidentiality), the SOC 2+ report includes additional principles that meet the unique assurance needs of a vendor's customers. Put simply, a SOC 2+ report provides the necessary level of assurance and can help restore a customer's confidence in vendor processes, which in turn will increase customer satisfaction and preserve valuable vendor/customer relationships.

Benefits to vendors include:

- Reduced time and money spent on resources dedicated to the vendor questionnaire process.
- More time to proactively address risks and deliver value to customers.
- A decrease in the number of on-site audits.
- Enhanced vendor marketability as the report can be used to differentiate a vendor from its peers.
- A greater understanding of expectations and what vendors are being measured against, regardless of the customer.

Benefits to customers include:

- A greater level of assurance over vendors operations (positive assurance).
- Savings associated with the reduction in the need to perform on-site visits.
- Savings associated with not having to create questionnaires, or having to evaluate inconsistent reports, with varying criteria from vendors.

In short, the Attestation Report gives vendors a measure of control over the timing, content and cost of reporting, and delivers a consistent, uniform response to the demands of their customers.

What are the components of the SOC 2+ report?

The SOC 2+ report contains:

- A written assertion by management regarding the description of the system and the suitability of the design and operating effectiveness of controls in meeting the applicable Trust Services Criteria and other customized criteria aligned to the vendor services.
- A type 1 report includes a service auditor's opinion on the fairness of the presentation of the description of the system and the suitability of the design of the controls to meet the applicable criteria.
- In a type 2 report, in addition to what is included in a type 1 report, the operating effectiveness of those controls is also reflected as well as a description of the service auditor's tests of controls and the results of the tests.

The SOC 2+ report can be distributed to existing customers/users and may be used to address the following:

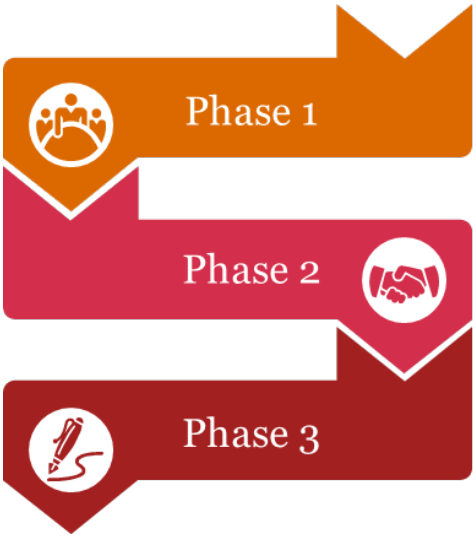
- Oversight of the service organization (e.g. vendor management program)
- Internal corporate governance, risk management and compliance processes
- Regulatory oversight

Executing the engagement

When planning to issue a SOC 2+ report, we recommend a "phased approach" from readiness to ultimately executing a SOC 2+ engagement. Taking a phased approach to obtaining a SOC 2+ report will help to:

- Define the reporting needs and expectations of your customers,
- Identify and assess controls,
- Pave the way for an efficient SOC 2+ engagement, and
- Address potential control gaps prior to reporting to customers.

While the service auditor can assist in any or all of these phases, the typical progression of phases an organization goes through is as follows:



Readiness: A readiness assessment is performed including identification of key customers and definition of relevant scope and approach. A Health Check on the vendors control environment is conducted, prior to performing a formal assessment.

Remediation: Management performs remediation activities to rectify control weaknesses identified during the readiness phase, to assist in becoming SOC 2+ ready.

SOC 2+ Assessment execution: A SOC 2+ assessment is performed and an opinion on the vendor's control environment is executed by the service auditor.

What's next

Determining whether a SOC 2+ report is the right fit for your company

When deciding whether a SOC 2+ report is most appropriate for your company, some questions to consider are:

For vendors:

- How many customers ask you to complete their vendor risk annual questionnaires? How much time, effort, and cost is put into answering vendor risk annual questionnaires?
- Do your customers obtain the required comfort from the questionnaire responses and/or from other control reports provided (such as SOC 1 and 2 reports) or are there gaps in coverage?
- Do you have on-site audits performed by customers, impacting your resource time and availability?
- How much internal time do you spend on managing vendor risk management processes relating to satisfying your customer inquiries/questionnaires and/or on-site audits?

For customers:

- Are you receiving adequate comfort over the management of key risks from your vendors?
- Are you obtaining sufficient comfort from completed vendor questionnaires?
- How much time, effort, and cost are you spending on developing vendor questionnaires and following up on remediation activity?
- Are on-site audits costing you unnecessary time and effort, and only providing comfort to you at a point in time?

Contacts

Adopting a SOC 2+ approach to vendor risk management eases the pressure on vendors and their customers. Both can return their focus to their organization's core business. Both can reap significant savings in time, expense, and human resources.

For a deeper discussion of Vendor Controls Attestation, contact:

Jeff Trent

Vendor Controls Attestation Leader
Tel: (646) 471-7343
jeff.s.trent@us.pwc.com

Julianne Inozemcev

Risk Assurance Partner
Tel: (617) 530-5119
julianne.inozemcev@us.pwc.com

Igor Maryams

Risk Assurance Director
Tel: (646) 471-2766
igor.maryams@us.pwc.com

Shona Brady

Risk Assurance Director
Tel: (646) 471-7118
shona.e.brady@us.pwc.com