Vendor Controls Reporting: SOC 2+

A cost effective approach to building customers' trust

pwc

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

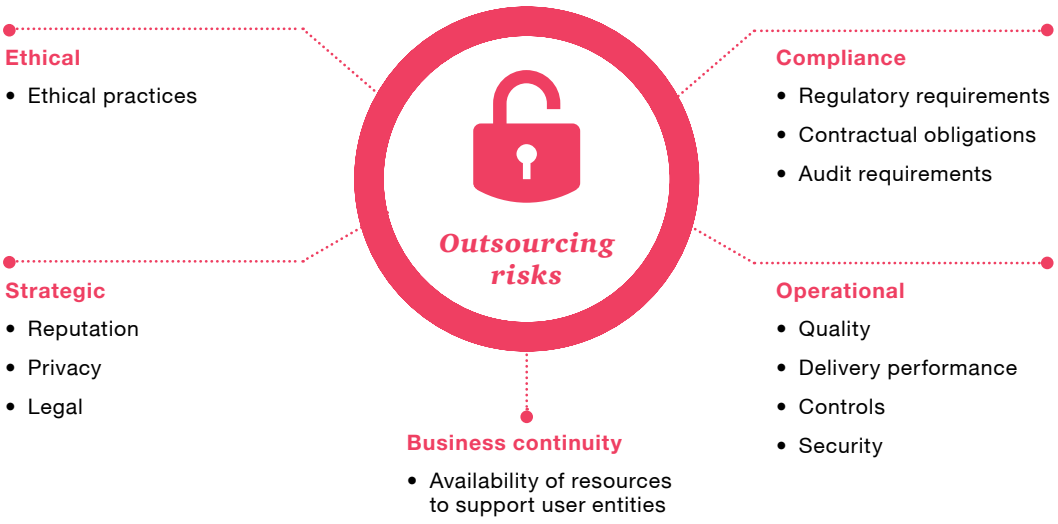
Spotlight on the current outsourcing environment

Today's service economy has put outsourcing and service organisations front and centre. From 2010 to 2016, the size of the Asia Pacific region business process outsourcing market has increased by 74.04%[1] and China is the second preferred offshoring destination worldwide[2] . China's growing back-office service offerings to the US and UK and near-shore markets of Japan and South Korea amount to about 4% of the global offshore business process outsourcing (BPO) market, and we expect this figure will continue to grow.

It's no secret outsourcing can reduce costs and increase business agility. Furthermore, thanks to the data hosting, cloud, and business-process services of vendors and the upscaling of their people, the word outsourcing far from conjures up images of call centres in faraway lands; rather, outsourcing is increasingly showing its potential to provide value to the business and boost the overall economics of the company. The more complex and up the value chain the outsourcing arrangements are, the more careful the consideration needed on the risks associated when a third party is responsible for running a part of the business and how therefore the risks are mitigated and control is yet maintained. For service organisations, in order to maintain and grow their BPO business, it is vital to demonstrate the risks are managed and controls are at par to those at the user entity, if not better.

An independent report over internal controls, being those relating to internal controls over financial reporting (SOC 1) or reports focusing on operational and compliance controls (SOC 2 and SOC 3) can sometimes still be somewhat limited.

Key risks faced by vendors and customers from outsourcing arrangements



1 IDC Worldwide BPO Services Revenue by Region, 2005-2016, April 2012 and PwC analysis
2 A.T. Kerney 2016 Global Services Location Index (GSLI), January 2016

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.

Meanwhile, regulators including the HKMA 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.

What are the current challenges service organisations are facing?

Many vendors are receiving multiple and varied requests for reporting on their control environment from a significant number (hundreds, in some cases) of customers, at unpredictable times and mostly in the form of questionnaires that can range from 40 to 800 questions. 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 Organisation 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. 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 costeffective, consistent, and controllable ways to give their customers the assurance they need while maintaining their ability to conduct business as usual without disruption. PwC has developed a framework to help service organisations respond to multiple requests from customers as well as save them, and their customers, time and money. PwC's Vendor Controls Attestation Report (SOC 2+), is a report built upon AICPA SOC (Statement of Controls) 2 reporting principles that allows an independent, standardised assessment to be performed over vendor operations to eliminate or reduce the time needed today.

In addition to the most commonly used principles covered in SOC 2 reports (security, availability and confidentiality), the SOC 2+report also provides coverage on additional principles and criteria based on the specific assurance requirements of customers.

In short, the SOC 2+ 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.

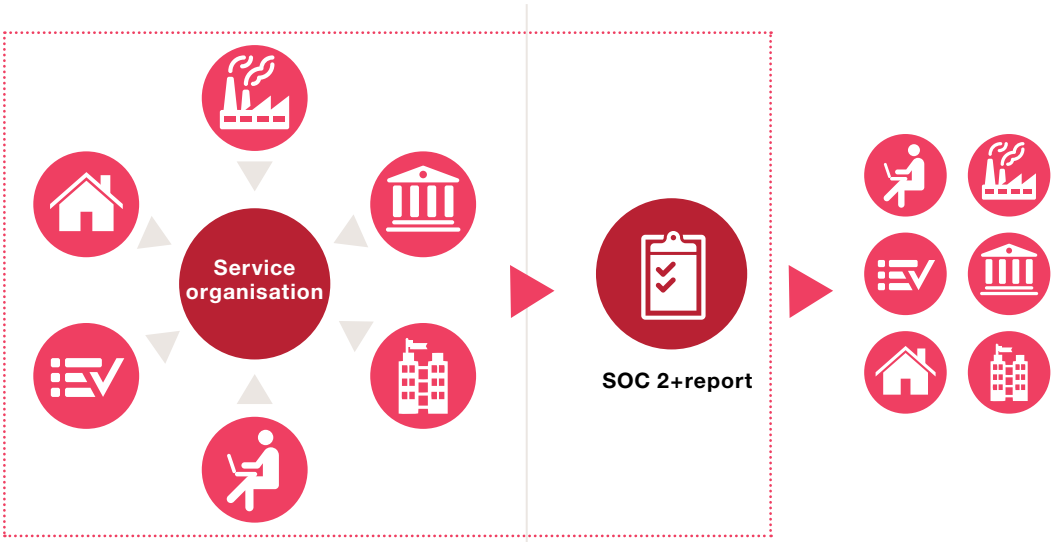
SOC 2 + benefits

Potential benefits to customers

- Reduces time and money spent on resources and travel;
- Helps restore confidence;
- Provides positive assurance;
- Independent third party performs an attestation.

Potential benefits to vendors

- Reduces time and money spent on resources;
- Can be used as a differentiator from peers, enhancing vendor marketability;
- Offers more time to proactively address risks;
- Improves management of costs;
- Decreases the number of on-site audits.



Multiple requests from regulators, auditors and customers with different objectives and requirements

One report addressing key requirements (regulatory and commercial) relevant to all users

Key considerations

Determining whether a SOC 2 + 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?

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?

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?

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?

Executing the engagement

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 customised 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 organisation (e.g. vendor management programme)
- Internal corporate governance, risk management and compliance processes
- Regulatory oversight

The approach

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 organisation goes through is as follows:

Phase 1

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.

Phase 2

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

Phase 3

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

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 organisation's core business. Both can reap significant savings in time, expense, and human resources.

To have a deeper conversation on SOC 2+ reporting contact:

Nick Hamer

Third Party Trust China and Hong Kong Leader
+852 2289 8545
nick.j.hamer@hk.pwc.com

Aileen Wang

Partner, Shanghai
+86 (21) 2323 6655
aileen.wang@cn.pwc.com

Albert Lam

Partner, Beijing
+86 (10) 6533 7923
albert.t.lam@cn.pwc.com

www.pwchk.com