Deloitte.

Managing Risk from Every Direction

Take control of third-party risk with third-party assurance reporting

Content

How do companies today manage all of the risks associated with using third-party vendors? It's a balancing act. As an Outsourced Service Provider (OSP), it's critical to know what risks may affect your clients — and the best ways to manage those risks — to ensure you are meeting your clients' control needs and requirements.

As a user of outsourced services, it's critical to manage any potential risk to your company and to have proper assurances that your vendors have a well-established internal control framework that is operating effectively.
When you feel like risk is coming at you from every direction, a well-planned third-party assurance program can help provide the control you need.

Third-Party Assurance

Although many organizations have been outsourcing core and non-core services to a third party for years now, outsourcing is still becoming more popular by day and is playing a vital role in helping companies increase their efficiency and profitability. Examples of such outsourced services include payroll services, cloud computing, managed security, health care claims management and processing, asset management etc.

As OSPs are becoming more integrated with their clients' day-to-day operations, they can have more of an impact on their clients' internal control framework, including their financial reporting and compliance requirements.

This increased reliance on OSPs — and the critical role that they can play in their clients' business — has led to an increase in demand for service auditor reports.

A strategic view of outsourcing

It's important for companies to take a high level look, or a strategic view, at their existing outsourcing programs and vendors. This strategic overview should help companies identify potential issues and be better equipped to take advantage of available third-party assurance programs, including third party reporting.

The strategic view of outsourcing is generally comprised of three distinct views — global, risk, and industry views — and can help companies anticipate and mitigate the variety of risks that come with using third-party vendors associated with existing outsourcing programs.

Global view of outsourcing

Today, the reasons for outsourcing extend far beyond Information Technology (IT) processing or the need to find the lowest-cost alternative to in-house operations. Companies are seeking cost and competitive advantages by outsourcing at global levels, as the need for OSPs has evolved over the years from single process outsourcers and hosts to providers of fully integrated cross-border solutions. With global integration comes an added layer of risk — how does a company understand and evaluate OSP risk from a global perspective? Implementing globally-accepted reporting standards and controls can help OSPs provide the assurances that their customers expect.

You can outsource a process, but you can't outsource the risk…

Risk view of outsourcing

It is important for companies to be aware of all of the risks that may be typically associated with outsourcing, including, but not limited to reputational, control, compliance, privacy, financial, and operational risks. Outsourcing any component of a company's business to a service organization can introduce any or all of these risks — either directly or indirectly. Direct risks are typically associated with the actual processing or hosting of data. Indirect risks, which can be equally as critical, are normally associated with how the data is managed (or mismanaged) and the clients' perception of the relationship between the provider and users of outsourced services. To effectively manage these risks, executives rely on specific reports (see the "Service auditor reporting options" section on page 5) from their service organizations.

Industry view of outsourcing

Outsourcing practices and controls are unique to each industry and as the awareness of vendor risk management has increased across industries, the role of third-party assurance has become more important than ever.

Compliance with industry, government, and other regulations has become more challenging as companies manage increasingly complex reporting requirements. At the same time, many companies are vying for new business and demanding that their OSPs meet certain requirements as a condition of their outsourcing relationship.

A robust control and assurance program, tailored and integrated to address specific industry standards including the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Payment Card Industry (PCI) Data Security Standard, to name a few, can help provide companies with the industry perspective that they need.

Once the company has compiled their strategic view of outsourcing — and identified areas of potential risk to the organization — they can establish a plan to begin managing risk from these different directions. Attestation reporting is the first but vital step in the right direction.

Background of service auditor reporting

A service auditor report

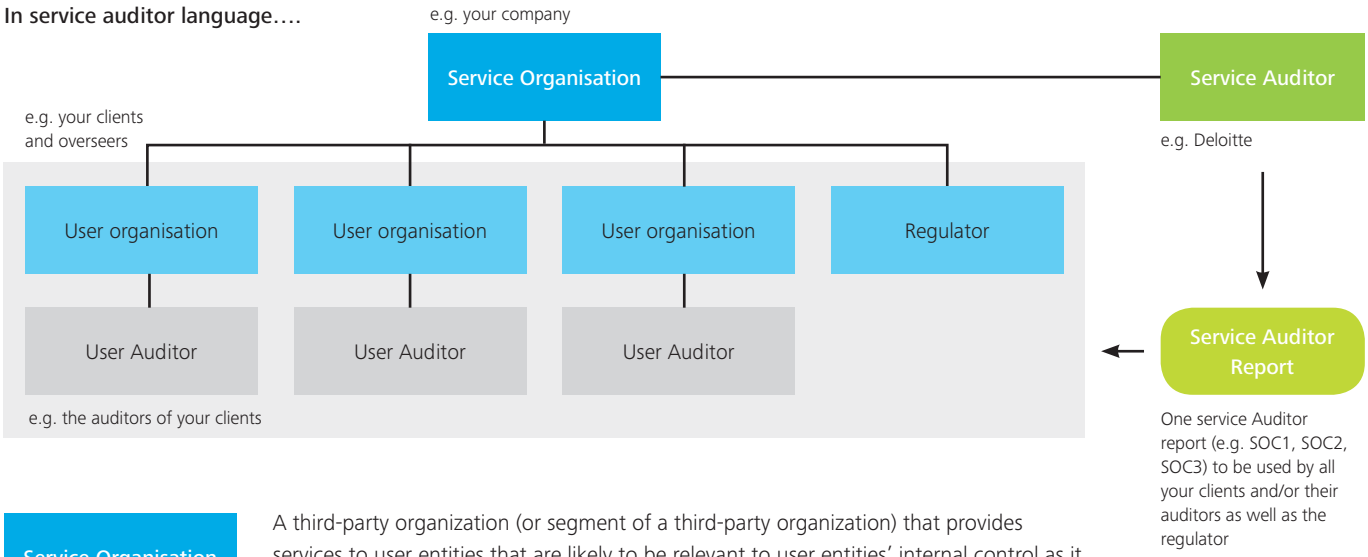
As mentioned on the previous page, outsourcing any component of a companies' business introduces certain risks. As a consequence, the use of outsourcing requires companies to better manage their risks associated with the outsourced services. Specifically, the outsourcing companies (user organization) requires a degree of assurance that the service provider has a well-established internal control framework, that is suitably designed and operating effectively.

One of the most effective ways a service organization can communicate information about its risk management and controls is through a service auditor report (e.g. ISAE3402, SSAE16 (SOC1), ISAE3000, SOC2, and SOC3).

The purpose of such a service auditor report is to provide clients and/or their auditors with an objective report that expresses an opinion about the control environment of a service organization (i.e. provider of services). The result is an independent and objective opinion about a standardized set of service objectives that are tested only once to minimize business disruption.

User organizations that obtain a service auditor report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls. The user organization receives a detailed description of the service organization's controls as well as an independent assessment of whether the controls were placed in operation, suitably designed and/or operating effectively.

In service auditor language….



Service Organisation — A third-party organization (or segment of a third-party organization) that provides services to user entities that are likely to be relevant to user entities' internal control as it relates to financial reporting.

Service Auditor — A professional accountant in public practice who, at the request of the service organization, provides an assurance report on controls at a service organization e.g. Deloitte.

User organisation — The entity that has traditionally engaged a service organization to perform services for them that are considered a part of the user organization's "System" e.g. your clients.

User Auditor — The auditor that conducts the financial statement audit on the user organization - these auditors rely heavily on audits from service organizations in helping plan and prepare for the user organization's annual financial statement audit, specifically the auditors of your clients.

Benefits of service auditor reporting

Third-party attestation reporting provides a range of benefits for users and providers of outsourced services.

User benefits include

- Ensuring that the expectations of the third-party vendor relationship are met
- Ensuring that the company's multi-purpose reporting requirements — including operational and financial — are met
- Valuable information- independent assessment of whether the controls of the service organization were in place, suitably designed and operating effectively.
- Cost savings- avoiding additional costs in sending the auditors of the user entity to the service organization to perform their procedures.
- Maintaining compliance with industry, governmental and other relevant regulatory requirements.

Provider benefits include

- Commercial advantage – a method to differentiate a service organization from its peers/competitors.
- Cost savings- providing reports issued by the service auditor rather than customer audits – savings on answering questionnaires.
- Broad assurance – provides reasonable assurance to a broad range of clients with a single report.
- Compliance requirements- demonstrates to regulatory bodies that controls are in place and operating effectively.
- Improve overall control awareness- generates increased awareness within the organization of the importance of controls and embeds a strong control culture.

Service auditor reporting options

Leading edge professional service organizations understand the challenges that integrated, outsourcing relationships can present. These organizations can help their clients effectively and efficiently meet existing and growing demands for third-party assurance reporting by incorporating multiple views — global, risk, compliance, industry, and customer views — into their approach. As indicated in the following table, most professional service organizations offer a range of third-party assurance reporting services including Service Organization Control (SOC) 1, 2 and 3 reports, ISAE3402, ISAE3000, Agreed-Upon Procedures (AUP) and readiness assessments.

The International Auditing and Assurance Standards Board (IAASB), which is part of the International Federation of Accountants (IFAC) created the International Standard for Assurance Engagements reporting framework (ISAE) – ISAE 3402 and ISAE 3000 – covering controls over services provided by organizations with the intent to: (1) address various needs and reporting requirements by service organizations, and (2) provide valuable information to address user needs, including risk assessment related to outsourcing. Similar to the ISAE standards, American Institute of Certified Public Accountants (AICPA)'s has created the Service Organization Control (SOC) reporting framework.

	ISAE3402 - SOC 1	SOC2	ISAE 3000	SOC 3
Purpose	Report on controls over a service organization that may be relevant for to user entities' internal controls over financial reporting.	Report on non-financial processing based on one or more of the Trust Service criteria on security, availability, privacy, confidentiality and processing integrity.	Report on non-financial processing based on one or more of the Trust Service criteria on security, availability, privacy, confidentiality and processing integrity.	Report on non-financial processing based on one or more of the Trust Service criteria on security, availability, privacy, confidentiality and processing integrity.
Scope	Services and processes covered in the report are defined by the management of the service organization.	Consist of 1 or more of Trust Service criteria on security, availability, confidentiality, processing integrity and privacy. For each domain principles and controls are predefined.	Consist of 1 or more criteria defined by the management of the organization, or embodied in law or regulation…	Services and processes covered in the report are defined by the management of the service organization.
Report Layout	Service auditor's opinion on fairness of the presentation of the description of the system of suitability of design and implementation of controls; and operating effectiveness of controls, including test of controls and related test results).			No report other than a summary statement that can be distributed to anyone.
Standards	ISAE3402 SSAE16	AT 101	ISAE3000	AT 101
Types	Type I & Type II	Type I & Type II		Type II
Intended users	Distribution restricted to the users of the services and their auditors.	Distribution restricted to the users of the services, their auditors and specified parties (e.g. prospects).	Distribution restricted to the users of the services, their auditors and specified parties (e.g. prospects)	Distribution to anyone.

Service auditor reporting – steps to consider

Which Service auditor report is appropriate for you?

Service organizations should understand the needs of their clients and select the reporting option that best suits client needs. Management should consider the following:

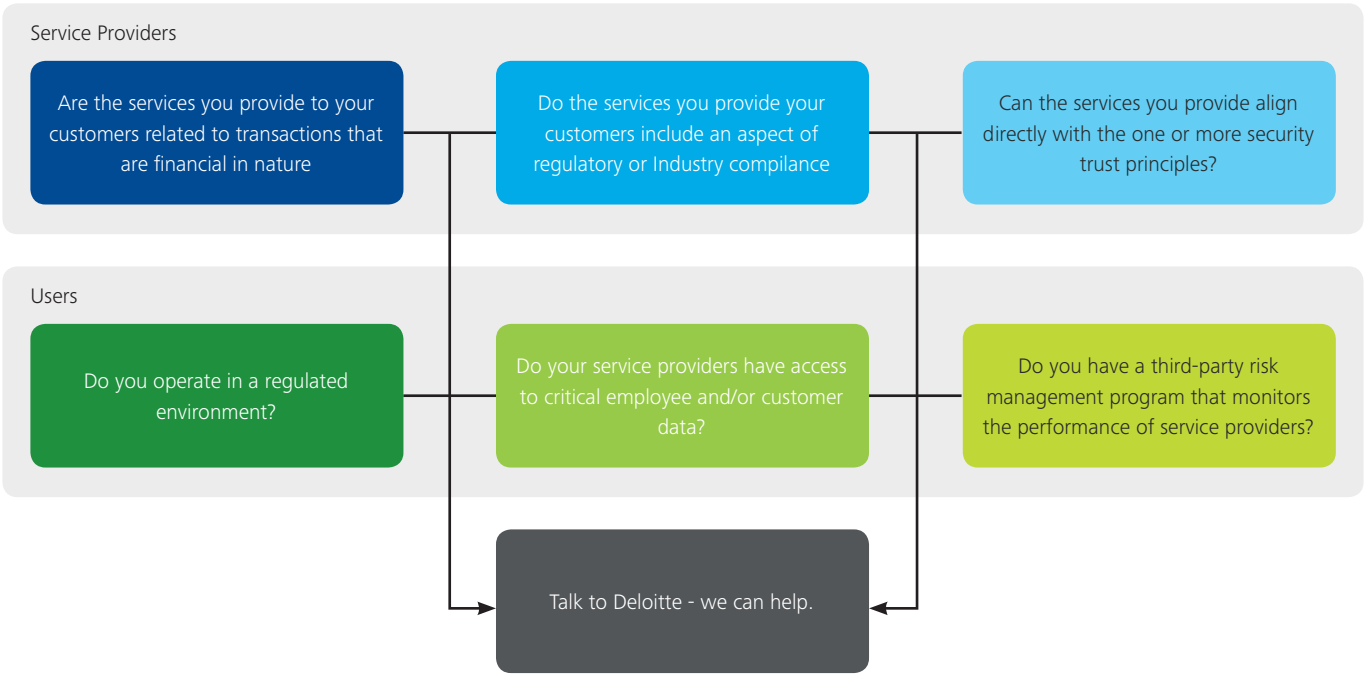
What is the intended user of the report?

- Are users focused on internal control over financial reporting?
- Are key compliance and operational controls such as those related to security, availability, processing integrity, confidentiality or privacy of primary interest?

Level of information related to your systems and processes?

- Are users in need of details related to systems, processes and controls?
- Will the posting of a summary report or seal suffice

Below are some questions that service providers and users of third-party services should consider when determining their options when it comes to selecting the most relevant solution for third-party attestation reports:



Answers to FAQs related to service auditor reporting

Given the similarities between ISAE3402 (SOC1) and ISAE3000 or SOC2 reports, how can the ISAE3000 and SOC2 help service organizations?

Customer/User Needs – We often see service organizations being asked by their users for assurance related to areas/controls, not directly related to user's financial statements. SOC2 was created with the intent that it would enable organizations, such as cloud computing vendors or managed services vendors to demonstrate that their controls are sound and they are meeting a third party standard.

Potentially decrease the number of individual audits that your organization undergoes – Even with ISAE3402 or SSAE16 (SOC1), many organizations still needed to accommodate individual audits for significant customers. This is particularly true in certain industries such as data center hosting, credit and payments transaction processing and cloud based computing providers. ISAE3000 or SOC2 offers the potential to rationalize the number and extent of these individual audits by providing more in-depth reporting around areas of critical concern.

Meeting regulatory and other industry requirements – With the evolution of businesses today, including the drive for greater technology sophistication, regulators, industry groups and users are demanding more transparency from their service providers. An ISAE3000 or SOC2 report can assist with meeting several regulatory requirements, while also demonstrating competitiveness with the industry and satisfying customer demand.

What are the benefits of a SOC3 report over a SOC report?
SOC3 reports are designed to meet the needs of users who want assurance on controls at a service organization related to the AICPA's Trust Service Principles and Criteria, but where the detailed report is not needed. However, there can't be any carved out sub service providers, nor can there be any significant user control consideration in order to receive an unqualified opinion.

Conclusion

The outsourcing of key components of a business — in order to meet cost, competitive, and operational demands — has become a strategic imperative within many industries. A multidirectional approach is required to manage these complex relationships because of the global nature, risks, and industry regulations associated with outsourcing. Third-party assurance reporting can help OSPs clearly define, assess, and communicate their approach to their clients.

Since the circumstances around each OSP relationship are unique, a leading OSP process leverages a tailored reporting approach that uses multiple reporting methods. By taking the necessary steps to identify the need for third-party assurance reporting and the appropriate reporting type, the OSP (and the associated users) will help ensure that their risk and compliance needs are addressed. Anticipating and managing these multiple risks is vital to effective third-party relationships.

About the authors

Johan van Grieken
Partner
Deloitte & Touche LLP
+32 2 800 2453
jovangrieken@deloitte.com

Johan is leading the IT Risk Consulting team in Belgium. He has specialized in the risks of Governance, Continuity, Quality and Sourcing. He leads Consulting and Assurance missions, helping clients to connect business and ICT and to manage the related risks. This expertise is built on a strong operational and financial foundation gained as consultant, interim IT manager and IT auditor. Johan has a broad view on ICT-related projects and easily links up with financial and business processes.

Bert Truyman
Director
Deloitte & Touche LLP
+32 2 800 23 20
btruyman@deloitte.com

Bert is leading the ICT Audit and Assurance group in Belgium which provides ICT (internal) Audit, Third party assurance (e.g. ISAE 3402, SOC 2), Risk & Controls, and compliance services. He has specialized in providing (IT) assurance and advisory services with respect to strategic and operational risk management, (IT) governance, information security and outsourcing. Bert has been active as auditor and advisor in various industries, and has a specific focus on the financial services industry.

3559