Getting the right fit on service organization/provider controls reporting

The one-size-fits-all approach of a SAS 70 report no longer meets the needs of today's service organizations and their users

At a glance

With the transition from SAS 70, now is the time to take a fresh look at business needs and customer needs to determine what form of reporting is best for your organization.

A number of new report options exist—all rooted in the same base standard, AT 101.

Highlighting the changing needs of service organizations and their customers for controls comfort, the AICPA created a reporting framework to address emerging outsourcing concerns related to issues such as privacy, security, and availability.

pwc

Introduction

It would be difficult to find a company today that does not hire vendors to perform part of its daily business operations. Outsourcing, to save costs and for a variety of other reasons, has long been the world's business norm. But today's world is changed. Amid a rise in emerging technologies such as cloud computing and social networking, the focus is on availability, security, and privacy. And as businesses become more interconnected, demands for trust and transparency are expected to grow.

SAS 70 sunset

Most everyone in the business world has heard of a SAS 70 report. For years, the report was the predominant standard and de facto trademark for internal controls over financial reporting at service organizations. Although designed as auditor-to-auditor communication with a focus on internal controls related to financial reporting, over time the role and scope of the SAS 70 report became distorted within the marketplace. It was not uncommon for service providers to tout that they were "SAS 70 certified" or had "passed the SAS 70" when in fact, neither assertion was true. Simply put, SAS 70 is not a certification or a test.

It was also common for organizations to believe that receipt of a SAS 70 report from their service organization would address their control concerns, such as needs for privacy and availability, as well as providing transparency on business areas outside of financial reporting. In reality, a SAS 70 report covered only areas specific to the processing of financial transactions and was not designed to cover this broader set of issues.

In June 2011, the SAS 70 standard will go away. Its sunset will provide service organizations and users a fresh opportunity to evaluate which controls reporting option is the right fit over these non-financial business issues.

Finding comfort in service provider internal controls

Outsourcing today includes core functions of business operations and strategy—not just routine back-office tasks. Outsourcing has become especially popular for processes that are complex, time intensive, fully customized, and that require specialized knowledge of systems and regulations. For example, organizations that rely on the latest information technology to remain competitive might hire a vendor to stay ahead of the innovation curve. Even startup companies engage in outsourcing as a way to focus on the things they do best while letting someone else handle processes such as system hosting and back-office recordkeeping.

Businesses are inundated with demands from their trading partners and vendors for increased transparency into their operations. In addition to staying ahead of Sarbanes-Oxley (SOX), service organizations and users must meet other compliance or regulatory reporting requirements.

Organizations also seek comfort over the activities of interconnected business partners outside the traditional service organization and contractual outsourcing arrangements. In the investment marketplace, the need for increased investor trust and transparency has reached new levels since the 2008 financial crisis began. Increasing regulatory and public watchdog oversight of such diverse areas as the sourcing of raw materials, health and safety practices, executive compensation, and data protection practices are also driving organizations to be more transparent when dealing with regulators and other stakeholders. Increasingly, business partners and vendors are demanding more disclosure and transparency related to issues such as corporate social responsibility, sustainability, privacy, and business operations. In short, even without a formal contractual agreement, organizations are faced with providing a higher degree of transparency to their various stakeholders covering these emerging business practices and processes.

Meanwhile, as the use of cloud computing and social networking technology becomes more popular, companies must contend with myriad privacy and security issues, which go beyond financial reporting. It's one thing to stay ahead of possible financial and operational internal controls gaps in one or two vendors, but what if your company contracts for services with several providers employing a mixture of existing and emerging technologies?

Simply put, businesses and their stakeholders may ask: How can I bridge the gap between a report on financial reporting controls (the traditional SAS 70) and my need to cover a broader set of business, commercial, and regulatory risks?

Enter AT 101 and service organization control (SOC) reports

For service organizations and their users, the marketplace is flooded with acronyms related to controls reporting. Despite the apparent complexity, making sense of this alphabet soup is relatively straightforward once you have a good understanding of the underlying base standard, AT 101.

AT 101, titled *Attest Engagements*, is governed by the American Institute of Certified Public Accountants (AICPA) and establishes the framework for controls and non-financial attest work. Reports issued directly under AT 101 cover a variety of topics and uses, including providing trust and transparency outside of a traditional service organization setting, and can be unrestricted in distribution.

In an attempt to simplify reporting choices for service organizations/ service providers and to provide a means for service organizations/ service providers and users to tailor reporting to their needs, the AICPA recently developed the reporting designations, all of which are derived from AT 101, with specific definition and usage. These designations are called service organization control (SOC) reports SOC 1, SOC 2, and SOC 3.

SOC 1 is the intended direct replacement for the SAS 70. SOC 1 (also known as SSAE 16—the technical underlying replacement standard for the SAS 70 in the United States) focuses on a service organization's internal controls over financial reporting. SOC 1 (SSAE 16) is meant to be primarily an auditor- to-auditor communication, and in every material way, mirrors the legacy SAS 70. Despite the emergence of new risks and needs, SOC 1 (SSAE 16) is essentially the same as SAS 70. It does not address non-financial reporting-related controls, which would give service organization users greater comfort and a window into the service organization's business and control structure.

In contrast, the SOC 2 designation provides reporting options that go beyond financial controls. It covers technology-related areas of primary interest to service providers and user entities, such as privacy, availability, confidentiality, processing integrity, and security. SOC 2 reports also allow for the detailed description of the service auditor's tests and results (similar to SOC 1).

It is important to note that these reporting designations have not created anything new. They are effectively AT 101 reports with defined scope and usage.

Finally, the SOC 3 designation encapsulates reporting on areas such as security, privacy, availability, confidentiality, and processing integrity in accordance with the AICPA/CICA Trust Services Principles and Criteria. These engagements often result in the issuance of a "branded report" (i.e., SysTrust and WebTrust reports). SOC 3 also can have a broader distribution than the SOC 2; however, it will not contain the detailed description of the service auditor's tests and results.

It is important to note that these reporting designations have not created anything new. They are effectively AT 101 reports with defined scope and usage. These designations help clarify for the service organization/service provider and user what the scope and purpose of a given report is intended to cover. And more directly, they eliminate the perception that the traditional SAS 70 was a "one size fits all" solution for emerging business concerns. However, these reporting designations still may not fully fit the bill—and they don't govern non-service organization relationships.

What about reporting for non-service organizations?

As we know, the need for increased trust and transparency is not limited to traditional service organizations and their users. Organizations are pressured to provide transparency over controls, processes, data, and business results for a diverse set of stakeholders. Companies wishing to disclose information relating to areas such as corporate social responsibility, sustainability, regulatory compliance, executive compensation, data integrity, and business operations (to name a few) are leveraging customized forms of AT 101 to make these statements to the market. For example, certain hedge funds are using customized AT 101 reports to provide transparency into the processing controls for their investors, while Internet application providers are using customized AT 101 reports to provide transparency to business partners over areas such as advertising and content. The broad flexibility in the subject matter, as well as the ability to customize the report to the intended audience, makes a customized AT 101 report the ideal solution in situations where the need to provide trust and transparency goes beyond the defined SOC 1, SOC 2, and SOC 3 constructs.

How to decide which report is right for my business

When deciding what level of reporting is the right fit for your company, the first step is to evaluate whether there is any concern about the scope of your existing controls report (e.g., SAS 70 report). The need for this evaluation applies to both the service organization as well as its users. For example, are there critical functions performed by the service organization that are important for its users that are not included in the traditional SAS 70 report? Or has the SAS 70 report expanded over the years to include topics beyond internal controls over financial reporting?

Next, service organizations and users must understand their respective needs. For example, if the focus is limited to internal control over financial reporting, a SOC 1 (SSAE 16) report may be sufficient. If the user is concerned about privacy, security, confidentiality, availability, or regulatory compliance, a different report is likely a better fit.

The service organization should also consider its intended audience. Will it be limited to current customers, or is there a broader audience who would want to see a report?

The choice of reports is offered as a way to help companies address risks that go beyond financial reporting. Because these reports are performed under AT 101, the challenge for service organizations/service providers and their users is to determine what type of report will best meet the needs of today's marketplace and provide the greatest value in terms of sharing information with customers and the public.

If your company is asking whether it needs to provide greater trust, transparency, and information to stakeholders, including regulators, shareholders, vendors, customers, or the public at large, you should consider contacting your PwC professional.

Acknowledgements

Authors

George Galindo
Angela Shiffette

For a deeper discussion about how service organization/provider controls reporting may affect your business, please contact:

Steve Del Vecchio
Risk Assurance Partner
617 530 7999
stephen.l.delvecchio@us.pwc.com

Chris Thompson
Risk Assurance Partner
646 471 2700
chris.thompson@us.pwc.com

Kevin Knight
Risk Assurance Partner
703 918 3505
kevin.knight@us.pwc.com

George Galindo
Risk Assurance Director
713 356 4622
george.a.galindo@us.pwc.com

www.pwc.com