SUTHERLAND

LEGAL ALERT

May 19, 2011

Outsourcing: SAS 70 Superseded for Service Provider Control Reporting By SSAE 16

Executive Summary

Prior to 2011, customers (user entities) who engaged third-party service providers (service organizations) to perform functions and/or processes that impacted the user entities' internal control over financial reporting (ICFR) typically required Statement on Auditing Standards (SAS) No. 70 Type 2 reports[1] from service organization auditors (service auditors) that could be relied upon by the user entities' management and auditors (user auditors) in discharging management's responsibilities under the Sarbanes-Oxley Act of 2002 (SOX) and assuring the effectiveness of the user entities' ICFR. SAS 70 contained the requirements and guidance for both service auditors reporting on controls at service organizations and user auditors auditing the user entities' financial statements. Statement on Standards for Attestation Engagements (SSAE) No. 16[2] now provides the requirements and guidance for service auditors in such contexts and to that extent supersedes SAS 70. Going forward, where the service organization's services affect the user entity's ICFR, user entities should require in their outsourcing services contracts that service organizations provide Service Organization Control (SOC) 1 Type 2 reports under SSAE 16 rather than SAS 70 Type 2 reports. Additionally, user entities will want to more carefully focus on the limitations of the SOC 1 Type 2 report which, as was also the case with the SAS 70 Type 2 report, addresses only financial reporting and does not address controls over other important matters such as the security, availability, processing integrity, confidentiality or privacy of the user entities' information or operations handled by the service organizations' system[3] that do not relate to financial reporting. SOC 2 and SOC 3 reports[4] (which will be described in a future Legal Alert) will address these elements of the service organizations' system that do not impact the user entities' ICFR.

SOX and SOC Reports

SOX § 404 and Securities and Exchange Commission (SEC) rules promulgated thereunder require each public company to produce a report on the company's ICFR as part of the annual report filed with the SEC. This report must include management's assessment of the effectiveness of the company's ICFR. Additionally, the company's auditor must report on management's assessment. Where a user entity has contracted with a service organization to provide services that impact the user entity's ICFR, the

---

[1] Statement on Auditing Standards No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, Professional Standards, Vol. 1, AU § 324) issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in April 1992.

[2] Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*, Vol. 1, AT § 801) (SSAE 16) issued by the Auditing Standards Board of the AICPA in April 2010 and effective for service auditors' reports for periods ending on or after June 15, 2011.

[3] The "system" of the service organization is generally viewed as consisting of the services provided to the user entity together with the supporting processes, policies, procedures, personnel and operations that constitute the service organization's core activities that are relevant to the services provided to user entities.

[4] These are reports under AT § 101, *Attest Engagements* (AICPA, Professional Standards, Vol. 1) based on SysTrust and WebTrust criteria.

management of the user entity must satisfy itself as to the design and effectiveness of the controls at the service organization that can affect the user entity's ICFR. The user entity's auditor must also perform certain audit procedures to satisfy itself that it can report on management's assessment.[5] Before now, both the user auditor and the service auditor looked to SAS 70 for the requirements and guidance relative to this process. Now the service auditor must look to SSAE 16.

SOC 1 Reports Replace SAS 70 Reports

SAS 70 reports may continue to be issued for service organization reporting periods ending prior to June 15, 2011. However, for periods from and after that date, service auditors will be issuing SOC 1 reports in accordance with SSAE 16. User auditors will continue to look to SAS 70.[6] As was the case with SAS 70, SSAE 16 provides for two types of reports that can be issued by the service auditor: **(1)** a Type 1 "report on management's description of a service organization's system and the suitability of the design of controls"; and **(2)** a Type 2 "report on management's description of a service organization's system and the suitability of the design of controls and operating effectiveness of controls." It would be rare that an SOC 1 Type 1 report would satisfy a user entity's requirements. While the SOC 1 report is similar to the SAS 70 report in many respects, it includes important additional elements, including the service organization management's assertion describing the service organization's system and its internal controls. Unlike the SAS 70 Type 2 report, which speaks as of a specific point in time, the SOC 1 Type 2 report covers a defined period of time.

"Significant deficiencies" and "material weaknesses"[7] identified by a user auditor during an audit must be communicated in writing to the user entity's management. User entity management must consider, and may be required to respond to, the user auditor's report in issuing its own SOX § 404 report.

SOC Reporting Requirements in Outsourcing Services Contracts

At the time of entering into an outsourcing services contract, a threshold analysis must be conducted by the user entity (and its auditor) to determine whether the activities being outsourced impact a process that could affect the user entity's ICFR.[8] If it is determined that the service organization's services do in fact impact the user entity's ICFR, then further due diligence is required on the service organization's system of controls as they relate to the services provided to the user entity. As part of its due diligence process, the user entity should require the service organization to provide the user entity with the service organization's most recent SOC 1 report, if available, and if not available, the information that would be required to be developed by management of the service organization in connection with the production of an SOC 1 report. In any event, the user entity should insist that a provision be included in the outsourcing

---

[5] SAS 70/SOC 1 Type 2 reports are not just required for public companies. Any user entity that has audited financial statements prepared in accordance with generally accepted accounting principles (GAAP) and audited in accordance with generally accepted auditing standards (GAAS), and/or simply wishes to pursue best practices in vendor management, must become familiar with the requirements of the SAS 70/SOC 1 Type 2 report.

[6] The Accounting Standards Board has issued its Clarified Statement on Auditing Standards, *Audit Considerations Relating to an Entity Using a Service Organization,* which will supersede the requirements and guidance for user auditors in SAS 70, but will be effective no earlier than for reporting periods ending after December 15, 2012.

[7] These terms are defined in Statement on Auditing Standards No. 115, *Communicating Internal Control Related Matters Identified in an Audit* (AICPA, Professional Standards, AU § 325).

[8] The prospective user entity's inquiry should not end with ICFR issues. It should also extend to non-ICFR risks that are the subject of SOC 2 and SOC 3 examinations and reports as well.

services contract that requires the service organization to obtain on an ongoing basis an SOC 1 Type 2 report on the service organization's controls that affect the user entity's ICFR.

Allocation of Costs of SOC 1 Reports

If the service organization regularly undergoes SOC 1 Type 2 examinations, the user entity should not be required to pay for the base SOC 1 Type 2 examination or report. The service organization will often negotiate for the user entity to absorb the cost of additional audit work required specifically for the user entity. If the service organization does not regularly undergo SOC 1 Type 2 examinations and the user entity determines that an SOC 1 Type 2 report is required, responsibility for the cost of such undertaking will be the subject of negotiation between the parties. However, the user entity should have a strong argument that at least the cost of the baseline SOC 1 Type 2 examination and report should be absorbed by the service organization as an integral part of best practices assumed to be followed by leading service organizations.

Multiple Service Organization Locations

Even if the service organization undergoes a regular cycle of SOC 1 Type 2 examinations, if its operations are geographically dispersed, the regular reports may not have been performed at or cover the services location relevant to the services provided to the user entity. In such cases, the user entity must be satisfied that the service organization's SOC 1 Type 2 report will suffice. If not, the user entity may require supplemental audit work against controls at the particular services location.

Service Organization Subcontractors

If the service organization intends to subcontract any portion of the outsourced services, those subcontracted services must also be subject to SOC 1 Type 2 examination if they affect the user entity's ICFR. In such event, the user entity must make certain that the service organization's SOC 1 Type 2 report is inclusive of activities performed and controls observed at the subcontractor's facilities or a separate SOC 1 Type 2 report must be obtained from the subcontractor. Because, under the SOC 1 reporting process, assertions by management are required, it can be anticipated that there will be resistance from some subcontractors to providing SOC 1 Type 2 reports.[9]

"Significant Deficiencies" and "Material Weaknesses"

In instances in which the service auditor issues a satisfactory SOC 1 Type 2 report that the service organization's system of controls are adequate and operating effectively without exception, the user entity's management (and the user auditor) can generally rely on the report and focus on its (and their) assessment of the user entity's internal controls.[10] Where the service auditor's SOC 1 Type 2 report notes discrepancies or issues, however, the user entity's management and the user auditor must consider and

[9] Subcontractors' services may not impact ICFR, but may impact other aspects of the services that are appropriately the subject of SOC 2 or SOC 3 examinations and reports.

[10] The user entity and its auditor must carefully review the service organization's report to: (1) confirm that the description of services aligns to the services contracted for; (2) the controls described are consistent with the control expectations already established by the user entity; (3) the tests of controls are consistent with the user entity's expectations; and (4) the results of the tests are satisfactory.

assess the control deficiencies at the service organization and determine whether they require disclosure or qualification in the user entity's annual report.

The date of issuance of the service organization's SOC 1 Type 2 report must allow sufficient time: **(1)** for the service organization to identify control deficiencies and implement remediation plans prior to the close of the user entity's fiscal year and report filing deadlines; and **(2)** for the user entity to review and evaluate the deficiencies, if any (and any such remediation plans), prior to the end of its fiscal year and in a manner that accommodates its report filing deadlines. The user entity should also insist upon a "bring-down letter" that covers the "stub period" between the date of the report and the end of the user entity's fiscal year. To the extent significant deficiencies or material weaknesses were noted in the SOC 1 Type 2 report, such bring-down letter should further report on the status of the service organization's remediation efforts.

Given the impact of both significant deficiencies and material weaknesses on a user entity's financial reporting, user entities should require meaningful service level credits in the event a material weakness and/or a significant deficiency exists attributable to the service organization, and a contract termination right in the event of the service organization's failure to timely correct/remediate such significant deficiencies and material weaknesses. Because material weaknesses pose a greater risk of a misstatement of the user entity's financial statements, the period within which the service organization must correct/remediate any material weaknesses prior to the accrual of service level credits/liquidated damages and/or the user entity's termination right should be shorter than in the case of significant deficiencies. Service level credits should not be the exclusive remedy available to the user entity for such breaches and the user entity should retain the right to recover damages.

■ ■ ■

If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed below or the Sutherland attorney with whom you regularly work.

Scott M. Hobby	404.853.8051	scott.hobby@sutherland.com
Charles F. Hollis III	404.853.8100	chuck.hollis@sutherland.com
Derek C. Johnston	404.853.8099	derek.johnston@sutherland.com
John B. Miller, Jr.	404.853.8095	jay.miller@sutherland.com
Peter C. Quittmeyer	404.853.8186	peter.quittmeyer@sutherland.com
Timothy R. Dodson	404.853.8109	tim.dodson@sutherland.com