SUTHERLAND

LEGAL ALERT

July 5, 2011

Outsourcing: Service Organization Control (SOC 2 and SOC 3) Reports on Controls Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

Executive Summary

This Legal Alert complements our Legal Alert dated May 19, 2011, relating to SOC 1 reports entitled *Outsourcing: SAS 70 Superseded for Service for Service Provider Controls Reporting by SSAE 16* (SOC 1 Legal Alert) and completes our coverage of the new service organization control reporting framework (SOC 1, SOC 2 and SOC 3) established by the American Institute of Certified Public Accountants (AICPA).

Customers (user entities) engaging outsource service providers (service organizations) to perform services involving the collection, processing, transmitting, sorting, organizing, maintaining or disposing of user entity information expose themselves to additional risks associated with the system utilized by the service organization to deliver the services. The user entities and the management of these user entities remain ultimately accountable to the various regulatory bodies and user entities' stakeholders (boards of directors, shareholders, customers, etc.) for the successful and compliant conduct of the user entities' outsourcing arrangements with service organizations.

With the AICPA's issuance of its *Guide*: *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, updated May 1, 2011 (SOC 2 Guide), accountants for service organizations (service auditors) are now able to issue three service organization control reports in the AICPA framework – SOC 1[1], SOC 2 and SOC 3[2] reports. This framework of reports provides user entities' management with tools to obtain certain assurances regarding the performance of outsource service providers' service delivery systems.

Following the SOC 2 Guide, service auditors may issue SOC 2 type 2 reports on the service organization's controls over its systems used to perform, provide and deliver the services to a specific user entity. SOC 2 type 2 reports have the flexibility to cover some or all of the five "trust services principles" – security, availability, processing integrity, confidentiality and privacy. Specifically, these reports contain (1) the service organization management's description of the service organization's system, (2) a detailed description of the service auditor's tests of the operating effectiveness of the service organization's controls, and (3) the results of those tests, which enable the user entity's management to better assess, address and report on the risks associated with the outsourced services.

---

[1] See Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*, Vol. 1, AT Sec. 801) relating to service auditor reports on controls at service organizations affecting user entities' internal controls over financial reporting. The SOC 1 report replaces the old SAS 70 report.

[2] SOC 3 reports are attest reports by service auditors for general use by stakeholders in the subject service organization issued under AT Sec.101, *Attest Engagements* (AICPA, *Professional Standards*, Vol. 1) and TSP Sec. 100, *Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (TSP Sec. 100).

Going forward, user entities should require in their outsourcing services agreements that the service organizations provide the user entities with annual, unqualified SOC 2 type 2 reports on the service organization's controls relative to the five trust services principles applicable to the services being provided.[3]

As discussed below, seldom will either an SOC 2 type 1 or the general SOC 3 report satisfy a user entity's need for assurances regarding the services provided to it. However, SOC 3 reports, if available, can be valuable to a potential customer of a service organization in qualifying the service organization for consideration as an outsourcing services provider.

SOC 1, 2 and 3 Reports Distinguished

As discussed in our SOC 1 Legal Alert, SOC 1 type 2 reports relate solely to controls at a service organization that impact the user entity's internal controls over financial reporting. The SOC 1 report addresses the trust services principles only within the limited context of financial reporting and will typically only touch on security as it relates to financial infrastructure, processing integrity relative to calculation of financially relevant amounts and perhaps marginally on availability as it relates to backup and restore functions. This relatively narrow focus is not likely to provide user entities' management with the required assurances relative to the broader operational issues that are of concern to the user entities.[4]

Under the SOC 2 Guide, service auditors can now address these broader user entity needs to assess and address risks related to non-financial reporting issues arising out of outsourcing services arrangements, such as compliance with laws and regulations applicable to the user entity (for which it remains responsible notwithstanding the outsourcing of related functions), and the efficiency and effectiveness of the user entity's overall operations.

The SOC 2 type 2 report is a "restricted report" for the use of the particular user entity, since it requires knowledge of the specific services being provided and how the service organization's system interacts with the user entity (including complementary user entity controls). The SOC 2 type 2 report is not intended to be available to, for instance, prospective customers of the service organization generally.

This is contrasted with SOC 3 reports, which also address one or more of the five trust services principles at the service organization, but are designed to be general-use reports that may be made available to anyone. The SOC 3 report does not contain a description of the service organization's system of controls prepared by the service organization's management, nor does it include the service auditor's tests of the operating effectiveness of the service organization's controls or the results of those tests. These elements are typically necessary for the user entity's management to determine how it may be affected by the service organization's controls.[5]

---

[3] Depending on the nature of the services outsourced, fewer than all five of the trust services principles may need to be addressed in the SOC 2 report. The baseline position of the user entity, however, should be to require an SOC 2 type 2 report on all five principles, unless and until it is determined that fewer are relevant to the services.

[4] SOC 1 and SOC 2 reports are not permitted to be combined. SOC 2 Guide Sec. 1.23.

[5] SOC Guide, Sec.1.24 provides a helpful chart comparing SOC 1, SOC 2 and SOC 3 reports.

SUTHERLAND

Service Organization System, Trust Services Principles and Criteria Explained

A service organization's "system" consists of the following components, which are organized and utilized to achieve a specified objective (i.e., delivering a specific service or group of services): (1) the infrastructure (the physical and hardware components of a system including facilities, equipment and networks); (2) software (programs and operating software, including systems, applications and utilities); (3) people (the personnel involved in the operation and use of a system, including developers, operators, users and managers); (4) procedures (the automated and manual procedures involved in the operation of the system); and (5) data (the information used and supported by a system, including transaction streams, files, databases and tables).

The term "trust services" is defined as "a set of professional attestation and advisory services based on a core set of principles and criteria that addresses the risks and opportunities of IT-enabled systems and privacy programs." [6] The five "trust services principles" (which are broad statements of objectives) under the SOC 2 and SOC 3 reporting framework are as follows[7]:

a. *Security*. The system is protected against unauthorized access (both physical and logical).

b. *Availability*. The system is available for operation and use as committed or agreed.

c. *Processing integrity*. System processing is complete, accurate, timely and authorized.

d. *Confidentiality*. Information designated as confidential is protected as committed and agreed.

e. *Privacy*. Personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the service organization's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and the Canadian Institute of Chartered Accountants.[8]

The trust services principles and criteria of security, availability, processing integrity and confidentiality are organized into four broad areas, as follows:

a. *Policies*. The service organization has defined and documented its policies relevant to the particular principle.

b. *Communications*. The service organization has communicated its defined policies to responsible parties and authorized users of the system.

c. *Procedures*. The service organization has placed in operation procedures to achieve its objectives in accordance with its defined policies.

---

[6] TSP Sec. 100.03.

[7] TSP Sec, 100.10; SOC 2 Guide, Sec. 1.06.

[8] SOC 2 Guide, Sec. 1.06.

d. *Monitoring*. The service organization monitors the system and takes action to maintain compliance with its defined policies.[9]

The trust services principles for privacy are organized into two broad areas, as follows:

a. *Policies and communications*. Privacy policies are written statements that set out management's intent, objectives, requirements, responsibilities and standards concerning privacy. Communication refers to the organization's communication to individuals, internal personnel and third parties about its privacy notice and its commitments stated in the notice and related information.

b. *Procedures and controls*. The other actions the organization takes to achieve the criteria.[10]

The criteria for each of the trust services principles other than privacy are set forth at length in Appendix B to the SOC 2 Guide and again, together with illustrative controls at TSP Secs. 100.19 through 100.32. The privacy principles and criteria, as well as privacy concepts and Generally Accepted Privacy Principles, are set out at TSP Secs. 100.33 through 100.44.[11]

SOC 2 Reports

The SOC 2 type 2 report involves the engagement by service organizations of a service auditor (typically at the request of a user entity or regulator) to report on the design and operating effectiveness of the controls over the service organization's systems that deliver services to the user entity or are subject to the authority of the regulator that are relevant to one or more of the trust services principles.

Unlike the SOC 3 report that is designed to meet the needs of a broad range of users, the SOC 2 type 2 report contains management's detailed description of the service organization's system of controls relevant to the services to the user entity, the service auditor's tests of the operating effectiveness of the controls and the results of these tests. Specifically, a SOC 2 type 2 report includes:

(1) The service organization management's description of the service organization's system;

(2) The service organization management's written assertion that (a) such description fairly presents the service organization's system that was designed and implemented throughout the specified period based upon the criteria set forth, (b) the described controls were suitably designed to meet the applicable trust services criteria throughout the specified period, (c) the described controls operated effectively throughout the specified period to meet the applicable trust services criteria, and (d) where privacy is covered, the service organization complied with the commitments in its statement of privacy practices throughout the specified period; and

(3) The service auditor's report on the service organization management's assertion.
The SOC type 2 report should cover a period of time sufficient for the users of the services to gain an understanding of the efficacy of the controls included in the report (which could be the

[9] TSP Sec. 100.11.

[10] TSP Sec. 100.15.

[11] Discussing these criteria is beyond the scope of this Legal Alert, but they are an excellent resource for user entity management to develop a checklist for evaluating a potential service provider's controls over its service delivery system.

fiscal year of the service organization or a shorter period, depending on the circumstances). In its SOC 2 type 2 report, the service auditor expresses an opinion on (1) whether management's description of the service organization's system is fairly presented, (2) whether the controls are suitably designed to provide reasonable assurance that the applicable trust service criteria would be met if the controls operated effectively, (3) whether the controls were operating effectively to meet the applicable trust services criteria,[12] and (4) in reports covering privacy, whether the service organization complied with the commitments in its statement of privacy protection provided to the user entity.

Where applicable, the service organization's system description will include complementary user entity controls that are necessary, in conjunction with the service organization's controls, to fulfill the applicable trust services criteria.

As is the case with SOC 1 reports, controls at subservice providers (subcontractors) may be relevant and the issue of whether the SOC 2 report by the service organization takes the inclusive or the carve-out approach with respect to the controls at the subservice providers will be the subject of negotiations between the user entity and the service provider. The inclusive approach involves covering subservice organizations' controls in the report. The carve-out approach does not cover controls at subservice organizations.

Outsourcing Contract Requirements and Allocation of Costs

Customers/user entities should approach all outsourcing services arrangements with the baseline requirement and expectation that the service organization will provide it with annual (or more frequent interim) unqualified SOC 2 type 2 reports on the service organization's controls relative to the service delivery systems that address all relevant trust service principles. Service organizations should be required to clearly define the role of each subservice organization (e.g., a data center) involved in providing the services, the nature of the services being provided, the system being used to deliver those services, the risks represented by those services and their delivery, and the means by which the service organization has gained assurance that the subservice organization is effectively mitigating those risks. For those situations where the risks represented by the subservice organization may be significant to the user entity, the service organization should be required to use the inclusive method in its SOC 2 type 2 report or should be required to obtain an appropriate SOC 2 type 2 report from the subservice organization.

Industry leading service providers should be expected to have current SOC 3 reports available for examination by prospective customers. Requests for SOC 3 reports should become a standard requirement in all requests for proposal. Since there is a certain amount of overlap in the work required to obtain SOC 3 and SOC 2 reports, the customer should take the initial position that any costs associated with the SOC 2 type 2 reports should be baked into the pricing and should not be passed through to the customer.

Where no SOC 3 reports are available from the service provider, customers should request a detailed description of the service provider's system of controls similar to the description that would be included in an SOC 2 type 2 report as part of the original due diligence on the service provider.

[12] The applicable trust services criteria are set out in Appendix B to the SOC 2 Guide.

Until competition among service providers produces a standardized approach to the allocation of these costs, customers should expect that the cost allocation will likely be the subject of negotiation, and the service provider may push to pass some part or all of the costs through to the customer.

A logical approach to the cost issue would be to have the service provider bear the cost of a SOC 2 type 2 report covering the trust services principles at the level of detail required by its customers generally, with the cost of any "custom" or "one-off" aspects of the report required by a particular user entity passed through to that user entity.

Finally, the outsourcing contract should provide for appropriate service level credits/liquidated damages for the service organization's failure to provide timely satisfactory SOC 2 type 2 reports, as well as the right of the customer to terminate the contract and recover damages if the breach is not remedied within an agreed cure period.

Summary

SOC 1 reports focus only on controls at a service organization that relate to functions being performed that impact the user entity's internal controls over financial reporting. Due to its relatively narrow focus, an SOC 1 report is not likely to provide the user entities' management with sufficient information to assess the effectiveness of controls at the service organization that address the full spectrum of risks related to the outsourced services.

Although they address on a general basis the same subject matter and the same criteria as an SOC 2 report, SOC 3 reports do not include a description of the service organization's systems prepared by the management, nor do they contain a description of the auditor's tests of the operating effectiveness of those controls or the results of those tests. Additionally, even if the privacy principle is addressed in the SOC 3 report, the report will not contain a description of the auditor's tests of the service organization's compliance with its statement of privacy protection and the results of those tests.

The baseline position that customers should take in arrangements with outsource service providers is for the service organization to provide the customer with annual unqualified type 2 reporting for SOC 1 and/or SOC 2 (covering all applicable trust services principles) at the sole expense of the service organization.

■ ■ ■

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