November 2011

AICPA Technical Practice Aids

TIS Section 9530, *Service Organization Controls Reports*

.01 *Reporting on Controls at a Service Organization Relevant to Subject Matter Other Than User Entities' Internal Control Over Financial Reporting*

Inquiry—Is authoritative guidance available for reporting under AT section 101, *Attest Engagements* (AICPA, *Professional Standards*), on a service organization's controls relevant to subject matter other than user entities' internal control over financial reporting (ICFR)?

Reply—Yes. The AICPA has developed an authoritative guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)* (SOC 2 guide), to assist practitioners in reporting under AT section 101 on an examination of controls at a service organization relevant to the security, availability, or processing integrity of a system or the confidentiality, or privacy of the information processed by the system.

[Issue Date: November 2011.]

.02 *Service Organization Controls Reports*

Inquiry—What does the acronym "SOC" stand for?

Reply—The acronym SOC stands for service organization controls, as in "service organization controls reports." The AICPA introduced this term to make practitioners aware of the various professional standards and guides available to them for examining and reporting on controls at a service organization relevant to user entities and to help practitioners select the appropriate standard or guide for a particular engagement. The following are the designations for the three engagements included in the SOC report series and the source of the guidance for performing and reporting on them:

- SOC 1: Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*, AT sec. 801), and AICPA Guide *Service Organizations*: *Applying SSAE No. 16*, Reporting on Controls at a Service Organization *(SOC 1)*
- SOC 2: AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)* and AT section 101
- SOC 3: TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, and AT section 101

[Issue Date: November 2011.]

.03 *Authority of SOC 1 and SOC 2 Guides*

Inquiry—What is the authority of the SOC 1 and SOC 2 guides?

Reply—The SOC 1 and SOC 2 guides have been cleared by the AICPA's Auditing Standards Board. AT section 50, *SSAE Hierarchy* (AICPA, *Professional Standards*), classifies attestation guidance included in an AICPA guide as an interpretive publication and indicates that a practitioner should be aware of and consider interpretive publications applicable to his or her examination. If a practitioner does not apply the attestation guidance included in an applicable interpretive publication, the practitioner should be prepared to explain how he or she complied with the SSAE provisions addressed by such attestation guidance.

[Issue Date: November 2011.]

.04 *SOC 3 Engagements*

Inquiry—What is a SOC 3 engagement?

Reply—A SOC 3 engagement is similar to a SOC 2 engagement in that the practitioner reports on whether an entity (any entity, not necessarily a service organization) has maintained effective controls over its system with respect to security, availability, processing integrity, confidentiality, or privacy. Like a SOC 2 engagement, a SOC 3 engagement uses the criteria in TSP section 100. Unlike a SOC 2 engagement, a SOC 3 report (1) does not contain a description of the practitioner's tests of controls and results of those tests and (2) is a general-use report rather than a restricted use report. (The term *general use* refers to reports for which use is not restricted to specified parties.)

[Issue Date: November 2011.]

.05 *Types of Reports for SOC 2 Engagements*

Inquiry—Are there type 1 and type 2 reports for SOC 2 engagements?

Reply—Yes. In a SOC 2 engagement, like a SOC 1 engagement, the practitioner has the option of providing either a *type 1* or a *type 2 report*. In both reports, management of the service organization prepares a description of its system. In a type 1 report, the service auditor expresses an opinion on whether the description is fairly presented (that is, does it describe what actually exists) and whether the controls included in the description are suitability designed. Controls that are suitably designed *are able* to achieve the related control objectives or criteria if they operate effectively. In a type 2 report, the service auditor's report contains the same opinions that are included in a type 1 report, and also includes an opinion on whether the controls were operating effectively. Controls that operate effectively *do* achieve the control objectives or criteria they were intended to achieve. Both SOC 1 and SOC 2 reports are examination reports, which means the practitioner obtains a high level of assurance.

[Issue Date: November 2011.]

.06 *Minimum Period of Coverage for SOC 2 Reports*

Inquiry—Does the SOC 2 guide require that a type 2 report cover a minimum period?

Reply—The SOC 2 guide does not prescribe a minimum period of coverage for a SOC 2 report, however, paragraph 2.09 of the SOC 2 guide states that one of the relevant factors to consider when determining whether to accept or continue a SOC 2 engagement is the period covered by the report. The guide presents an example of a service organization that wishes to engage a service auditor to perform a type 2 engagement for a period of less than two months. The guide states that in those circumstances, the service auditor should consider whether a report covering that period will be useful to users of the report, particularly if many of the controls related to the applicable trust services criteria are performed on a monthly or quarterly basis. A practitioner would use professional judgment in determining whether the report covers a sufficient period.

[Issue Date: November 2011.]

.07 *Placement of Management’s Assertion in a SOC 2 Report*

Inquiry—In a SOC 2 engagement, does management’s assertion need to accompany the service organization’s description of its system?

Reply—Paragraph 2.13(b) of the SOC 2 guide states, in part, that a service auditor ordinarily should accept or continue an engagement to report on controls at a service organization only if management of the service organization acknowledges and accepts responsibility for "providing a written assertion that will be attached to management’s description of the service organization’s system and provided to users." The recommendation in the SOC 2 guide is that the assertion be attached to the description rather than included in the description to avoid the impression that the practitioner is reporting on the assertion rather than on the subject matter.

[Issue Date: November 2011.]

.08 *Illustrative Assertion for Management of a Service Organization in a SOC 2 Engagement*

Inquiry—Where can I find an illustrative management assertion for a SOC 2 engagement?

Reply—Appendix C, "Illustrative Management Assertions and Related Service Auditor’s Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy," of the SOC 2 guide contains illustrative assertions by management of a service organization for type 2 SOC 2 engagements.

[Issue Date: November 2011.]

.09 *Illustrative Assertion for Management of a Subservice Organization in a SOC 2 Engagement*

Inquiry—The SOC 2 guide contains illustrative management assertions for management of a service organization. Is an illustrative assertion for management of a subservice organization available in the SOC 2 guide?

Reply—No. However, the illustrative assertions in appendix C of the SOC 2 guide can be used to construct the subservice organization’s assertion. Paragraphs 2.13–2.15 of the SOC 2 guide address the requirement for an assertion by management of a subservice organization when the inclusive method is used.

[Issue Date: November 2011.]

.10 *Management of a Subservice Organization Refuses to Provide a Written Assertion in a SOC 1 or SOC 2 Engagement*

Inquiry—When using the inclusive method, if management of a subservice organization will not provide a written assertion, what should the service auditor do?

Reply—Paragraph .A8 of AT section 801 indicates that the subservice organization's refusal to provide the service auditor with a written assertion precludes the service auditor from using the inclusive method. However, the service auditor may instead use the carve-out method. Paragraph 2.15 of the SOC 2 guide contains similar guidance for SOC 2 engagements.

[Issue Date: November 2011.]

.11 *Determining Whether Management of a Service Organization Has a Reasonable Basis for Its Assertion (SOC 1 and SOC 2 Engagements)*

Inquiry—Paragraph .09(c)(ii) of AT section 801 states that one of the requirements for a service auditor to accept or continue a type 1 or type 2 engagement is that management acknowledge and accept responsibility for having a reasonable basis for its assertion. Paragraph .A17 of AT section 801 indicates that the service auditor's report on controls is not a substitute for the service organization's own processes to provide a reasonable basis for its assertion. How does the service auditor determine whether management has a reasonable basis for its assertion?

Reply—AT section 801 indirectly describes how the service auditor makes this determination. First, paragraph .14(a)(vii) of AT section 801 indicates, in part, that the service organization's description of its system should include the service organization's monitoring activities. Because a service auditor is required to determine whether the description is fairly stated, in doing so the service auditor would determine whether the section of the description that describes monitoring controls is fairly stated. Second, paragraph .A17 of AT section 801, shown subsequently, defines the term *monitoring of controls* and indicates that management's monitoring activities may provide evidence of the design and operating effectiveness of controls in support of management's assertion. Similar guidance for SOC 2 engagements is included in appendix A, "Information for Management of a Subservice Organization," of the SOC 2 guide, in the section titled "Providing a Written Assertion."

[Issue Date: November 2011.]

.12 *Reasonable Basis for Management of a Subservice Organization's Assertion (SOC 1 and SOC 2 Engagements)*

Inquiry—In an inclusive SOC 1 engagement, is the service auditor required to determine whether management of the subservice organization has a reasonable basis for its assertion?

Reply—Paragraph .09(c)(ii) of AT section 801 states that one of the requirements for a service auditor to accept or continue a type 1 or type 2 engagement is that management acknowledge and accept responsibility for having a reasonable basis for its assertion. Paragraph .A7 of AT section 801 states that when the inclusive method is used, the requirements of AT section 801 also apply to the services provided by the subservice organization, including the requirement to acknowledge and accept responsibility for the matters in paragraph .09(c)(i)–(vii) of AT section 801 as they relate to the subservice organization. Paragraph .09(c)(vii) requires a service organization to provide a written assertion; therefore, a subservice organization would also be required to provide a written assertion and have a reasonable basis for its assertion.

In determining whether a subservice organization has a reasonable basis for its assertion, the service auditor would analogize the requirements and guidance in AT section 801 to the subservice organization. Paragraph .14(a)(vii) of AT section 801 would require that the subservice organization's description of its system include the subservice organization's monitoring activities. Because a service auditor is required to determine whether the subservice organization's description is fairly stated, in doing so the service auditor would determine whether the section of the description that describes monitoring controls is fairly stated. Paragraph .A17 of AT section 801 defines the term *monitoring of controls* and indicates that management's monitoring activities may provide evidence of the design and operating effectiveness of controls in support of management's assertion. Similar guidance on this topic for a SOC 2 engagement is included in paragraphs 2.13(b)–(c) and 2.15 of the SOC 2 guide.

[Issue Date: November 2011.]

.13 *Point in a SOC 1 or SOC 2 Engagement When Management Should Provide Its Written Assertion*

Inquiry—At what point in a SOC 1 or SOC 2 engagement should management provide the service auditor with its written assertion?

Reply—Management may provide its written assertion to the service auditor at any time after the end of the period covered by the service auditor's type 2 report and, for a type 1 report, at any time after the as of date of the type 1 report. The date of the service auditor's report should be no earlier than the date on which management provides its written assertion.

[Issue Date: November 2011.]

.14 *Implementing Controls Included in Management's Description of the Service Organization's System (SOC 1 and SOC 2 Engagements)*

Inquiry—In a type 1 report for a SOC 1 or SOC 2 engagement, do the controls included in management's description of the service organization's system need to be implemented?

Reply—Yes. In order for the description of the service organization's system to be fairly presented, the controls included in the description would have to be placed in operation (implemented). See paragraph 4.01(b) of the SOC 1 guide and paragraph 3.13 of the SOC 2 guide.

[Issue Date: November 2011.]

.15 *Responsibility for Determining Whether a SOC 1, SOC 2, or SOC 3 Engagement Should Be Performed*

Inquiry—Who determines whether a SOC 1, SOC 2, or SOC 3 engagement should be performed—the service auditor or management of the service organization?

Reply—SOC 1 engagements address a service organization's controls relevant to user entities' ICFR, whereas SOC 2 and SOC 3 engagements address a service organization's controls relevant to the security, availability, or processing integrity of a system or the confidentiality or privacy of the information the system processes. In SOC 2 and SOC 3 engagements, the service auditor uses the criteria in TSP section 100 for evaluating and reporting on controls relevant to the security, availability, or processing integrity of a system, or the confidentiality or privacy of the information processed by the system. In TSP section 100, these five attributes of a system are known as *principles.* A service auditor may be engaged to report on a description of a service organization's system and the suitability of the design and operating effectiveness of controls relevant to one or more of the trust services principles The criteria in TSP section 100 that are applicable to the principle(s) being reported on are known as the *applicable trust services criteria*.

If management of the service organization is not knowledgeable about the differences among these three engagements, the service auditor may assist management in obtaining that understanding and selecting the appropriate engagement. Determining which engagement is appropriate depends on the subject matter addressed by the controls and the risk management and governance needs of the user entities, and it often involves discussion with the user entities regarding their needs.

[Issue Date: November 2011.]

.16 *Criteria for SOC 2 and SOC 3 Engagements*

*Inquiry***—**Are there a prescribed set of control objectives for SOC 2 and SOC 3 engagements?

Reply—In SOC 1 engagements, the service auditor determines whether controls achieve specified control objectives. In SOC 2 and SOC 3 engagements, the service auditor determines whether controls meet the applicable trust services criteria. Although the terminology is different in these engagements (control objectives versus criteria), the control objectives in a SOC 1 engagement serve as criteria for evaluating the design and, in a type 2 report, the operating effectiveness of controls. Unlike SOC 1 engagements, in which management of the service organization determines the service organization’s control objectives based on the nature of the service provided and how the service is performed, in all SOC 2 and SOC 3 engagements, the service organization’s controls must meet all of the criteria in TSP section 100 that are applicable to the principle(s) being reported on. The applicable trust services criteria serve as a prescribed set of criteria.

[Issue Date: November 2011.]

.17 *Using Existing Set of Controls for a New SOC 2 or SOC 3 Engagement*

Inquiry—In the past, many IT service organizations provided their user entities with SAS No. 70 reports (SAS No. 70, *Service Organizations* [AICPA, *Professional Standards*, AU sec. 324]), covering the IT services. If a service organization plans to undergo a SOC 2 or SOC 3 examination for the first time and has a fully defined set of controls and control objectives related to its IT services, does the service organization need to adopt a new set of controls to meet the applicable trust services criteria?

*Reply***—**The SOC 2 guide and appendix C of TSP section 100 require the service organization to establish controls that meet all of the applicable trust services criteria. A service organization that is planning to undergo a SOC 2 or SOC 3 engagement for the first time may have controls in place that address all of the applicable trust services criteria. However, the service organization will need to determine whether its existing control objectives align with the applicable trust services criteria and whether its controls address all of the applicable trust services criteria. If not, it will need to implement or revise certain controls to meet all of the applicable trust services criteria.

[Issue Date: November 2011.]

.18 *Reporting on Compliance With Other Standards or Requirements in SOC 2 or SOC 3 Engagements*

Inquiry—May a SOC 2 or SOC 3 report cover compliance with other standards or authoritative requirements that are substantially similar to the applicable trust services criteria, for example, requirements in Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, issued by the National Institute of Standards and Technology (NIST) or in Payment Card Industry (PCI) Security Standards issued by the PCI Security Counsel?

Reply—Yes. A service organization may request that a SOC 2 or SOC 3 report address additional subject matter that is not specifically covered by the applicable trust services criteria. An example of such subject matter is the service organization's compliance with certain criteria established by a regulator, for example, security requirements under the Health Insurance Portability and Accountability Act of 1996 or compliance with performance criteria established in a service-level agreement. Paragraph 1.38 of the SOC 2 guide states that in order for a service auditor to report on such additional subject matter, the service organization provides the following:

- An appropriate supplemental description of the subject matter
- A description of the criteria used to measure and present the subject matter
- If the criteria are related to controls, a description of the controls intended to meet the control-related criteria
- An assertion by management regarding the additional subject matter

Paragraph 1.39 of the guide states

> The service auditor should perform appropriate procedures related to the additional subject matter, in accordance with AT section 101 and the relevant guidance in this guide. The service auditor's description of the scope of the work and related opinion on the subject matter should be presented in separate paragraphs of the service auditor's report. In addition, based on the agreement with the service organization, the service auditor may include additional tests performed and detailed results of those tests in a separate attachment to the report.

[Issue Date: November 2011.]

.19 *Issuing Separate Reports When Performing Both a SOC 1 and SOC 2 Engagement for a Service Organization*

Inquiry—Going forward, will service organizations that include control objectives relevant to user entities ICFR along with control objectives that are not relevant to user entities' ICFR in their descriptions need to request two separate reports—SOC 1 and SOC 2?

Reply—Yes. Service organizations will now need to request two separate SOC reports if the service organization would like to address control objectives relevant to user entities' ICFR and control objectives (criteria) that are not relevant to user entities' ICFR. See paragraph 1.23 of the SOC 2 guide.

[Issue Date: November 2011.]

.20 *Deviations in the Subject Matter (SOC 1 and SOC 2 Engagements)*

Inquiry—In a SOC 1 or SOC 2 engagement, if the service auditor identifies deviations in the subject matter (that is, the fairness of the presentation of the description, the suitability of the design of the controls, and the operating effectiveness of the controls) and qualifies the report because of these deviations, does management need to revise its assertion to reflect these deviations?

Reply—If management of the service organization agrees with the service auditor's findings regarding the deviations, management would be expected to revise its assertion to reflect the deviations identified in the service auditor's report. If management does not revise its assertion, the service auditor should add an explanatory paragraph to the report indicating that the deficiencies identified in the service auditor's report have not been identified in management's assertion. Similar guidance for a SOC 2 engagement is included in paragraph 3.105 of the SOC 2 guide.

[Issue Date: November 2011.]

.21 *Use of a Seal on a Service Organization's Website*

Inquiry—Will there be a SOC seal that can be displayed on a service organization's website indicating that the service organization has undergone a SOC1, SOC 2, or SOC 3 engagement?

Reply—A seal is available only for SOC 3 engagements. A SOC 3 SysTrust for Service Organization Seal (seal) may be issued and displayed on a service organization's website. All practitioners who wish to provide this registered seal must be licensed by the Canadian Institute of Chartered Accountants (CICA). Typically the seal is linked to the report issued by the practitioner. For more information on licensure, go to http://www.webtrust.org. It is important to note that a practitioner can perform a SOC 3 engagement and issue a SOC 3 report without issuing a SOC 3 seal. In such cases the practitioner does not need to be licensed by the CICA. The license is only for the issuance of a seal.

In addition, SOC logos are available for use by (*a*) CPAs for marketing and promoting SOC services and (*b*) service organizations that have undergone a SOC 1, SOC 2, or SOC 3 engagement within the prior 12 months. These logos are designed to make the public aware of these SOC services and do not offer or represent assurance that an organization obtained an unqualified (or clean) opinion. For additional information about logos, go to http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/soclogosinfo.aspx.

[Issue Date: November 2011.]

.22 Attestation Standards and Interpretive Guidance for Reporting on a Service Organization's Controls Relevant to User Entities and for Reporting on an Entity's Internal Control

Inquiry—AICPA professional literature includes a variety of attestation standards and interpretive guidance for reporting on a service organization's controls relevant to user entities and for reporting on an entity's internal control. How does a practitioner determine the applicable attestation standard and interpretive guidance for these engagements?

Reply—The following table identifies a variety of attestation engagements that involve reporting on a service organization's controls relevant to user entities, or reporting on an entity's internal control. The table also identifies the appropriate attestation standard or interpretive guidance to be used in the circumstances.

Engagement	***Professional Standard or Other Guidance***	***Restrictions on the Use of the Report***
Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting: **Controls were not designed by the service organization; management of the service organization will not provide an assertion regarding the suitability of the design of the controls** Reporting on		
• the fairness of the presentation of management's description of the service organization's system and	Report on the fairness of the presentation of the description under AT section 101, *Attest Engagements* (AICPA, *Professional Standards*), using the description criteria in paragraph .14 of AT section 801, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*), and adapting the relevant requirements and guidance therein	Management of the service organization, user entities, and the auditors of the user entities' financial statements
• the operating effectiveness of the service organization's controls relevant to user entities internal control over financial reporting. Such a report may include a description of tests of the operating effectiveness of the controls and the results of the tests.	Report on the operating effectiveness of controls under AT section 101 or AT section 201, *Agreed-Upon Procedures Engagements* (AICPA, *Professional Standards*)	The specified parties that agreed upon the sufficiency of the procedures for their purposes
Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting: **Controls were not designed by the service organization; management of the service organization provides an assertion regarding the suitability of design of controls**	AT section 801	Management of the service organization, user entities, and the auditors of the user entities' financial statements

Engagement	*Professional Standard or Other Guidance*	*Restrictions on the Use of the Report*
***Reporting on Controls at a Service Organization Relevant to Security Availability, Processing Integrity, Confidentiality, or Privacy*: Includes Description of Tests and Results**		
Reporting on the fairness of the presentation of management's description of a service organization's system; the suitability of the design of controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy; and in a type 2 report, the operating effectiveness of those controls A type 2 report includes a description of tests of the operating effectiveness of controls performed by the service auditor and the results of those tests.	AT section 101 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)*	Parties that are knowledgeable about • the nature of the service provided by the service organization • how the service organization's system interacts with user entities, subservice organizations, and other parties • internal control and its limitations • the criteria and how controls address those criteria • complementary user entity controls and how they interact with related controls at the service organization
***Reporting on Controls at a Service Organization Relevant to Security Availability, Processing Integrity, Confidentiality, or Privacy:* No Description of Tests and Results**		
Reporting on whether an entity has maintained effective controls over its system with respect to security, availability, processing integrity, confidentiality, or privacy If the report addresses the privacy principle, the report also contains an opinion on the service organization's compliance with the commitments in its privacy notice. This report does not contain a description of the service auditor's tests performed and the results of those tests.	AT section 101 AICPA/Canadian Institute of Chartered Accountants Trust Services Principles, Criteria, and Illustrations (TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*)	This is a general-use report.[1]

[1] The term *general use* refers to reports for which use is not restricted to specified parties.

Engagement	*Professional Standard or Other Guidance*	*Restrictions on the Use of the Report*
Reporting on a Service Provider's Controls to Achieve Compliance Control Objectives Relevant to SEC Rules 38a-1 and 206(4)-7		
Reporting on the suitability of the design and operating effectiveness of a service provider's controls over compliance that may affect user entities' compliance This report does not contain a description of the practitioner's tests performed and the results of those tests.	AT section 101 Statement of Position (SOP) 07-2, *Attestation Engagements That Address Specified Compliance Control Objectives and Related Controls at Entities that Provide Services to Investment Companies, Investment Advisers, or Other Service Providers* (AUD sec. 14,430)	Chief compliance officers, management, boards of directors, and independent auditors of the service provider and of the entities that use the services of the service provider
Performing the Agreed-Upon Procedures Referred to in Paragraph .03 of AT section 801		
Performing and reporting on the results of agreed-upon procedures related to the controls of a service organization or to transactions or balances of a user entity maintained by a service organization This report contains a description of the procedures performed by the practitioner and the results of those procedures.	AT section 201	The specified parties that agreed upon the sufficiency of the procedures for their purposes
Reporting on Controls Over Compliance With Laws and Regulations		
Reporting on the effectiveness of an entity's internal control over compliance with the requirements of specified laws, regulations, rules, contracts, or grants	AT section 601, *Compliance Attestation* (AICPA, *Professional Standards*)	Use is restricted if the criteria are • appropriate for only a limited number of parties who established the criteria or can be presumed to understand the criteria. • available only to specified parties.
Reporting on Internal Control in an Integrated Audit		
Reporting on the design and operating effectiveness of an entity's internal control over financial reporting that is integrated with an audit of financial statements	AT section 501, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements* (AICPA, *Professional Standards*)	This is a general-use report.

[Issue Date: November 2011.]

DISCLAIMER: This publication has not been approved, disapproved or otherwise acted upon by any senior technical committees of, and does not represent an official position of, the American Institute of Certified Public Accountants. It is distributed with the understanding that the contributing authors and editors, and the publisher, are not rendering legal, accounting, or other professional services in this publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.