TIS Section 9520, *SSAE No. 16,* Reporting on Controls at a Service Organization

.01 *New Standards for Service Auditors and User Auditors*

Inquiry—Did the issuance of Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*, AT sec. 801), in April 2010, replace the guidance for service auditors and user auditors in AU section 324, *Service Organizations* (AICPA, *Professional Standards*)?

Reply—In part. AU section 324 contains the requirements and guidance for service auditors reporting on controls at a service organization relevant to user entities' internal control over financial reporting (ICFR) and for auditors auditing the financial statements of entities that use a service organization (user auditors). AT section 801 replaces the guidance for service auditors in AU section 324. However, the guidance for user auditors in AU section 324 will be unchanged until the new clarified AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), which has been approved by the Auditing Standards Board (ASB), becomes effective.

[Issue Date: June 2011. Revised, November 2011.]

.02 *Requirements and Guidance for Service Auditors Moved to Attestation Standards*

Inquiry—Why was the guidance for service auditors reporting on a service organization's controls relevant to user entities' ICFR moved from the Statements on Auditing Standards (SASs) to the SSAEs (attestation standards)?

Reply—The SASs primarily provide guidance on reporting on an audit of financial statements, whereas the SSAEs primarily provide guidance on reporting on other subject matter. In a service auditor's engagement under AT section 801, and also under AU section 324, the practitioner reports on a service organization's description of its system and on the service organization's controls relevant to user entities' ICFR. Because an examination of a description of a system and controls is not an audit of financial statements, the ASB concluded that the new standard should be placed in the attestation standards, along with 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*), in which a CPA reports on an entity's own controls over financial reporting. AT section 801 is a product of the ASB's project to clarify its standards and to converge with standards of the International Auditing and Assurance Standards Board (IAASB). The IAASB's standard for service auditors, International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, is included in its assurance standards (the equivalent of the attestation standards). Accordingly, the guidance for service auditors was moved to the attestation standards.

[Issue Date: June 2011. Revised, November 2011.]

.03 *Changes Resulting From the New AU-C Section 402 for User Auditors*

Inquiry—Does the new AU-C section 402 for user auditors contain any significant changes?

Reply—No. The new AU-C section 402 does not contain any significant changes for user auditors. However, the ASB believes that because the new AU-C section 402 is written in clarity format, it will be easier for user auditors to use and, thereby, meet their responsibilities. The new guidance for user auditors will remain in the SASs.

[Issue Date: June 2011. Revised, November 2011.]

.04 *Definition of* Service Organization *and* User Entity

Inquiry—AT section 801 uses the terms *service organization* and *user entity*. What do these terms mean?

Reply—AT section 801 defines a *service organization* as an organization or segment of an organization that provides services to user entities, which are likely to be relevant to user entities' ICFR. A service organization performs a function or task for the user entities that results in data or other information that the user entities incorporate in their financial statements. Some examples of service organizations are custodians for investment companies, mortgage servicers that service loans for others, and claims processors that process medical claims for self-insured entities. AT section 801 defines a *user entity* as an entity that uses a service organization.

[Issue Date: June 2011. Revised, November 2011.]

.05 *Effective Dates of AT Section 801 and AU-C Section 402*

Inquiry—When will AT section 801 and the new AU-C section 402 for user auditors become effective?

Reply—AT section 801 is effective for service auditors' reports for periods ending on or after June 15, 2011, with earlier implementation permitted. This is the same effective date as the effective date of the IAASB's standard for service auditors. The new AU-C section 402 for user auditors will have the same effective date as the other ASB clarified SASs.

[Issue Date: June 2011. Revised, November 2011.]

.06 *Paragraphs That Address User Auditors in AU Section 324*

Inquiry—During the period after AT section 801 becomes effective and before AU-C section 402 for user auditors becomes effective, will the guidance for service auditors in AU section 324 be deleted?

Reply—No. The guidance for service auditors and user auditors in AU section 324 is so intertwined that if the guidance for service auditors were deleted, the guidance for user auditors would not be meaningful. During the interim period before the new AU-C section 402 for user auditors becomes effective, a notation will be placed at the beginning of AU section 324 informing readers that the guidance for service auditors has been superseded by AT section 801. The guidance for user auditors can be gleaned without deleting the guidance for service auditors.

[Issue Date: June 2011. Revised, November 2011.]

.07 *Types of Reports Under AT Section 801*

Inquiry—Are there type 1 and type 2 reports under AT section 801?

Reply—Yes, AT section 801 enables practitioners to provide two types of service auditor's reports. In both reports the service organization must prepare a description of its system that includes, among other things, the nature of the service provided, how the service is performed, and the service organization's controls and related control objectives as they relate to the service provided. 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 they were intended to achieve. Both reports are examination reports, which means the practitioner obtains a high level of assurance.

[Issue Date: June 2011. Revised, November 2011.]

.08 *Changes Introduced by AT Section 801*

Inquiry—Does the implementation of AT section 801 result in significant changes to a service auditor's engagement?

Reply—The following are the three major changes introduced by AT section 801:

1. Management of the service organization will now be required to provide the service auditor with a written assertion about the fairness of the presentation of management's description of the service organization's system, the suitability of the design of the controls included in the description and, in a type 2 engagement, the operating effectiveness of those controls. That assertion will either be attached to or included in the service organization's description of its system.
2. In a type 2 engagement, the description of the service organization's system and the service auditor's opinion on the description will cover a period (the same period as the period covered by the service auditor's tests of the operating effectiveness of controls). In AU section 324, the description of the service organization's system in a type 2 report was as of a specified date, rather than for a period.
3. The service auditor is required to identify, in the description of tests of controls, any tests of controls performed by the internal audit function (other than those performed in a direct assistance capacity) and the service auditor's procedures with respect to that work. Tests of controls are procedures designed to evaluate the operating effectiveness of controls in achieving the control objectives stated in management's description of the service organization's system.

The following are other differences introduced by AT section 801:

- Suitable criteria are used by management to measure and present the subject matter and by the service auditor to evaluate the subject matter. Paragraphs .14–.16 of AT section 801 provide suitable criteria for the fairness of the presentation of a service organization's description of its system and the suitability of the design and operating effectiveness of its controls. Criteria are the standards or benchmarks used to measure and present the subject matter and against which the service auditor evaluates the subject matter.
- The service auditor's examination report contains the report elements identified in paragraph .85 of AT section 101, *Attest Engagements* (AICPA, *Professional Standards*). Paragraphs .52–.53 of AT section 801 tailor these report elements to a service auditor's engagement.
- The service auditor may not use evidence obtained in prior engagements about the satisfactory operation of controls in prior periods to provide a basis for a reduction in testing in the current period, even if it is supplemented with evidence obtained during the current period.
- AT section 801 specifically states that it is not applicable when the service auditor is reporting on controls at a service organization relevant to subject matter other than user entities' ICFR (such as controls related to regulatory compliance or privacy).

[Issue Date: June 2011. Revised, November 2011.]

.09 *Implementation Guidance for Reporting on Controls at a Service Organization Under AT Section 801*

Inquiry—Has the existing AICPA Guide *Service Organizations: Applying SAS No. 70, as Amended* (commonly known as the SAS 70 guide)[1] been rewritten to reflect AT section 801?

Reply—Yes. AICPA Guide *Service Organizations: Applying SAS No. 70, as Amended* was rewritten to reflect the requirements and guidance in AT section 801 and is now available as AICPA Guide *Service Organizations, Applying SSAE No. 16*, Reporting on Controls at a Service Organization (SOC 1) (SOC 1[2] guide).

[Issue Date: June 2011. Revised, November 2011.]

.10 *Illustrative Assertion for Management of Service Organization in an SSAE No. 16 Engagement*

Inquiry—Where can I find an illustrative management assertion for an SSAE No. 16 engagement?

Reply—Exhibit A, "Illustrative Assertions by Management of a Service Organization," of AT section 801 contains illustrative management assertions for type 1 and type 2 engagements. In addition, appendix B, "Illustrative Service Auditor's Reports," of the SOC 1 guide contains illustrative type 2 reports that include management assertions.

[Issue Date: June 2011. Revised, November 2011.]

---

[1] Prior to the issuance of Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*, AT sec. 801), the guidance for service auditors reporting on controls at a service organization and for user auditors auditing the financial statements of a user entity was contained in Statement on Auditing Standards (SAS) No. 70, *Service Organizations* (AICPA, *Professional Standards*, AU sec. 324) (issued April 1992). Since then, reports on controls at a service organization frequently have been called "SAS 70 reports," and the related AICPA Guide *Service Organizations, Applying SAS No. 70, as Amended* has been called the "SAS 70 guide."

[2] The AICPA has introduced the service organization controls (SOC) series of reports, which are further explained in section 9530.02, "Service Organization Controls Reports." Engagements performed under AT section 801 have been designated as SOC 1 engagements. AICPA Guide *Service Organizations, Applying SSAE No. 16,* Reporting on Controls at a Service Organization *(SOC 1)* is referred to as the SOC 1 guide.

.11 *Illustrative Assertion for Management of Subservice Organization in an SSAE No. 16 Engagement*

Inquiry—AT section 801 requires management of a subservice organization to provide a written assertion when the inclusive method is used. AT section 801 contains illustrative management assertions for management of a service organization. Is an illustrative assertion for management of a subservice organization available?

Reply—Yes. Example 2 of appendix B of the SOC 1 guide contains an illustrative assertion for an inclusive engagement.

[Issue Date: June 2011. Revised, November 2011.]

.12 *Another CPA Firm Acts as the Accounting Department for Your Client—Auditor Responsibility*

Inquiry—An auditor is in the process of planning an audit for a client and determines that significant accounting and financial reporting processes and controls are performed by an outside CPA firm. What is the auditor's responsibility with respect to the functions performed by the other CPA firm?

Reply—Paragraph .01 of AU section 314, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* (AICPA, *Professional Standards*), states that the auditor must obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risks of material misstatements of the financial statements. Therefore, the auditor's responsibility is the same regardless of whether the client designs and operates its own accounting processes and controls or whether those processes and controls are outsourced to a third party.

Assuming that the other CPA firm has not undergone a type 1 or type 2 service auditor's examination and, therefore, cannot provide user entities with such a report, the auditor may obtain the necessary understanding by visiting the other CPA firm's office where the information is processed to understand how the processes and controls have been designed and whether those controls have been implemented.

If the auditor intends to rely on any of the controls performed by the other CPA firm, then those controls would need to be tested to determine if they are operating effectively, just as they would if the controls had been implemented by the client.

[Issue Date: November 2011.]

.13 *Placement of Management's Assertion in an SSAE No. 16 Engagement*

Inquiry—Does AT section 801 require that management's assertion accompany the service organization's description of its system?

Reply—Yes. Paragraph .09(c)(vii) of AT section 801 states that one of the conditions for engagement acceptance or continuance is that management provide a written assertion that will be included in or attached to management's description of the service organization's system.

[Issue Date: November 2011.]

.14 *Type 2 Reports That Cover Less Than a Six-Month Period*

Inquiry—Does AT section 801 require that a type 2 report cover a minimum period? If so, does that period differ from the minimum period in AU section 324?

Reply—Both AT section 801 and AU section 324 discourage the service auditor from performing a type 2 engagement that covers a period of less than six months. Paragraph .A42 of AT section 801 indicates that a type 2 report that covers a period that is less than six months is unlikely to be useful to user entities and their auditors. However, there are certain limited circumstances, such as the following, in which a type 2 report covering less than six months may be considered:

- The service auditor was engaged close to the date by which the report on controls is to be issued, precluding the service auditor from testing the operating effectiveness of controls for a six month period.
- The service organization or a particular system or application has been in operation for less than six months.
- Significant changes have been made to the controls, and it is not practicable either to wait six months before issuing a report or to issue a report covering the system both before and after the changes.

[Issue Date: November 2011.]

.15 *Information About Relevant IT Control Objectives and Related Controls in Description of Service Organization's System*

Inquiry—Does AT section 801 require that management's description of the service organization's system include a description of the service organization's IT control objectives and related controls? If so, does the SOC 1 guide address which IT control objectives and controls would usually be relevant to a user entity's ICFR?

Reply—The definition of *service organization's system* in paragraph .07 of AT section 801 indicates that the description of the service organization's system includes the policies and procedures designed, implemented, and documented by management of the service organization to provide user entities with the services covered by the service auditor's report. Paragraph .A11 of AT section 801 further clarifies that sentence: "The policies and procedures referred to in the definition of service organization's system refer to the guidelines and activities for providing transaction processing and other services to user entities and include the infrastructure, software, people, and data that support the policies and procedures." Paragraph 3.65 of the SOC 1 guide indicates that if the control objectives in a service organization's description of its system only address application controls, and the proper functioning of general computer controls is necessary for the application controls to operate effectively, the service organization would be expected to include the relevant general computer controls in its description of the system as they relate to the specified control objectives. Appendix D, "Illustrative Control Objectives for Various Types of Service Organizations," of the SOC 1 guide includes illustrative control objectives related to general computer controls.

[Issue Date: November 2011.]

.16 *Identification of Risks in the Description of the Service Organization's System*

Inquiry—Does the service organization's description of its system need to identify the risks that could prevent the service organization's controls relevant to user entities ICFR from achieving the related control objectives?

Reply—AT section 801 does not require that management identify, in its description of the service organization's system, the risks related to each control objective included in the description. However, the service auditor would probably expect management to be able to discuss its consideration of risks in designing the controls to achieve the related control objectives.

[Issue Date: November 2011.]

.17 *Information About the Risk Assessment Process to Be Included in the Description*

Inquiry—Paragraph .14 of AT section 801 indicates that management's description of a service organization's system should include aspects of the service organization's risk assessment process. What information should be included in describing the risk assessment process?

Reply—The content of the description of the risk assessment process will vary depending on the complexity of the service organization's process. Paragraph .A18 of AT section 801 indicates that management may have a formal or informal process for identifying relevant risks. A formal process may include estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. In those circumstances, nothing precludes management from including the details of its process in the description. However, because control objectives relate to the risks that controls seek to mitigate, paragraph .A18 of AT section 801 indicates that thoughtful identification by management of the control objectives when designing, implementing, and documenting the service organization's system may itself comprise an informal process for identifying relevant risks.

[Issue Date: November 2011.]

.18 *Purpose of SSAE No. 16 Reports and SAS No. 70 Reports*

Inquiry—Will entities now become "SSAE 16 certified"?

Reply—No. A popular misconception about SAS No. 70, *Service Organizations* (AICPA, *Professional Standards*, AU sec. 324), is that a service organization becomes "certified" as SAS No. 70 compliant after undergoing a type 1 or type 2 service auditor's engagement. No such certification exists under AU section 324 nor does it exist under AT section 801. An SSAE No. 16 report (as with a SAS No. 70 report) is primarily an auditor-to-auditor communication, the purpose of which is to provide user auditors with information about controls at a service organization that are relevant to the user entities' ICFR.

[Issue Date: November 2011.]

.19 *Providing a Service Organization With a Bridge Letter*

Inquiry—May a service auditor provide a service organization with a *bridge letter* under AT section 801 (a letter from a service auditor stating that nothing has changed since the last type 1 or type 2 report)*?*

Reply—No. Neither AU section 324 nor AT section 801 addresses such letters or reports. A service organization may choose to issue a letter that describes updates or changes in its controls since the previous type 1 or type 2 report. However, there are no provisions in AT section 801 for service auditors to report on such a letter. Service auditors and user auditors are cautioned against providing assurance on or inferring assurance from such letters, respectively.

[Issue Date: November 2011.]

.20 *Format of Type 1 and Type 2 SSAE No. 16 Reports*

Inquiry—Other than the addition of management's assertion and changes to the auditor's report, will the format of the SSAE No. 16 report package be the same as it was under AU section 324?

Reply—Except for the addition of management's assertion, AT section 801 continues to have the same report package as it did under AU section 324. That package consists of the following components:

- Section 1: The service auditor's report, that is, the letter from the service auditor
- Section 2: Management of the service organization's written assertion
- Section 3: Management's description of the service organization's system
- Section 4: The service auditor's description of tests of the operating effectiveness of controls and results of those tests (type 2 reports only)
- Section 5: Optional other information provided by management of the service organization

[Issue Date: November 2011.]

.21 *Understanding Internal Control in Audit of a Service Organization's Financial Statements When Also Reporting on Service Organization's Controls Under AT Section 801*

Inquiry—If an auditor performs an SSAE No. 16 engagement for a service organization and also audits that service organization's financial statements, when auditing the service organization's financial statements, will the auditor still need to obtain a sufficient understanding of the service organization and its environment, including its internal control, sufficient to assess the risk of material misstatement and design audit procedures?

Reply—In an SSAE No. 16 engagement, the service auditor focuses on controls at the service organization that are relevant to the *user entities'* ICFR, rather than controls at the service organization that are relevant to the *service organization's* ICFR. Some of the controls included in the service organization's description of its system may be relevant to the service organization's ICFR, but because controls evaluated and tested for the purposes of an SSAE No. 16 engagement are not necessarily controls that affect the service organization's financial reporting, the auditor of the service organization's financial statements would still need to obtain an understanding of the service organization's internal control for the purpose of the audit.

[Issue Date: November 2011.]

.22 *Determining Control Objectives and Controls in an SSAE No. 16 Engagement*

Inquiry—Does AT section 801 define or suggest specific control objectives for service organizations that provide services that are likely to be relevant to user entities' ICFR or does the service organization continue to define its own control objectives and controls, as is the case in AU section 324?

Reply—AT section 801 does not define or suggest specific control objectives for service organizations that provide services that are likely to be relevant to user entities' ICFR. In an SSAE No. 16 engagement, the service auditor evaluates whether the service organization's controls were suitably designed or operating effectively by determining whether the control objectives specified by management of the service organization were achieved. AT section 801 requires that the control objectives be reasonable in the circumstances. Although most service organizations that provide similar services will have similar control objectives, in order for control objectives to be reasonable in the circumstances, they should reflect features of the particular service organization, such as the nature of the services provided, the industry in which the user entity operates, and the needs of the user entities. Accordingly, in SSAE No. 16 engagements, not all service organizations will have the same control objectives. However, certain control objectives are typical for certain types of service organizations. To assist service auditors, appendix D of the SOC 1 guide contains illustrative control objectives for various types of service organizations, including application service providers, claims processors, credit card payment processors, investment managers, payroll processors, and transfer agents. The appendix also includes illustrative general control objectives that may be applicable to any service organization.

[Issue Date: November 2011.]

.23 *Reporting Under International Standard on Assurance Engagements 3402,* Assurance Reports on Controls at a Service Organization

Inquiry—AT section 801 is based on ISAE 3402. May a U.S. CPA perform and report on a service auditor's engagement under ISAE 3402?

Reply—Unless they also meet the international requirements, a U.S. CPA could not issue a stand-alone ISAE 3402 report. However, a U.S. CPA could issue a report indicating the examination was performed in accordance with AICPA and IAASB standards, assuming that the requirements of both standards have been met.

[Issue Date: November 2011.]

.24 *Engagements Performed Under AICPA and IAASB Standards*

Inquiry—Under what circumstances would a service organization request that the service auditor report under both AICPA and IAASB standards?

Reply—Engagements performed under AT section 801 and ISAE 3402 are very similar. (Exhibit B, "Comparison of Requirements of Section 801, *Reporting on Controls at a Service Organization*, With Requirements of International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*," of AT section 801 identifies differences between AT section 801 and ISAE 3402.) For service organizations with international operations or international clients, there may be a benefit to obtaining a report indicating that the examination was performed in accordance with AICPA and IAASB standards. An engagement that is performed in accordance with both sets of standards would not be expected to involve a substantially different examination scope or approach than an individual SSAE No. 16 engagement would.

[Issue Date: November 2011.]

.25 *Applying AT Section 801 Internationally*

Inquiry—If a service organization in the United States provides services to a user entity in Europe, may the practitioner perform the examination under AT section 801 or should it be performed under ISAE 3402?

Reply—The applicability of AT section 801 is not limited to user entities located in the United States. Accordingly, a user entity in Europe could be a recipient of an SSAE No. 16 report.

[Issue Date: November 2011.]

.26 *Reporting on Controls at a Service Organization Relevant to Subject Matter Other Than User Entities' ICFR*

Inquiry—May AT section 801 be used for reporting on a service organization's controls relevant to subject matter other than user entities' ICFR?

Reply—No. AT section 801 does not apply to examinations of controls over subject matter other than user entities' ICFR. In the past, some CPAs used AU section 324 to report on controls at a service organization relevant to subject matter other than user entities' ICFR. However, AU section 324 was never intended for such reporting, and neither is AT section 801. Paragraph .A2 of AT section 801 clarifies this point, and paragraph .02(a) of AT section 801 indicates that AT section 801 may be helpful to practitioners in developing and performing such engagements under AT section 101. AT section 101 provides a framework that enables practitioners to develop engagements and report on subject matter other than financial statements. For example, an entity may be required by law or regulation to maintain the privacy of the information it collects from its customers. Such information may be passed on to a service organization that performs certain tasks for the user entity. Even though certain controls over the privacy of the information are implemented by the service organization, management of the user entity is not relieved of its responsibility for effective internal control over the privacy of the information it processes for the user entity. In this situation, management of the service organization may engage a CPA to report on the effectiveness of its controls over privacy that are relevant to the user entities, and it may provide that report to the user entities and other specified parties identified in the report. Such an examination would be performed under AT section 101, not AT section 801. The increasing use of *cloud computing* companies (that provide user entities with on-demand network access to a shared pool of computing resources, such as networks, servers, storage, applications, and services) has created an increasing demand for CPAs to report on a cloud computing service organization's controls relevant to subject matter other than user entities' ICFR.

[Issue Date: November 2011.]