Ms. Sharon Macey
Audit and Attest Standards
American Institute of Certified Public Accountants
1211 Avenue of the Americas
New York, NY 10036-8775

Proposed Statement on Standards For Attestation Engagements, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting: Clarification and Recodification* (to supersede AT section 801, *Reporting on Controls at a Service Organization, of Statements on Standards for Attestation Engagements* [AICPA, Professional Standards])

Dear Ms. Macey:

Ernst & Young LLP (Ernst & Young) is pleased to submit this comment letter to the Auditing Standards Board (ASB) in response to the ASB’s request for comment regarding the above-referenced proposed Statement on Standards for Attestation Engagements, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting* (proposed SSAE).

We support the issuance of the proposed SSAE. We believe that the changes resulting from applying the clarity drafting conventions are appropriate and their effect on the content of the proposed SSAE will be positive.

Attached are our responses to the ASB’s questions for respondents and additional comments for your consideration. We would be pleased to discuss them with members of the ASB or its staff.

Sincerely,

Ernst & Young LLP
Responses to guide for respondents

**Question 1:** Are the objectives of the practitioner in the ED appropriate?

Yes, we believe they are appropriate.

**Question 2:** Are the substantive and language changes to extant AT section 801 made by the ED appropriate?

Yes, we believe they are appropriate. Specifically, we agree with:

- Introducing and defining the term “complementary subservice organization controls” to replace “controls at a subservice organization”
- Revising the definition of “complementary user entity controls”
- Introducing requirements for the service auditor as part of the risk assessment process
- Deleting certain paragraphs within AT 801 related to the use of the internal audit function, except as set forth in the “Additional commentary on using the work of internal audit” section below
- Adding requirements for the service auditor to determine that management’s assertion includes all of the criteria management used to evaluate the fairness of the presentation of the description, the suitability of the design of the controls and, in a type 2 engagement, the operating effectiveness of the controls
- Further clarifying how a service auditor performs a risk assessment in a service auditor’s engagement
- Adding application guidance for indicating that the service auditor may include in the description of tests of controls and results the procedures the service auditor performed to verify the completeness and accuracy of information provided by the service organization
- Indicating that the alternative to obtaining the required written representations provided for in paragraph 2.44b (i.e., obtaining oral representations from the responsible party) does not apply in a service auditor’s engagement
- Deleting the phrase “in all material respects” as it relates to management’s assertion from the definitions in paragraph .07 of AT section 801 of the terms report on management’s description of a service organization’s system and the suitability of the design of controls (type 1 report) and report on management’s description of a service organization’s system and the suitability of the design and operating effectiveness of controls
- Clarifying in paragraph 8.A10 of the ED that if management’s assertion is included in the description of the service organization’s system, it should be clearly segregated from the description of the service organization’s system
Adding illustrative paragraphs to the type 1 and type 2 reports in appendix A, “Illustrative Service Auditor’s Reports,” of AT section 801


**Additional commentary on using the work of internal audit**

The proposed standard would delete the paragraphs in AT 801 related to using the work of internal auditors if those paragraphs are not specific to a service auditor’s engagement. If this information is excluded from AT 801, additional requirements and application guidance on using the work of internal auditors should be added to the proposed Chapter 2.

**Question 3: Are there considerations for less complex entities and governmental entities that should be addressed in the exposure draft?**

No, we have not identified any additional considerations for less complex entities or governmental entities.
Paragraph specific comments

Paragraph 8.A7

We recommend moving this paragraph from the application guidance on the definition of “inclusive method” (paragraph 8.8f) and inserting it immediately after paragraph 8.10.

Paragraph 8.A8

Paragraph 8.A8 provides guidance on performing procedures at a subservice organization and references to paragraph 8.8f. We recommend deleting the reference to paragraph 8.8f and referencing this guidance in the new requirement included in paragraph 8.A7.

Paragraph 8.8g

Paragraph 8.8g currently defines the term “report on management’s description of a service organization’s system and the suitability of the design of controls” as a document that includes the following components:

- Management’s description of the service organization’s system

- A written assertion by management of the service organization about whether, based on suitable criteria:
  - Management’s description of the service organization’s system fairly presents the service organization’s system that was designed and implemented as of a specified date
  - The controls related to the control objectives stated in management’s description of the service organization’s system were suitably designed to achieve those control objectives as of the specified date
  - A service auditor’s report that expresses an opinion on the matters set forth in management’s assertion

Using the term “report on management’s description of a service organization’s system and the suitability of the design of controls” to refer to the entire Type 1 document rather than just the service auditor’s report can create the impression that the service auditor is responsible for the system’s description. A more appropriate term would be “management’s description of a service organization system and service auditor’s report on that description and the suitability of design of controls” (referred to in this chapter as type 1 report). We recommend that similar changes be made to paragraph 8.8h.
Paragraph 8.8m

Paragraph 8.8m defines a subservice organization as “a service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities’ internal control over financial reporting.” Currently, this definition is applied inconsistently, resulting in these entities being treated differently in service organization reports. We recommend including additional application guidance to assist service organizations and service auditors in determining whether a service provider to a service organization meets the definition of a subservice organization. Such guidance should take into consideration the objective of a user auditor provided in AU-C section 402 paragraph 07:

The objectives of the user auditor, when the user entity uses the services of a service organization, are to

a) Obtain an understanding of the nature and significance of the services provided by the service organization and their effect on the user entity’s internal control relevant to the audit, sufficient to identify and assess the risks of material misstatement.

b) Design and perform audit procedures responsive to those risks.

We suggest including the following application guidance:

A service provider to a service organization is likely to be a subservice organization if either of the following is true:

► A user auditor is likely to require an understanding of the service provider’s services to obtain an understanding of the nature and significance of the service provided by the service organization.

► Testing the service provider’s controls would permit the user auditor to reduce the assessment of control risk. Tests of controls at a subservice organization usually permit the user auditor to reduce the assessment of control risk at the user entity only if the controls at the subservice organization are necessary to achieve or help achieve one (or more) control objective.

Paragraph 8.A9

Paragraph 8.A9 provides application guidance to assist the service auditor in determining whether controls at a service provider to a service organization are relevant to user entities’ internal control over financial reporting; however, it does not address when the understanding of the subservice organization’s services is necessary for the user auditor to obtain an understanding of the nature and significance of the service provided by the service organization. In such situations, the service organization should use either the inclusive method or the carve-out method for the subservice organization within the description. We recommend rewording the application guidance as follows:

There may be instances when the service organization’s controls (especially monitoring controls) related to services provided by another entity, make it unnecessary for the user auditor to understand controls at the other entity in order to obtain an understanding of the service
organization's system or reduce the assessment of control risk. permit the service organization to include in its assertion the relevant aspects of the subservice organization's system, including the relevant control objectives and related controls of the subservice organization. In such instances, management's description does not treat the entity as a subservice organization and the service auditor’s opinion is based solely on the controls at the service organization, and hence, the inclusive method is not applicable.

Because this guidance addresses whether the service provider of the service organization is a subservice organization, we recommend including it in paragraph 8.8m rather than in the definition of inclusive method.

**Paragraph 8.A10**

Paragraph 8.A10 provides guidance on the presentation of management’s assertion in the document that contains management’s description of its system and the associated service auditor’s report. This application guidance addresses management’s assertion that accompanies management’s description of its system as set forth in 8.10b (vi). It does not provide application guidance on the definitions in 8.8g(ii) or 8.8h(ii) of a report on management’s description of a service organization’s system and the suitability of design of controls or a report on management’s description of a service organization’s system and the suitability of design and operating effectiveness of controls, respectively. We recommend that the references to 8.8g(ii) and 8.8h(ii) be removed from paragraph 8.A10 and that the paragraph be inserted after paragraph 8.A18 to align with the requirement in 8.10b(iv) regarding management’s responsibility for providing a written assertion to accompany the description.

**Paragraph 8.A35**

The fifth bullet of paragraph 8.A35 contains the following sentence: “If the carve-out method has been used, the description need not describe the detailed processing or controls at the subservice organization.” Because a service auditor does not perform procedures at a subservice organization when management’s description of a system is prepared using the carve-out method, the service auditor does not have a basis for concluding that detailed information on the processing or controls at a subservice organization is fairly stated. We suggest revising the bullet as follows:

If the inclusive method has been used, does the description separately identify controls at the service organization and controls at the subservice organization? If the carve-out method is used, does the description identify the functions that are performed by the subservice organization and include controls at the service organization that monitor the effectiveness of controls at the subservice organization? If the carve-out method has been used, the description need does not describe the detailed processing or controls at the subservice organization. (Ref. par8.8f and8.23d)

**Paragraph 8.A37**

Paragraph 8.A37 provides application guidance regarding the term “reasonable in the circumstances.” In current practice, this term is applied inconsistently, resulting in significant variation in the coverage of control objectives in service organization reports issued by different service auditors. Furthermore, the language “if the control objectives are specified by an outside party, including control objectives
specified by law or regulation, the outside party is responsible for their completeness and reasonableness" creates an impression that control objectives specified by an outside party are always reasonable in the circumstances. While the specification of control objectives by an outside party provides evidence of their reasonableness in the circumstances, this evidence is inconclusive. Such outside parties may not have sufficient knowledge or understanding to make a definitive determination on completeness of the control objectives for a broad range of users of the system. We recommend revising the guidance as follows:

8.A37 Control objectives are the aim or purpose of specified controls at the service organization and address the risk that controls are intended to mitigate. For reports prepared in accordance with this chapter, these risks are the risks that the service organization's system represents to user entities' internal control over financial reporting. Paragraph 8.23a requires the service auditor to evaluate whether the control objectives stated in management's description of the service organization's system are reasonable in the circumstances. The control objectives are usually reasonable in the circumstances if they address the risks that the service organization's system represents to user entities' internal control over financial reporting. Considering the following questions may assist the service auditor in this evaluation:

- Do the control objectives stated in the description and specified by the service organization relate to the types of assertions commonly embodied in the broad range of user entities' financial statements to which controls at the service organization could reasonably be expected to relate (for example, assertions about existence and accuracy that are affected by access controls that prevent or detect unauthorized access to the system)? Although the service auditor ordinarily will not be able to determine how controls at a service organization specifically relate to the assertions embodied in individual user entities' financial statements, the service auditor considers the following to identify the types of assertions to which the controls are likely to relate:
  - The types of services provided, including the classes of transactions processed
  - The contents of reports and other information prepared for user entities
  - The information used in the performance of procedures
  - The types of significant events other than transactions that occur in providing the services
  - The responsibility of the service organization to implement controls, including responsibilities established in contracts and agreements with user entities
  - The risks to a user entity's internal control over financial reporting arising from information technology used or provided by the service organization

- controls, and the services being provided is used to identify the types of assertions to which those controls are likely to relate.
Are the control objectives stated in the description and specified by the service organization complete? Although a complete set of control objectives can provide a broad range of user auditors with a framework to assess the effect of controls at the service organization on assertions commonly embodied in user entities' financial statements, the service auditor ordinarily will not be able to determine how controls at a service organization specifically relate to the assertions embodied in individual user entities' financial statements and cannot, therefore, determine whether control objectives are complete from the viewpoint of individual user entities or user auditors. It is the responsibility of individual user entities or user auditors to assess whether the service organization's description addresses the particular control objectives that are relevant to their needs.

Have the control objectives stated in the description been specified by the service organization or by outside parties, such as regulatory authorities, a user group, a professional body, or others? If the control objectives are specified by an outside party, including control objectives specified by law or regulation, such specification may provide sufficient evidence of the outside party is responsible for their completeness and reasonableness of the control objectives.

Paragraph 8.A45

Paragraph 8.A45 states 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.” We believe that this statement is no longer appropriate for the following reasons:

AU-C 402 does not provide user auditors with guidance on a specific minimum acceptable coverage period but requires the user auditor to determine whether the report provides sufficient appropriate evidence (AU-C 402. 17) and provides guidance when additional appropriate evidence is necessary (AU-C 402 .A32-A40).

A type 2 report that addresses a period of less than six months of the user entity's financial period continues to provide a user auditor with evidence of the suitability of design and operating effectiveness of controls for a portion of the period being audited. This reduces the amount of evidence that the user auditor needs to obtain that is relevant to the service organization.

In many situations, the service auditor may conclude that a type 2 report covering a six-month period is insufficient to meet his or her needs without obtaining additional evidence. In practice, service organizations have used the six-month-minimum-period guidance set forth in this paragraph to justify not providing a report that covers longer periods. This has resulted in reports that do not meet the needs of user auditors.

We recommend removing the reference to a minimum period from the standard and suggest the following language:

8.A45. 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. If management's description of the service organization's system covers a period that is less than twelve months, it is often useful to the auditor if the
The description may describe the reasons for the shorter period and the service auditor's report may include that information as well. Circumstances that may result in a report covering a period of less than six months include the following:

- The service auditor was engaged close to the date by which the report on controls is to be issued, and controls cannot be tested for operating effectiveness 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. (Ref: par. 8.26 and 8.27)

**Paragraph 8.25**

Paragraph 8.10(b)(v) states that management is responsible for “identifying the risks that threaten the achievement of the control objectives stated in the description and designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the control objectives stated in the description of the service organization's system will be achieved.” However, paragraph 8.25 states that “the service auditor should determine which of the controls at the service organization are necessary to achieve the control objectives and...” The determination by the service auditor of the controls necessary to achieve the control objectives conflicts with the previous guidance on management's responsibility for identifying the risks that threaten the achievement of the control objectives and designing, implementing and operating controls to achieve the control objectives and results in an assumption of management's responsibility in the controls' achievement of the control objectives.

In addition, paragraph 8.25 requires the service auditor to identify the risks that threaten the achievement of the control objectives. We believe that it also may be appropriate for the service auditor to obtain and evaluate management's identification of the risks that threaten the achievement of the control objectives in lieu of performing a separate independent evaluation of the risks.

We suggest the following revisions to paragraphs 8.25 and 8.26:

8.25 The service auditor should determine which of the controls at the service organization are necessary to achieve the control objectives stated in management's description of the service organization's system and should assess whether the those controls identified by management as achieving the control objectives were suitably designed to achieve the control objectives by (Ref: par: 8.A26-8.A27 and 8.A39-8.A42)

a. obtaining management's documentation of its identification of the risks that threaten the achievement of the control objectives stated in management's description of the service organization's system and assessing the completeness of management's identification of the risks or independently identifying the risks that threaten the achievement of the control objectives stated in management's description of the service organization's system, and (Ref: par. 8.39)
b. evaluating the linkage of the controls identified in management's description of the service organization's system with those risks.

**Paragraph 8.26**

Consistent with the change recommended above, paragraph 8.26 should be revised as follows:

8.26 When performing a type 2 engagement, the service auditor *should* test those controls that *the service auditor has determined* are necessary to achieve the control objectives stated in management's description of the service organization's system and *should* assess their operating effectiveness throughout the period. Evidence obtained in prior engagements about the satisfactory operation of controls in prior periods does not provide a basis for a reduction in testing, even if it is supplemented with evidence obtained during the current period. (Ref: par. 8.A26–8.A28, and 8.A43–8.A48)

The intention of having the service auditor identify the controls necessary to achieve the control objectives lies in the fact that the service auditor can best determine which controls are most effective in achieving the control objectives and which are most efficient to test. In order to retain the benefit of efficient testing of effective controls, we recommend providing additional guidance in paragraph 8.26 to address those situations where a service organization identifies more controls than are necessary to achieve the control objectives. We propose including the following guidance:

The service auditor determines the nature, timing and extent of testing to assess the operating effectiveness of the controls necessary to achieve the control objectives stated in management's description of the service organization's system. When determining the nature, timing and extent of testing of each control, the service auditor may consider the relative effectiveness of each control in the set of controls necessary to achieve each control objective and accordingly vary the nature, timing and extent of testing of individual controls based on the effectiveness of each control. The service auditor also may consider the efficiency with which testing can be performed when determining the nature, timing and extent of testing.