December 18, 2014

Ms. Sharon Macey
American Institute of Certified Public Accountants
1211 Avenue of the Americas, 19th Floor
New York, NY 10036-8775

Re: 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

Dear Ms. Macey:

Deloitte & Touche LLP appreciates the opportunity to respond to the request by the American Institute of Certified Public Accountants (AICPA) for public comment on the proposed Statement on Standards for Attestation Engagements (SSAE), Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting: Clarification and Recodification (the “proposed SSAE”). We are supportive of the proposed SSAE and believe that the clarification and recodification was completed in accordance with the clarity conventions and criteria adopted by the AICPA’s Auditing Standards Board (ASB).

We have responded to questions posed in the explanatory memorandum and provided overall comments on the proposed SSAE, as well as on specific paragraphs. In our recommendations for specific changes, additions are noted in bold underline and deletions are noted in strike-through text. Where text has been moved, this is noted by double underline.

Response to the Issue for Consideration in the Explanatory Memorandum

Does the revised structure facilitate understanding and implementation of the standards?

In general, the concept of the revised structure does facilitate the understanding and implementation of the subject-matter specific attestation standards.

Responses to Questions Posed in the Explanatory Memorandum

1. Are the objectives of the practitioner in the ED appropriate?

We believe that the objectives to be achieved by the practitioner are appropriate.
2. Are the substantive and language changes to extant AT section 801 made by the ED appropriate? (The disposition of the requirements in extant AT section 801 are shown in the supplement to this exposure draft described subsequently.)

While in general we believe the substantive and language changes to extant AT section 801, Reporting on Controls at a Service Organization (extant AT section 801), made by the proposed SSAE are appropriate, we do have specific comments relating to the requirements, and application and other explanatory material paragraphs that are addressed below.

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

While there is only limited guidance in the proposed SSAE with respect to smaller, less complex entities and governmental entities, we do not believe any additional specific guidance for these types of entities is necessary.

**Overall Comment**

**Internal Audit**

We noted in the Explanatory Memorandum to the proposed SSAE that certain paragraphs in extant AT section 801 related to using the work of internal auditors were deleted if they were not specific to a service auditor’s engagement. We understand that additional requirements and application guidance pertaining to using the work of internal auditors is being considered for inclusion in chapter 2, Examination Engagements.¹ This would also have the added benefit of applying to other attestation examination engagements such as Statement of Position 07-2, Attestation Engagements That Address Specified Compliance Control Objectives and Related Controls at Entities That Provide Services to Investment Companies, Investment Advisors, or Other Service Providers, and Service Organization Controls ("SOC") 2 engagements. However, if the additional requirements and application guidance are not included within chapter 2, we recommend that they be incorporated into this proposed SSAE. When developing the requirements and application guidance to be incorporated into the attestation standards, we encourage the ASB to conform to the language that is included in AU-C Section 610, Using the Work of Internal Auditors.

¹ See Proposed Statement on Standards for Attestation Engagements, Attestation Standards: Clarification and Recodification, issued by the Auditing Standards Board on July 24, 2013.
Paragraph-Specific Comments

Paragraph 8.A2

We noted that the reference to the AICPA guide, *Prospective Financial Information*, in chapter 5, *Financial Forecasts and Projections*, is included as an introductory paragraph, and is not included as application material. Consequently, we recommend consistent placement of this paragraph throughout the SSAEs. Further, we recommend changing the order of the sentences in paragraph 8.A2 so that the requirement to consider applicable interpretive publications precedes the listed interpretive guidance. The suggested modification as follows:

8.A2. Chapter 1 requires the practitioner to consider applicable interpretive publications when planning and performing an attestation engagement. Additional interpretive guidance for a practitioner examining controls at a service organization relevant to user entities’ internal control over financial reporting is provided in the AICPA guide *Service Organizations: Reporting on Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting*. Chapter 1 requires the practitioner to consider applicable interpretive publications when planning and performing an attestation engagement. (Ref: par. 8.2)

Paragraph 8.A4

We believe that in the current context the word “issues” may have been inappropriately used and that the identifications of these matters may ultimately result in issues needing to be addressed by the service auditor. We recommend the following edit to the paragraph:

8.A4. When a service auditor conducts an engagement under chapter 2 to report on controls at a service organization other than those controls likely to be relevant to user entities’ internal control over financial reporting, and the service auditor intends to use the guidance in this chapter in planning and performing that engagement, the service auditor may encounter issues that differ significantly from those associated with engagements to report on a service organization’s controls likely to be relevant to user entities’ internal control over financial reporting. The following are examples of such issues:

Further, given how closely aligned the SOC 2 engagement is to an engagement to report under the proposed SSAE, we believe that the application material should make an explicit statement to address SOC 2 engagements. See the following recommended application material paragraph:

8.A4x. The guidance in this chapter may be adapted and applied, as applicable, when a practitioner performs an examination of a service organization’s description of its systems and controls that are likely to be relevant to the security, availability, or processing integrity of a service organization’s system or the

---

confidentiality or privacy of the information processed by the system. Such an engagement is referred to as a service organization controls (SOC) 2 engagement, and a report on that engagement is referred to as a SOC 2 report. (Ref: par. 8.3a)

Paragraph 8.5

This requirement paragraph appears to be an exception to applying the concepts and requirements in chapter 2 and therefore we recommend moving paragraph 8.5 to follow immediately after paragraph 8.2.

Paragraph 8.6

We recommend that the effective date be for periods on or after June 15, as this timing will allow for those service auditor’s reports using the proposed SSAE, to be available to the user auditor reporting on the financial statements with an upcoming calendar year-end. Early implementation would continue to be permitted. This was consistent with the approach used in SSAE No. 16, Reporting on Controls at a Service Organization (AICPA, Professional Standards, AT sec. 801) (“SSAE 16” or “AT section 801”).

Paragraph 8.7a

We recommend modifying paragraph 8.7a[i] to include language to note that type 1 reports are as of a specified date as follows:

8.7. The objectives of the service auditor are to

   a. obtain reasonable assurance about whether, in all material respects, based on suitable criteria,

      i. management’s description of the service organization’s system fairly presents the service organization’s system that was designed and implemented throughout the specified period: (or in the case of a type 1 report, as of a specified date).

      ii. ...

Paragraph 8.8b

We believe that the inclusion of the phrase “carved out subservice organization” in the definition of complementary service organization controls in paragraph 8.8b restricts the defined term to only carve-out situations. We believe that the definition should be broader to encompass any situations in which subservice organizations exist. Accordingly, we recommend modifying paragraph 8.8b as follows:

8.8b. Complementary subservice organization controls. Controls that management of the service organization assumes, in the design of the service organization’s system, will be implemented by carved out the subservice organizations, and are necessary
to achieve the control objectives stated in management’s description of the service organization’s system.

**Paragraph 8.8c**

We believe that the definition as written in paragraph 8.8c is too narrow and may result in management not including “core” complementary user entity controls in management’s description of the service organization’s system (e.g., requiring the proper authorization of transactions provided by the user entity to the service organization or ensuring that the transactions submitted to the service organization are complete and accurate). We recommend using the definition in extant AT section 801, with minor edits, and adding new application material to paragraph 8.8c to clarify what complementary user entity controls are relevant, as illustrated in paragraph 8.A5x below. The proposed wording in paragraph 8.A5x is based on language in the AICPA guide, *Service Organizations: Reporting on Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting* (the “SOC 1 guide”), paragraph 3.49. The proposed revisions are as follows:

8.8c. Complementary user entity controls. Controls that management of the service organization assumes, in the design of the service organization’s system, will be implemented by user entities, and which, if necessary to achieve the control objectives stated in management’s description of the service organization’s system, are identified as such in that description. (Ref: par. 8.A5x)

8.A5x. Meaningful complementary user entity controls are specific and relevant to the services provided by the service organization applicable to user entities’ internal control over financial reporting. Providing a long list of generic “good practice” controls generally is not helpful to user entities and their auditors. (Ref: par. 8.8c)

**Paragraphs 8.8d and 8.8e**

We recommend adding application material to paragraph 8.8d to clarify that there is a direct link between the control objectives at the service organization and internal control over financial reporting (“ICFR”) at the user entity as well as the relevant controls. We also recommend adding application material to paragraph 8.8e to describe specific circumstances when a service organization uses another service organization to perform some of the services provided to user entities. This application material is to address the circumstances currently illustrated in the SOC 1 guide Example B in Table 3-2. A reference to the new application material would also be included in paragraphs 8.8d and 8.8e. Accordingly, we propose the following:

8.8d. Control objectives. The aim or purpose of specified controls at the service organization. Control objectives address the risks that controls are intended to mitigate. (Ref: par. 8.A5x)

8.8e. Controls at a service organization. The policies and procedures at a service organization likely to be relevant to user entities’ internal control over financial reporting. These policies and procedures are designed, implemented, and documented by the service organization to provide reasonable assurance about the
achievement of the control objectives relevant to the services covered by the service auditor’s report. (Ref: par. 8.A5x, 8.A6, and 8.A6x)

8.A5x. For purposes of this proposed SSAE, the control objectives at the service organization are relevant to the user entities’ internal control over financial reporting. The related controls achieve the control objectives outlined in management’s description of the service organization’s system. (Ref: par. 8.8d and 8.8e)

8.A6x. Where the service organization uses another service organization to perform some of the services provided to user entities, but the service organization has controls in place, including monitoring controls, such that they are able to achieve the related control objectives included in their description of the system, then the services being provided by another service organization may not be relevant to the user entities internal control over financial reporting. In such situations, there may be no need to identify another service organization in the description of the system as a subservice organization, or use the carve-out method of reporting because the service organization has sufficient controls in place. (Ref: par. 8.8e)

Paragraphs 8.8f, 8.A7 and 8.A8

We believe that paragraphs 8.A7 and 8.A8 contain performance language and as such these paragraphs should be moved out of the definition section to under the heading “Acceptance and Continuance.” We recommend reflecting paragraph 8.A7 and the first sentence of paragraph 8.A8 as new requirements directly following existing paragraph 8.11, with the balance of paragraph 8.A8 being included as related application material. Consequently, the paragraph numbers and related cross-references would also change.

We also believe that the use of the carve-out method may be inappropriate when the service auditor is unable to obtain a written assertion from the subservice organization, as noted in paragraph 8.A20x. This may represent a scope limitation that could result in the service auditor considering whether to withdraw from the engagement. The service auditor may in any event consider the implications on the examination engagement when encountering this circumstance. We recommend the following modifications:

8.8f. **Inclusive method.** Method of addressing the services provided by a subservice organization whereby management’s description of the service organization’s system includes a description of the nature of the services provided by the subservice organization as well as the subservice organization’s relevant control objectives and related controls. (Ref: par. 8.A7–8.A9 and 8.A35)

8.A711v. When the inclusive method is used, the requirements of this chapter should also apply to the services provided by the subservice organization, including the requirement to obtain management’s acknowledgement and acceptance of responsibility for the matters in paragraph 8.10b(i)–(vi) as they relate to the subservice organization. (Ref: par. 8.8f and 8.A35)
Performing procedures at the subservice organization should entail coordination and communication between the service organization, the subservice organization, and the service auditor. (Ref: par. 8.A20x) The inclusive method is generally feasible if, for example, the service organization and the subservice organization are related, or if the contract between the service organization and the subservice organization provides for issuance of a service auditor’s report. If the service auditor is unable to obtain an assertion from the subservice organization regarding management’s description of the service organization’s system provided, including the relevant control objectives and related controls at the subservice organization, the service auditor is unable to use the inclusive method but may instead use the carve-out method. (Ref: par. 8.8f)

Paragraph 8.A9

We believe that this paragraph is unclear as written and the proposed application guidance provided above in paragraph 8.A6x outlines the specific points needed regarding the circumstances being referred to. We recommend paragraph 8.A9 be deleted.

Paragraph 8.8m

We recommend adding application material to paragraph 8.8m to clarify that there may be situations in which a subservice organization of a service organization uses another subservice organization in performing services for the service organization and including a reference to the new application material in paragraph 8.8m. The suggested wording for paragraph 8.A11x is as follows:

8.A11x. There may be instances where a subservice organization of a subservice organization also exists that is, directly or indirectly, performing services for the service organization. (Ref: par. 8.8m)
Paragraph 8.8

We recommend adding application material to paragraph 8.8 to clarify situations in which the user entity uses a service organization, but the service auditor’s report only covers certain aspects of the services provided to the user entity. Consider the following example: A claims processing service organization has two SOC 1 reports, one covering its medical claims processing and one covering its pharmacy claims processing. The user entity may use a service organization for its medical claims processing, but not the service auditor’s report related to the pharmacy claims processing. Therefore, even though the user entity uses the services of the service organization itself (per the definition), they are not entitled to be a user of the pharmacy claims processing report.

Further, we recommend additional application guidance to encompass situations in which a prospective customer has requested a copy of the service auditor’s report as part of the prospective customer’s evaluation of the service organization’s control environment. A reference to the new application material, reflected as paragraphs 8.A11y and 8.A11z below with our suggested language, would also be included in paragraph 8.8. Additionally, the SOC 1 guide could include additional guidance to address situations where the prospective customer’s auditor (or the user entity’s auditor, once the prospective customer has become a user entity) also may have access to the service auditor’s report.

8.8. **User entity.** An entity that uses a service organization. *(Ref: par. 8.A11y and 8.A11z)*

8.A11y. **The services used by the user entity for the purposes of this proposed SSAE** are those included in the scope of the examination engagement. *(Ref: par. 8.8p)*

8.A11z. **A prospective customer, and their auditor, may also be considered a user entity in situations where the prospective customer is engaged in active negotiations with the service organization to provide some or all of the services described in the service auditor’s report.** *(Ref: par. 8.8p)*

Paragraph 8.10b

Consistent with our comment on paragraph 8.8d, we believe that it is important to assert that the control objectives must relate to ICFR of the user entity. We suggest including application material related to paragraph 8.10b[iv] as follows:

8.A17x. **The control objectives stated in management’s 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.** *(Ref: par. 8.10b[iv])*

Paragraph 8.A23

While we agree with the application material in paragraph 8.A23, we believe that greater clarity is needed and it would be beneficial if the guidance was expanded to include a description of the
elements that may not be appropriate if the system being described is not a system that processes transactions. We suggest including application material related to paragraph 8.A23 as follows

8.A23. Paragraph 8.13 identifies a number of elements that are included in management’s description of the service organization’s system as appropriate. These elements may not be appropriate if the system being described is not a system that processes transactions; for example, if the system relates to general controls over the hosting of an IT application but not the controls embedded in the application itself, there may not be transactions that are being initiated, authorized or recorded, and therefore would not be appropriate for inclusion in management’s description of the service organization’s system. (Ref: par. 8.13)

Paragraph 8.A27

We believe that the phrase “significant transactions” in the first bullet should be amended to delete “significant” so that management does not omit transactions that should be covered in the description. Further, in the scope paragraph of the service auditor’s report, as illustrated in paragraph 8.A71 Exhibit A: Illustrative Service Auditor’s Reports - Example 1: Type 2 Service Auditor’s Report, the description of the examination engagement is as follows: “We have examined XYZ Service Organization’s description of its system entitled … for processing user entities’ transactions … throughout the period…. .” There is no reference to “significant” transactions. In addition, the qualitative factor around design, as noted in the third bullet, should include whether, for each class of transaction and assertion (e.g. authorization, completeness, accuracy, timeliness), there exist mitigating controls. As such, we recommend the application material be modified as follows:

8.A27. …

- management’s description of the service organization’s system includes the significant aspects of the processing of significant transactions.
- management’s description of the service organization’s system omits or distorts relevant information.
- the controls have the ability, as designed, to provide reasonable assurance that the control objectives stated for each class of transaction and relevant assertion in management’s description of the service organization’s system would be achieved.

Paragraphs 8.18 and 8.19

We believe that the requirements in paragraphs 8.18 and 8.19 do not constitute risk assessment procedures. We recommend changing the heading of the section to “Obtaining an Understanding of the Service Organization’s System,” which is both more illustrative of the requirements and in line with the terminology in ISAE 3402.

We also recommend that additional application material be included for paragraph 8.18 to further expand on the service auditor’s responsibilities as it relates to obtaining an understanding of the
interrelationship between user entity financial statements and the service organization’s description of the system, as illustrated in paragraph 8.A29 below.

**8.A29x. The engagement partner may also take into consideration the engagement team’s understanding of the user entity financial statements and the interrelationship between those financial statements and the service organization’s description of the system. (Ref: par. 8.18)**

Paragraph 8.A31

We believe that this application material should be cross-referenced to requirement paragraph 8.23 We also recommend adding a reference in paragraph 8.A31 to the application material in paragraph 8.A29 in order to be consistent with extant AT section 801.

**8.A31. The service auditor’s procedures to obtain the understanding referred to in paragraph 8.A29, may include the following:**

- Inquiring of management and others within the service organization who, in the service auditor’s judgment, may have relevant information
- Observing operations and inspecting documents, reports, and printed and electronic records of transaction processing
- Inspecting a selection of agreements between the service organization and user entities to identify their common terms
- Reperforming the application of a control

One or more of the preceding procedures may be accomplished through the performance of a walkthrough. (Ref: par. 8.923)

Paragraph 8.21

While we agree with the intent of this requirement, we suggest modifying the language in paragraph 8.21, as follows, to provide for the situation where there is no internal audit function.

**8.21. In situations where there is an internal audit function, the service auditor should read the reports of the internal audit function and as well as regulatory examinations that relate to the services provided to user entities and the scope of the engagement to obtain an understanding of the nature and extent of the procedures performed and the related findings. The findings should be taken into consideration as part of the risk assessment and in determining the nature, timing, and extent of the tests.**

Paragraph 8.A33

We recommend expanding the application material in paragraph 8.A33 to include prior year qualifications in the report as a risk factor. We suggest the following modification to the
application material:

8.A33. The risks identified in paragraph 8.A32 may include those related to new or changed controls, system changes, significant changes in processing volume, new personnel or significant changes in key management or personnel, new types of transactions, or new products or technologies, or qualifications within the prior year service auditor’s report.

Paragraph 8.A35

We recommend further clarifying the application material in paragraph 8.A35 related to complementary subservice organization controls pertaining to the carve-out method as follows:

8.A35. …

- If the carve-out method has been used, does the description include complementary subservice organization controls and include monitoring controls over subservice organizations? (Ref: par. 8.8a and 8.23d)

Paragraph 8.A37

We agree with the requirement that the service auditor must evaluate the control objectives for reasonableness; however, we believe that the language in the first bullet of paragraph 8.A37 could lead the service auditor to believe that if the control objectives have been specified, that they do not need to be assessed as reasonable. We suggest the following revision:

8.A37. …

- 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, and whether the control objectives are reasonable?

Paragraph 8.A38

We recommend the following edit be made to paragraph 8.A38 to further clarify the sentence:

8.A38. The service auditor’s procedures to determine whether the system described by the service organization has been implemented may be similar to, and performed in conjunction with, procedures to obtain an understanding of that system. Other procedures that the service auditor may use in combination with inquiry of management and other service organization personnel include observation, inspection of records and other documentation, as well as reperformance of the manner in which transactions are processed through the system and controls are applied. (Ref: par. 8.23b and 8.24)

Paragraph 8.25b

We believe that application material should be added to further expand upon the requirement in
paragraph 8.25b pertaining to controls. The application material would (1) note that controls are needed to address each assertion within the control objectives listed in management’s description of the service organization’s system and (2) address the concept of classes of transactions and that multiple controls may be needed in order for the service auditor to conclude on the design of controls relating to each assertion within the control objective, as illustrated by the proposed language in paragraphs 8.A42x-y below. This new application material would necessitate a change to the cross-references in paragraph 8.25b.

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 those controls were suitably designed to achieve the control objectives by (Ref: par. 8.A26-8.A27 and 8.A39-8.A42)

a. …

b. evaluating the linkage of the controls identified in management’s description of the service organization’s system with those risks. (Ref: par. 8.A42x and 8.A42y)

8.A42x. When determining which of the controls at the service organization are necessary to achieve the control objectives, consideration is given to the achievement of each assertion noted within the control objectives listed in management’s description of the service organization’s system. (Ref: par 8.25b)

8.A42y. Control objectives commonly include several assertions (e.g., the authorization, accuracy, completeness, and timeliness of transaction processing). In evaluating the design of controls, the service auditor links the applicable controls to each of the assertions listed in the control objective, while also taking into consideration the classes of transactions. The service organization may have different controls in place to achieve each assertion listed in the control objective, depending on the class of transaction; and, therefore, multiple controls may be needed in order for the service auditor to conclude on the design of controls relating to each assertion within the control objective. (Ref: par 8.25b)

Paragraph 8.27

We believe that the term “significant” in paragraph 8.27 may be difficult to consistently quantify and apply using the proposed SSAE. We recommend modifying the wording to further clarify the intent of the requirement paragraph. In addition, we recommend that new application material be added to address the circumstances in which the service auditor is unable to test the superseded controls, as illustrated below. We believe that being unable to test a superseded control may result in a modification to the service auditor’s report. Accordingly, we propose the following modifications:

8.27. When performing a type 2 engagement, the service auditor should obtain an
understanding of changes in the service organization’s system that were implemented during the period covered by the service auditor’s report. If the service auditor believes the changes would be considered significant relevant to the achievement of the control objectives by user entities and their auditors, the service auditor should determine whether those changes are included in management’s description of the service organization’s system. If such changes are not included in the description, the service auditor should describe the changes in the service auditor’s report and determine the effect on the service auditor’s report. If superseded controls are relevant to the achievement of the control objectives stated in the description, the service auditor should, if possible, test the superseded controls before the change. If the service auditor cannot test superseded controls relevant to the achievement of the control objectives stated in the description, the service auditor should determine the effect on the service auditor’s report. (Ref: par. 8.A45, and 8.A47–8.A48, and 8.A48x)

8.A48x. If the service auditor is unable to test the superseded controls, the service auditor may consider whether this results in a modification to the service auditor’s report and may refer to the application guidance in Chapter 2. [Footnote 1] (Ref: par. 8.27)

Footnote 1: Paragraph 2.A98 of chapter 2, Examination Engagements

Paragraph 8.A46

We suggest the following edits be made to the application material to further clarify the language:

8.A46. Evidence about the satisfactory operation of controls in prior periods does not provide evidence of the operating effectiveness of controls during the current period. The service auditor expresses an opinion on the effectiveness of controls throughout each period; therefore, sufficient appropriate evidence about the operating effectiveness of controls throughout the current period is required for the service auditor to express that opinion for the current period. Knowledge of qualifications or deviations observed in prior engagements may, however, be contemplated in assessing risk and lead the service auditor to increase the extent of testing during the current period. (Ref: par. 8.26)

Paragraph 8.37b

We recommend including as a separate application guidance paragraph an example of an appropriate addressee.

Paragraphs 8.37c and 8.38c

We believe that any parts of management’s description of the service organization system that

---

3 See Proposed Statement on Standards for Attestation Engagements, Attestation Standards: Clarification and Recodification, issued by the Auditing Standards Board on July 24, 2013.
are not covered by the service auditor’s report should be reflected in a different section of the type 2 report from that which is covered by the service auditor’s engagement. This would facilitate further clarity in the service auditor’s report as to what is covered. This proposed edit would also necessitate clarifying the cross references in paragraph 8.A56 (see below). Our recommended edit to paragraph 8.37c[ii] is as follows (a similar edit would be made to paragraph 8.38c[ii]):

8.37. A service auditor’s type 2 report should include the following: …

c. Identification of the following: …

   i. …

   ii. Any parts of management’s description of the service organization’s system section of the type 2 report that are not covered by the service auditor’s report (Ref: par. 8.A56)

Paragraph 8.A56

We believe that the edit suggested below to paragraph 8.A56 (first bullet) provides further clarity as to the location of the other information in the type 1 or type 2 report. Further, we recommend that additional application material be included, as reflected in paragraph 8.A56x below, to draw the practitioner’s attention to the restrictions on the use of the service auditor’s report contained in the alert language. Edits are also proposed to the cross-references to take into account the changes proposed to paragraphs 8.37c and 8.38c above. The edits are as follows:

8.A56. The other information referred to in paragraphs 8.36 may include

- information provided by the service organization and included in a separate section of the type 1 or type 2 report, or (Ref: par. 8.37c[ii] and 8.38c[iii])

- information outside the type 1 or type 2 report included in a document that contains the service auditor’s report. This other information may be provided by the service organization or by another party. (Ref: par. 8.36, 8.37c[iii]–[iii], and 8.38c[iii]–[iii])

8.A56x. Notwithstanding the requirement in paragraph 8.36, the practitioner also considers the implications of the alert language, contained in paragraphs 8.37l and 8.38l respectively, that is included in the service auditor’s report.

Paragraphs 8.37l

We recommend including application guidance for paragraph 8.37l, to include a reference to possible findings of the internal audit function, as illustrated below. We recommend the following:

8.A62x. Where findings were identified by the internal audit function, the service auditor may consider the implications of those findings, including how the
internal audit function adjusted the work relating to controls performed by internal audit. (Ref: par. 8.37/v)

Paragraph 8.A63

In order to clarify the application material, we propose the following modification to paragraph 8.A63:

8.A63. There is no identification of the service auditor’s use of internal auditors to provide direct assistance within the service auditor’s report or in the description of tests of controls and results of the service auditor’s use of internal auditors to provide direct assistance. (Ref: par. 8.37/v)

Paragraph 8.A64

We recommend modifying the language in paragraph 8.A64 to more accurately depict the requirements of a type 1 versus a type 2 report:

8.A64. Chapter 2 requires that the use of a practitioner’s report be restricted to specified parties when the criteria used to evaluate or measure the subject matter are available only to specified parties or appropriate only for a limited number of parties who either participated in their establishment or can be presumed to have an adequate understanding of the criteria. The criteria used for engagements to report on controls at a service organization are relevant only for the purpose of providing information about the service organization’s system, including controls, to those who have an understanding of how the system is used for financial reporting by user entities and, accordingly, the service auditor’s report states that the report and (for a type 2 report) the description of tests of controls are intended only for use by management of the service organization, user entities of the service organization (“during some or all of the period covered by the report” for a type 2 report, and the “as of the ending specified date of the period covered by the report” for a type 1 report), and their user auditors. (The illustrative service auditor’s reports in exhibit A of this chapter illustrate language for a paragraph restricting the use of a service auditor’s report.) (Ref: par. 8.37/l and 8.38/l)

Paragraph 8.A65

We recommend clarifying the application material in paragraph 8.A65 to indicate that the alert, as referenced in paragraphs 8.37/l and 8.38/l, would result in the restriction of use of the service auditor’s report. We propose the following modification:

8.A65. Chapter 2 indicates that the need for an alert on the restriction on the use of a report may result from a number of circumstances, including the potential for the report to be misunderstood when taken out of the context in which it was intended to be used, and the extent to which the procedures performed are known or understood. (Ref: par. 8.37/l and 8.38/l)

Paragraph 8.A66
We recommend modifying the lead-in to the application material in paragraph 8.A66 to also clarify the service auditor’s responsibilities as it relates to the restriction on use of the service auditor’s report in comparison to report distribution.

**8.A66.** Although the alert language in the service auditor’s report provides for a restriction on use, the service auditor is not responsible for controlling a service organization’s distribution of a service auditor’s report. A service auditor may inform the service organization of the following: …

**Paragraphs 8.37o and 8.38o**

We recommend expanding upon the requirement in paragraphs 8.37o and 8.38o to better describe when the service auditor’s report should be dated. We propose the following edit to paragraph 8.37o (a similar edit should be made to paragraph 8.38o):

**8.37o.** The date of the service auditor’s report. (The report should be dated no earlier than the date on which the service auditor has obtained sufficient appropriate evidence on which to base the service auditor’s opinion, including that the responsible party has provided a written assertion).

**Paragraph 8.38c**

We propose modifying the language in paragraph 8.38c[i] as follows, to reflect that type 1 reports are as of a specified date and not for a period:

**8.38.** A service auditor’s type 1 report should include the following elements: (Ref: par. 8.A68) …

  **c.** Identification of

  i. management’s description of the service organization’s system, the function performed by the system, and the period specified date to which the description relates

  ii. …

**Paragraph 8.38d**

We believe that when the service auditor is issuing a report on management’s description of a service organization’s system and the suitability of the design of controls (namely, a type 1 report), it should be self-evident, given the nature of the engagement, that the service auditor is not required to evaluate the operating effectiveness of complementary user entity controls. Consequently, we believe it is not necessary to include such a statement in the service auditor’s report as required by paragraph 8.38d.

**8.38.** A service auditor’s type 1 report should include the following elements: (Ref: par. 8.A68) …
If management’s description of the service organization’s system refers to the need for complementary user entity controls, a statement that the service auditor has not evaluated the suitability of the design or operating effectiveness of complementary user entity controls, and that the control objectives stated in the description can be achieved only if complementary user entity controls are suitably designed and operating effectively, along with the controls at the service organization.

e. …

Paragraph 8.38

We believe that the terminology within paragraph 8.38k[iii] and 8.38k[iv] is vague in relation to the phrase “a reference to this condition.” We recommend including a separate application guidance paragraph that provides example wording of such a condition.

Paragraph 8.39

We believe that the language “in all material respects” is used inappropriately within the lead in paragraphs as it is not necessarily applicable to all the sub-paragraphs. We recommend the following modifications to paragraphs 8.39 and 8.40:

8.39. The service auditor’s opinion should be modified and the service auditor’s report should contain a clear description of all the reasons for the modification, if the service auditor concludes that:

a. management’s description of the service organization’s system is not fairly presented, in all material respects,

b. the controls are not suitably designed to provide reasonable assurance that the control objectives stated in management’s description of the service organization’s system would be achieved, in all material respects, if the controls operated effectively,

c. in the case of a type 2 report, the controls did not operate effectively throughout the specified period to achieve, in all material respects, the related control objectives stated in management’s description of the service organization’s system, or

d. the service auditor is unable to obtain sufficient appropriate evidence.

Paragraph 8.42

We believe that if the service auditor becomes aware of incidents of noncompliance with laws and regulations, fraud, or uncorrected errors attributable to management or other service organization personnel that are not clearly trivial and that may affect one or more user entities, the service auditor should also assess management’s ability to providing an assertion and the impact on management’s assertion. We recommend the following modification to paragraph
8.42:  

8.42. If the service auditor becomes aware of incidents of noncompliance with laws and regulations, fraud, or uncorrected errors attributable to management or other service organization personnel that are not clearly trivial and that may affect one or more user entities, the service auditor should determine the effect on management’s ability to provide their assertion as well as the impact on management’s assertion. The service auditor should also determine the effect of such incidents on management’s description of the service organization’s system, the achievement of the control objectives, and the service auditor’s report. Additionally, the service auditor should determine whether this information has been communicated appropriately to affected user entities. If the information has not been so communicated, and management of the service organization is unwilling to do so, the service auditor should take appropriate action. (Ref: par. 8.A70)

Paragraphs 8.A71 and 8.A72  

We have included within the attached Appendix our proposed edits to Exhibit A: Illustrative Service Auditor’s Reports and Exhibit B: Illustrative Assertions by Management of a Service Organization.

Paragraph 8.A73  

We believe that Exhibit C: Assessing the Suitability of the Criteria, is redundant because the information contained therein is already incorporated into the requirements of the proposed SSAE. Accordingly, we recommend deleting Exhibit C.

*   *   *

We would be pleased to discuss our letter with you at your convenience. If you have any further questions, please contact Jennifer Haskell at (203) 761-3394.

Sincerely,

[Signature]

Deloitte & Touche LLP
Appendix

Paragraph 8.A71 — Exhibit A: Illustrative Service Auditor’s Reports

Example 1: Type 2 Service Auditor’s Report

We recommend re-ordering the paragraphs under the “Opinion” heading as it pertains to paragraphs b and c in order to be consistent with order of presentation under the “Scope” heading when the service organization uses a subservice organization, and for which the carve-out method is used to present the subservice organization, and complementary subservice organization controls are required to meet the control objectives. The following edits are suggested:

... Scope ...

[ A statement such as the following is added to the report when the service organization uses a subservice organization, and for which the carve-out method is used to present the subservice organization, and complementary subservice organization controls are required to meet the control objectives.]

... Opinion ...

In our opinion, in all material respects, based on the criteria described in XYZ Service Organization’s assertion,

  a. the description fairly presents the [type or name of] system that was designed and implemented throughout the period [date] to [date].

  b. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period [date] to [date] if complementary user entity controls and subservice organization controls assumed in the design of XYZ Service Organization’s controls operated effectively throughout the period [date] to [date].

  b.c. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period [date] to [date] and user entities and subservice organizations applied the complementary controls assumed in the design of XYZ Service Organization’s controls throughout the period [date] to [date].

  e. the controls operated effectively to provide reasonable assurance that the control-
objectives stated in the description were achieved throughout the period [date] to [date]. If complementary user entity controls and subservice organization controls assumed in the design of XYZ Service Organization’s controls operated effectively throughout the period [date] to [date].

Example 2: Type 1 Service Auditor’s Report

We recommend clarifying the wording under the heading “Other Matter” as follows:

... 

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and accordingly do not express an opinion thereon on operating effectiveness.

...

Paragraph 8.A72 — Exhibit B: Illustrative Assertions by Management of a Service Organization

Example 1: Assertion by Management of a Service Organization for a Type 2 Report

We believe that management of the service organization should also be responsible for identifying, in the description of the user entity’s system, when there are applicable subservice organizations and complementary user entity controls. We have included proposed illustrative language and other minor edits below.

XYZ Service Organization’s Assertion

We have prepared the description of XYZ Service Organization’s [type or name of] system (description) for user entities of the system during some or all of the period [date] to [date], and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities [and subservice organizations] of the system themselves, when assessing the risks of material misstatements of user entities’ financial statements.

[A statement such as the following is added to the assertion when the service organization uses a subservice organization, and for which the carve-out method is used to present the subservice organization, and complementary subservice organization controls are required to meet the control objectives.]

XYZ Service Organization uses a subservice organization to [identify the function or
The description includes only the control objectives and related controls of XYZ Service Organization and excludes the control objectives and related controls of the subservice organization(s). The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

A statement such as the following is added to the report when complementary user entity controls are required to meet the control objectives.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of XYZ Service Organization’s controls are suitably designed and operating effectively, along with related controls at the service organization.

We confirm, to the best of our knowledge and belief, that

- the description fairly presents the [type or name of] system made available to user entities of the system during some or all of the period [date] to [date] for processing their transactions [or identification of the function performed by the system]

- the description fairly presents the [type or name of] system made available to user entities of the system during some or all of the period [date] to [date] for processing their transactions [or identification of the function performed by the system]. The criteria we used in making this assertion were that the description
  - presents how the system made available to user entities of the system was designed and implemented to process relevant user entity [and subservice organization] transactions, including, if applicable,
    - the classes of transactions processed.
    - the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities [and subservice organizations] of the system.
    - the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities [and subservice organizations].
(4) how the system captures and addresses significant events and conditions other than transactions.

(5) the process used to prepare reports or other information provided to user entities’ [and subservice organizations] of the system.

(6) specified control objectives and controls designed to achieve those objectives.

(7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities [and subservice organizations] of the system.

ii. does not omit or distort information relevant to the scope of the [type or name of] system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the [type or name of] system that each individual user entity of the system and its auditor may consider important in its own particular environment.

be. the description includes relevant details of changes to the service organization’s system during the period covered by the description.

ed. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period [date] to [date] to achieve those control objectives [if user entities and subservice organizations applied the complementary controls assumed in the design of XYZ Service Organization's controls throughout the period [date] to [date]].

The criteria we used in making this assertion were that

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization.

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.