2016

Applying special purpose frameworks in state and local governmental financial statements; Practice Aid Series

American Institute of Certified Public Accountants (AICPA)

Using a SOC 1® Report in Audits of Employee Benefit Plans

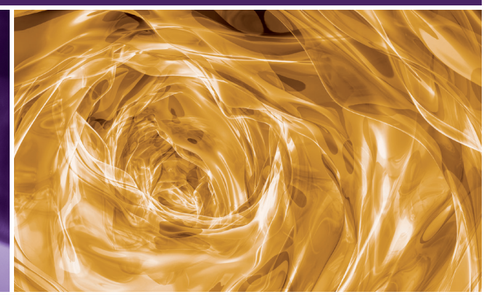
Using a SOC 1® Report in Audits of Employee Benefit Plans

PRACTICE AID SERIES

Using a SOC 1® Report in Audits of Employee Benefit Plans

9 781945 498183

APAS0C116P



AICPA American Institute of CPAs®

aicpa.org | www.AICPAStore.com

AICPA

SOC 1®

PRACTICE AID SERIES

Using a SOC 1® Report in Audits of Employee Benefit Plans

16368-349

AICPA®

SOC 1®

1 2 3 4 5 6 7 8 9 0 AAP 1 9 8 7 6

ISBN 978-1-94549-818-3

Notice to Readers

This practice aid, *Using a SOC 1® Report in Audits of Employee Benefit Plans*, has been developed to provide guidance to auditors when auditing the financial statements of an employee benefit plan that uses a service organization. This practice aid is intended for use in audits of the financial statements of employee benefit plans that are nonissuers.

This practice aid is an *other auditing publication* as defined in AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards* (AICPA, *Professional Standards*). Other auditing publications have no authoritative status; however, they may help the auditor understand and apply generally accepted auditing standards.

When applying the auditing guidance included in an other auditing publication, the auditor should exercise professional judgment and assess the relevance and appropriateness of such guidance to the circumstances of the audit.

This practice aid does not establish standards and is not a substitute for the original authoritative guidance. This practice aid has been reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA and is presumed to be appropriate. This document has not been approved, disapproved, or otherwise acted on by any senior committee of the AICPA.

Although this practice aid is not intended to provide guidance for audits of issuers, as defined by the Sarbanes-Oxley Act of 2002, and other entities, when prescribed by the rules of the SEC, it may be useful to auditors of employee benefit plans that file Form 11-K with the SEC if the plan uses a service organization.

Recognition

AICPA Staff

Diana Krupica, CPA
Lead Technical Manager
A&A Content Development

Judith Sherinsky, CPA
Senior Technical Manager
Audit and Attest Standards

Other Contributors

The A&A Content Development team would also like to thank Monique Elliott and Kriste Naples-DeAngelo, members of the AICPA Employee Benefit Plans Expert Panel, who reviewed and contributed to the development of this practice aid.

Standards Considered In This Edition

This edition of the practice aid has been modified by the AICPA staff to include certain changes necessary due to the issuance of authoritative standards since the practice aid was originally issued. This includes the issuance of

- Statement on Standards for Attestation Engagements No. 18, *Attestation Standards: Clarification and Recodification* (AICPA, *Professional Standards*) (Effective for service auditor's reports for periods ending on or after May 1, 2017.)

In addition, the following references were used in preparing this practice aid:

- AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* (AICPA, *Professional Standards*)
- AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*)
- AICPA Audit and Accounting Guide *Employee Benefit Plans* (January 1, 2016)
- AICPA Audit Risk Alert *Employee Benefit Plans Industry Developments—2016*

Feedback

We hope that you find this practice aid to be informative and useful. Please let us know what you think. What features do you like? What do you think can be improved or added? We encourage you to provide us with your comments and questions. Please send your feedback to the A&A Content Development team of the AICPA at A&Apublications@aicpa.org.

TABLE OF CONTENTS

Chapter 1
Introduction

Purpose of This Practice Aid

This practice aid provides guidance on

a. how the auditor of an employee benefit plan's financial statements (plan auditor) uses management's description of a service organization's system and a service auditor's report on that description and on the suitability of the design of controls (a type 1 report) or management's description of a service organization's system and the service auditor's report on that description and on the suitability of the design and operating effectiveness of controls (a type 2 report) prepared under AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*), in the audit of an employee benefit plan's (plan's) financial statements, and

b. the audit procedures, under AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), that a plan auditor should apply to the information included in a type 1 or type 2 report.

The glossary of this practice aid contains definitions of technical terms used in AT-C section 320 that are also used in this practice aid. Because the following terms are frequently used in this practice aid, their definitions are presented here to assist readers in understanding the practice aid.

Service auditor. A practitioner[1] who reports on controls at a service organization.

Service organization. An organization or segment of an organization that provides services to user entities that are likely to be relevant to those user entities' internal control over financial reporting. (Examples of service organizations that are commonly used by employee benefit plans include bank trustees, custodians, insurance entities, recordkeepers, and contract administrators.)

User auditor. An auditor who audits and reports on the financial statements of a user entity. (In this practice aid, the user auditor is the plan auditor.)

User entity. An entity that uses a service organization for which controls at the service organization are likely to be relevant to that entity's internal control over financial reporting. (In this practice aid, the user entity is an employee benefit plan.)

SOC Reports

In this practice aid, a report issued under AT-C section 320 is referred to as a *SOC 1® report*. Other SOC reports are described in appendix B, "An Overview of SOC 1, 2, and 3 Reports," of this practice aid.

Background

AU-C section 402 addresses the plan auditor's responsibility for obtaining sufficient appropriate audit evidence in an audit of the financial statements of a user entity that uses one or more service organizations and contains requirements and application guidance on how a plan auditor

[1] In the attestation standards, a CPA performing an attestation engagement ordinarily is referred to as a *practitioner*. AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*), uses the term *service auditor*, rather than *practitioner*, to refer to a CPA reporting on controls at a service organization, as does this practice aid.

- obtains 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.
- designs and performs audit procedures responsive to those risks.

AU-C section 402 identifies various ways in which the auditor of the financial statements of an entity that uses a service organization may obtain the required understanding of the entity's internal control. This practice aid is premised on the assumption that the user auditor (in this case, the plan auditor) has decided to obtain and use a SOC 1 report to obtain that understanding. The practice aid also addresses how a plan auditor evaluates a SOC 1 report.

This practice aid is not intended to be a substitute for reading the entire text of AU-C section 402. It is intended to be a supplement to the requirements and application guidance contained therein. For additional information about obtaining an understanding of a plan's internal control over financial reporting, see chapter 4, "Internal Control," of the AICPA Audit and Accounting Guide *Employee Benefit Plans*.

In April 2016, the AICPA Auditing Standards Board issued Statement on Standards for Attestation Engagements No. 18, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*), which clarified and restructured the attestation standards. AT-C section 320 of the clarified attestation standards establishes the requirements and application guidance for a service auditor examining controls at organizations that provide services to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting. The controls addressed in AT-C section 320 are those 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 service organization's control objectives relevant to the services provided to the plan. In addition, they include aspects of the information and communications component of user entities' internal control maintained by the service organization, control activities related to the information and communication component, and may also include aspects of one or more of the other components of internal control at a service organization (the service organization's control environment, risk assessment, monitoring activities, and control activities) when they relate to the services provided.

The service organizations addressed by AT-C section 320 may process transactions for the user entity or may provide a particular software application and technology environment that enables user entities to process transactions. These services result in data or other information that is incorporated in the user entities' financial statements. Because the practice of outsourcing tasks or functions to service organizations has increased, the demand for SOC 1 reports also has increased.

The demand for SOC reports on controls at service organizations that address subject matter other than user entities' internal control over financial reporting also has grown, for example, reports on controls at a service organization that affect the privacy of user entities' information or affect the availability of the service organization's system to user entities. AT-C section 320 is not applicable to such engagements. However, AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*), and interpretive publications such as the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* enable a practitioner to report on such controls. To make practitioners aware of the various standards available to them for examining and reporting on controls at a service organization and to help practitioners select the appropriate standard for a particular engagement, the AICPA introduced a series of SOC engagements and related reports. This series encompasses:

a. SOC 1 reports for engagements performed under AT-C section 320; these reports address controls at a service organization relevant to user entities' internal control over financial reporting (financial statements);

b. SOC 2® reports, which address controls at a service organization relevant to the security, availability, or processing integrity of a service organization's system, the confidentiality of the information that the service organization's system processes or maintains for user entities, or the privacy of personal information that the service organization collects, uses, retains, discloses, and disposes of for user entities; and

c. SOC 3® reports, which address the same subject matter as SOC 2 reports, but do not contain a description of the service auditor's tests of controls and the results of those tests.

This practice aid focuses on SOC 1 reports. For more information on SOC 2 and SOC 3 reports, see appendix B.

Types of SOC 1 Reports

SOC 1 reports are intended to meet the needs of plan auditors and management of user entities in evaluating the effect of a service organization's controls on a user entity's internal control over financial reporting. Paragraph .08 of AT-C section 320 defines the two types of SOC 1 reports:

Management's description of a service organization's system and a service auditor's report on that description and on the suitability of the design of controls (referred to as a *type 1 report*).

A service auditor's report that comprises the following:

a. Management's description of the service organization's system,[2]

b. A written assertion by management of the service organization about whether, based on the criteria

i. 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 and

ii. 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 a specified date

c. A service auditor's report that expresses an opinion on the matters in *b*(i)–(ii)

Use of a type 1 report is restricted to management of the service organization, user entities of the service organization's system as of the specified date, and the auditors who audit and report on such user entities' financial statements or internal control over financial reporting.

Management's description of a service organization's system and a service auditor's report on that description and on the suitability of the design and operating effectiveness of controls (referred to as a *type 2 report*).

A service auditor's report that comprises the following:

a. Management's description of the service organization's system

b. A written assertion by management of the service organization about whether, based on the 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,

ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives, and

iii. the controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives.

[2] Note that hereinafter, the term *management's description of the service organization's system* refers to management of the service organization as the term is used in AT-C section 320.

c. A auditor's report that

i. expresses an opinion on the matters in *b*(i)–(iii), and

ii. includes a description of the service auditor's tests of controls and the results thereof

Use of a type 2 report, including the description of tests of controls and results thereof, is restricted to management of the service organization, user entities of the service organization's system during some or all of the period covered by the report, and the auditors who audit and report on such user entities' financial statements or internal control over financial reporting.

Both type 1 and type 2 SOC 1 reports are intended to provide the plan auditor with information that will enable them to obtain an understanding of the entity, including its internal control, so that the plan auditor can identify and assess the risks of material misstatement of financial statements assertions affected by the services provided by the service organization. In addition to the information provided in a type 1 report, a type 2 report provides plan auditors with a description of the service auditor's tests of controls and results of those tests, which is intended to enable the plan auditor to respond to assessed risk.

A SOC 1 report is not a general use report and, as such, is not intended for use by anyone other than the specified parties named in the restricted use paragraph of the SOC 1 report.

Applicability to Employee Benefit Plans

It is common for an employee benefit plan administrator to use a service organization (also called a *third-party administrator*) to process certain transactions or perform certain functions on behalf of the employee benefit plan. Such service organizations may include recordkeepers, trustees, custodians, or insurance entities.

AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* (AICPA, *Professional Standards*), addresses the auditor's responsibility to identify and assess the risks of material misstatement of the financial statements by obtaining an understanding of the entity and its environment, including the entity's internal control. When an employee benefit plan uses a service organization to process transactions or perform other functions, questions may arise about how the plan auditor should obtain the necessary understanding related to controls at the service organization. One way an auditor may obtain this understanding is to obtain a SOC 1 report from the user entity, which is described in this practice aid in chapter 3, "Using the Services of a Service Organization," in the section titled "Using a SOC 1 Report to Obtain an Understanding of the Services."

One of the objectives of this practice aid is to help auditors of employee benefit plans determine how a SOC 1 report should be considered in their audits and the auditing procedures that should be applied to the information in a SOC 1 report. Some of the topics that are addressed in this practice aid related to using a SOC 1 report include

a. determining when a SOC 1 report, if available, should be obtained and whether a type 1 or type 2 report is applicable in the circumstances.

b. how to use a SOC 1 report when planning an audit of an employee benefit plan's financial statements in accordance with the Employee Retirement Income Security Act of 1974 (ERISA) limited-scope audit permitted by Title 29 U.S. *Code of Federal Regulations* Part 2520.103-8, Rules and Regulations for Reporting and Disclosure under Employee Retirement Income Security Act of 1974.

c. audit implications when a service organization uses subservice organizations.

d. how to read and understand a SOC 1 report and how the report affects the audit of an employee benefit plan's financial statements, including

i. illustrative procedures a plan auditor may perform to gain an understanding of the scope of the service auditor's work and whether that scope is adequate for the purposes of the audit of a particular employee benefit plan's financial statements;

ii. the procedures a plan auditor may perform to evaluate the results of tests of controls; and

iii. how to develop an appropriate audit response to identified testing exceptions and determine whether such exceptions represent deficiencies in the employee benefit plan's internal control.

This practice aid also includes several forms and checklists that may be used to implement the suggestions provided.

Chapter 2
A Brief Overview

Paragraph .03 of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* (AICPA, *Professional Standards*), states that the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and relevant assertion levels through understanding the entity and its environment, including the entity's internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement.

Before considering how an employee benefit plan's use of a service organization affects an audit of the employee benefit plan's financial statements, this practice aid presents a summary of the procedures the auditor should perform to assess the risks of material misstatement of those financial statements.

Risk Assessment Procedures and Related Activities

In accordance with paragraphs .05–.06 of AU-C section 315, the auditor should perform risk assessment procedures to provide a basis for the identification and assessment of risks of material misstatement at the financial statement and relevant assertion levels. Risk assessment procedures by themselves, however, do not provide sufficient appropriate audit evidence on which to base the audit opinion. Risk assessment procedures should include the following:

- Inquiries of management and others within the employee benefit plan who, in the auditor's professional judgment, may have information that is likely to assist in identifying risks of material misstatement due to fraud or error
- Analytical procedures
- Observation and inspection

Paragraphs .A1–.A23 of AU-C section 315 provide application guidance to assist the auditor in performing these risk assessment procedures. In addition to these three risk assessment procedures, paragraph .07 of AU-C section 315 states that the auditor should consider whether information obtained from the auditor's client acceptance or continuance process is relevant to identifying risks of material misstatement, and paragraph .08 states that if the engagement partner has performed other engagements for the plan, the engagement partner should consider whether information obtained is relevant to identifying risks of material misstatement.

The Auditor's Understanding of the Entity and Its Environment, Including Its Internal Control

Understanding the Entity and Its Environment

With respect to obtaining an understanding of the entity and its environment, paragraph .12 of AU-C section 315 states that the auditor should obtain an understanding of the following:

- Relevant industry, regulatory, and other external factors, including the applicable financial reporting framework.[1]

[1] For employee benefit plans, the applicable financial reporting framework is typically accounting principles generally accepted in the United States of America as promulgated by the Financial Accounting Standards Board or certain special purpose frameworks (for example, modified cash basis), as defined in AU-C section 800, *Special Considerations—Audits of Financial Statements Prepared in Accordance With Special Purpose Frameworks* (AICPA, *Professional Standards*), and as permitted by the Employee Retirement Income Security Act of 1974 (ERISA) and Department of Labor (DOL) regulations.

- The nature of the entity, including
  - — its operations;
  - — its ownership and governance structures;
  - — the types of investments that the entity is making and plans to make, including investments in entities formed to accomplish specific objectives; and
  - — the way that the entity is structured and how it is financed,

  to enable the auditor to understand the classes of transactions, account balances, and disclosures to be expected in the financial statements.
- The entity's selection and application of accounting policies, including the reasons for changes thereto. The auditor should evaluate whether the entity's accounting policies are appropriate for its business and consistent with the applicable financial reporting framework and accounting policies used in the relevant industry.
- The entity's objectives and strategies and the related business risks that may result in risks of material misstatement.
- The measurement and review of the entity's financial performance.

Understanding the Entity's Internal Control

An entity's *internal control* is defined in paragraph .04 of AU-C section 315 as "a process effected by those charged with governance, management, and other personnel that is designed to provide reasonable assurance about the achievement of the entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations." Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives.

The following are the five interrelated components of internal control:

1. Control environment
2. The entity's risk assessment process
3. The information system, including the related business processes relevant to financial reporting and communication
4. Control activities[2] relevant to the audit
5. Monitoring of controls

According to paragraph .13 of AU-C section 315, the auditor should obtain an understanding of internal control relevant to the audit. Although most controls relevant to the audit are likely to relate to financial reporting, not all controls that relate to financial reporting are relevant to the audit. The auditor uses professional judgment in determining whether a control, individually or in combination with others, is relevant to the audit. When obtaining an understanding of controls that are relevant to the audit, paragraph .14 of AU-C section 315 requires the auditor to evaluate the design of those controls and determine whether they have been implemented by performing procedures in addition to inquiry of the entity's personnel.

Evaluating the design of a control involves considering whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements. Assessing the implementation of a control that is not effectively designed is of little use, and so the design of a control is considered first.

Paragraph .10 of AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), requires a user auditor to evaluate the design and implementation of

[2] Control activities are also commonly referred to as *controls*.

controls at the user entity that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization. If a plan auditor is unable to obtain a sufficient understanding from the plan of the nature and significance of the services provided by the service organization and their effect on the plan's internal control relevant to the audit, the plan auditor should obtain that understanding from one or more of the procedures identified in paragraph .12 of AU-C section 402. One of those procedures is to obtain and read a SOC 1 report.

Control Activities and the Information System, Including the Accounting System

Paragraph .19 of AU-C section 315 states that the auditor should obtain an understanding of the information system, including the related business processes relevant to financial reporting, including the following areas:

- The classes of transactions in the entity's operations that are significant to the financial statements.
- The procedures within both IT and manual systems by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, transferred to the general ledger, and reported in the financial statements.
- The related accounting records, supporting information, and specific accounts in the financial statements that are used to initiate, authorize, record, process, and report transactions. This includes the correction of incorrect information and how information is transferred to the general ledger. The records may be in either manual or electronic form.
- How the information system captures events and conditions, other than transactions, that are significant to the financial statements.
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.
- Controls surrounding journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments.

When an employee benefit plan uses a service organization to process certain transactions or perform other functions, the service performed by the service organization will most directly affect the following two components of the plan's internal control:

- *Control activities relevant to the audit.* Paragraphs .21–.22 of AU-C section 315 state that the auditor should obtain an understanding of control activities relevant to the audit, which are those control activities the auditor judges necessary to understand in order to assess the risks of material misstatement at the assertion level and design further audit procedures responsive to assessed risks. An audit does not require an understanding of all the control activities related to each significant class of transactions, account balance, and disclosure in the financial statements or to every assertion relevant to them. However, the auditor should obtain an understanding of the process of reconciling detailed records to the general ledger for material account balances. In understanding the entity's control activities, the auditor should obtain an understanding of how the entity has responded to risks arising from IT. As stated in paragraph .A99 of AU-C section 315, control activities are the policies and procedures that help ensure that management directives are carried out. Control activities, whether within IT or manual systems, have various objectives and are applied at various organizational and functional levels. Examples of specific control activities include those relating to authorization, performance reviews, information processing, physical controls, and segregation of duties.
- *Information system, including the related business processes relevant to financial reporting and communication*. Paragraph .A92 of AU-C section 315 states that the information system relevant to financial reporting objectives, which includes the accounting system, consists of the procedures and records designed and established to
    - initiate, authorize, record, process, and report entity transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities, and equity;

- resolve incorrect processing of transactions (for example, automated suspense files and procedures followed to clear suspense items out on a timely basis);
- process and account for system overrides or bypasses to controls;
- transfer information from transaction processing systems to the general ledger;
- capture information relevant to financial reporting for events and conditions other than transactions, such as the depreciation and amortization of assets and changes in the recoverability of accounts receivables; and
- ensure information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized, and appropriately reported in the financial statements.

Identifying and Assessing the Risks of Material Misstatement

Paragraph .26 of AU-C section 315 states that to provide a basis for designing and performing further audit procedures, the auditor should identify and assess the risks of material misstatement at

a. the financial statement level and

b. the relevant assertion level for classes of transactions, account balances, and disclosures.

Paragraphs .27–.32 of AU-C section 315 indicate that the risk assessment process entails

- identifying risks throughout the process of obtaining an understanding of the entity and its environment, including relevant controls that relate to the risks, by considering the classes of transactions, account balances, and disclosures in the financial statements;
- assessing the identified risks and evaluating whether they relate more pervasively to the financial statements as a whole and potentially affect many assertions;
- relating the identified risks to what can go wrong at the relevant assertion level, taking account of relevant controls that the auditor intends to test;
- considering the likelihood of misstatement, including the possibility of multiple misstatements, and whether the potential misstatement is of a magnitude that could result in a material misstatement;
- determining whether any of the assessed risks are significant risks that require special audit consideration or
- risks for which substantive procedures alone do not provide sufficient appropriate audit evidence; and
- revising the auditor's assessment of risk if the auditor obtains audit evidence from performing further audit procedures or if new information is obtained, either of which is inconsistent with the audit evidence on which the auditor originally based the assessment, and modifying the further planned audit procedures.

Risk Assessment and a Plan's Use of IT

As indicated in paragraph .A60 of AU-C section 315, an entity's system of internal control contains manual elements and may contain automated elements. The characteristics of manual or automated elements are relevant to the auditor's risk assessment and further audit procedures based thereon. In addition, when obtaining an understanding of internal control, it is important for the auditor to consider how a plan's use of IT and manual procedures may affect controls relevant to the audit. As stated in paragraph .A61 of AU-C section 315, an entity's use of IT may affect any of the five components of internal control relevant to the achievement of the entity's financial reporting, operations, or compliance objectives and its operating units or business functions.

Whether the use of a service organization increases a plan's risk of material misstatement depends on the nature of the services provided by the service organization and the controls over these services; in some cases, the use of a service organization may decrease a plan's risk of material misstatement, particularly if the plan itself does not possess the expertise necessary to undertake particular activities, such as initiating, processing, and recording transactions, or does not have adequate resources (for example, an IT system).

Chapter 3
Using the Services of a Service Organization

Frequently, employee benefit plans use service organizations[1] to process certain transactions or perform other functions on behalf of the plan. In these circumstances, the employee benefit plan's internal control may consist of the controls at the plan as well as certain controls at the service organization. Paragraph .09 of AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), states that when obtaining an understanding of the user entity in accordance with AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* (AICPA, *Professional Standards*), the user auditor should obtain an understanding of how the user entity uses the services of a service organization in the user entity's operations.

Accordingly, paragraph .11 of AU-C section 402 indicates that the auditor of an employee benefit plan that uses the services of a service organization (plan auditor) should determine whether he or she has obtained a sufficient understanding of the nature and significance of the service provided by the service organization and their effect on the plan's internal control relevant to the audit to provide a basis for the identification and assessment of risks of material misstatement. As stated in paragraph .A49 of AU-C section 315, an understanding of internal control assists the auditor in (1) identifying types of potential misstatements and factors that affect the risks of material misstatement, and (2) designing the nature, timing, and extent of further audit procedures.

The nature and extent of the work to be performed by the auditor of an employee benefit plan's financial statements regarding the services provided by a service organization depend on the nature of the services, their significance to the plan, and the relevance of those services to the audit (discussed in more detail later).

An employee benefit plan may use a service organization to perform a wide variety of services. These services may include acting as a(n)

a. recordkeeper for participant accounts, which includes processing participant-level activity and maintaining participant accounts.

b. trustee or custodian, which includes maintaining custody of the plan's investment assets, reporting investment income, pricing exchange traded investments, accounting for investment shares, executing trades, and preparing checks or electronic funds transfers.

c. payroll provider, which includes processing payroll, withholding employee contributions, and maintaining related records.

d. claims processor, which includes processing claims for health and welfare benefit plans.

e. insurance entity, which includes maintaining and processing participant-level activity and participant accounts as well as plan-level investment activity.

f. benefit payment processor, which includes processing benefit payments on behalf of a plan.

g. human resource administrator, which includes performing portions of the human resource function for the plan.

h. investment manager or adviser, which includes providing investment advice and research services and performing certain administrative services under a contract.

i. ERISA counsel, which includes serving as legal counsel that has a specialization in the IRC, ERISA, and legal matters related to plan operations.

[1] The AICPA Audit and Accounting Guide *Employee Benefit Plans* sometimes uses terms such as *third-party administrators*, *third-party insurers*, and *third-party providers* to refer to service organizations.

j. plan appraiser, which includes valuing plan assets by an expert, based on standardized appraisal methodologies.

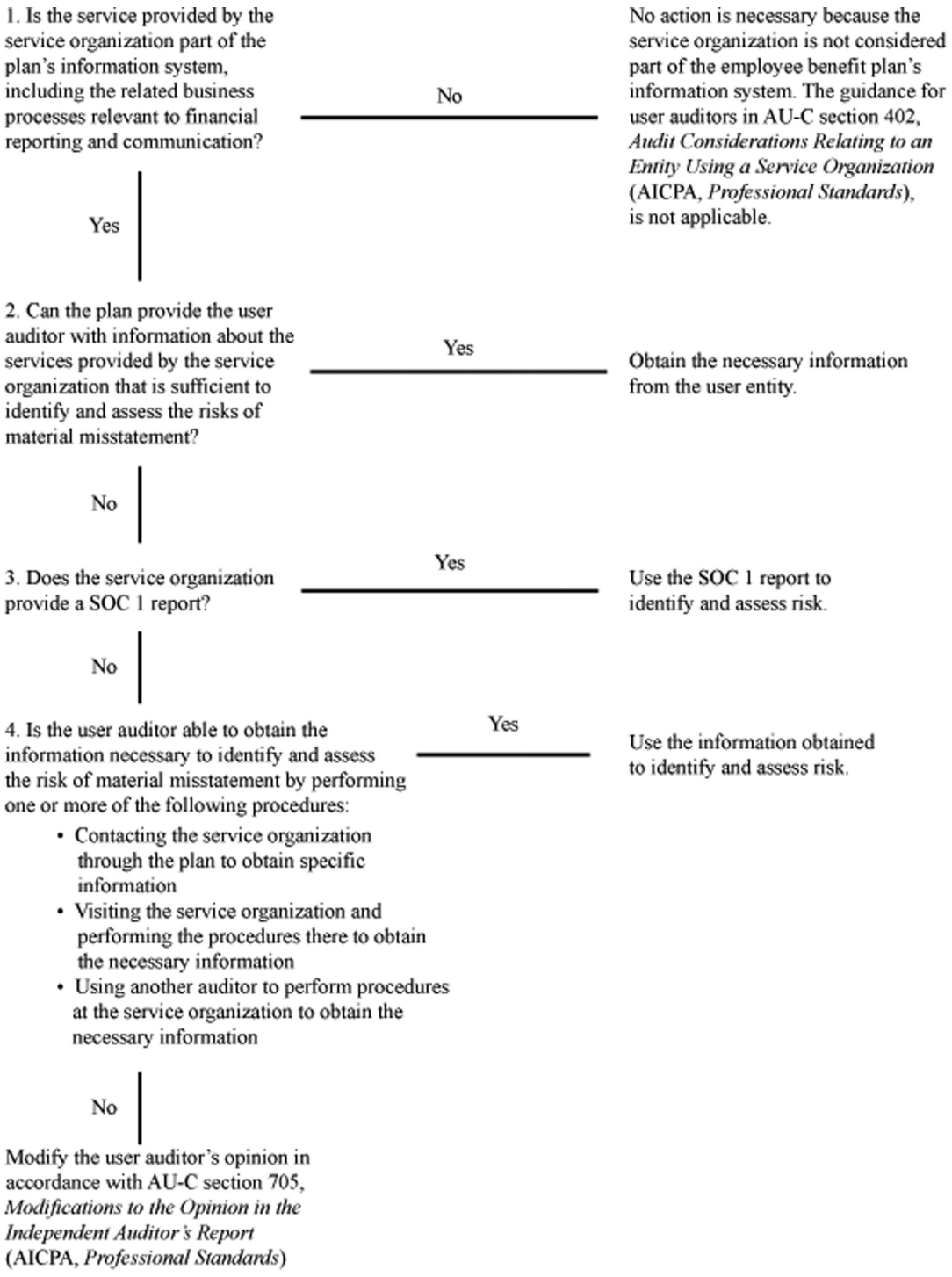
k. third-party pricing vendor, which includes providing pricing information for investments that are valued at fair value in situations in which there are no observable inputs.

l. outside administrator, which includes performing administrative functions such as enrollment, payment of benefits, collection of contributions for specific groups, annual tax compliance testing, and data storage for personnel records.

Exhibit 3-1, "Considering a Service Organization in an Employee Benefit Plan Audit," provides an overview of the key questions that are important for the auditor to consider when auditing the financial statements of an employee benefit plan that uses a service organization.

Exhibit 3-1

Considering a Service Organization in an Employee Benefit Plan Audit



See chapter 1, "Introduction," for a brief overview of SOC 1 reports. This chapter, as well as chapters 4–5, provides a more detailed discussion of SOC 1 reports. The following sections discuss the flowchart in exhibit 3-1.

Determining Whether the Service Organization Is Part of the Employee Benefit Plan's Information System

An employee benefit plan's use of a service organization does not, in and of itself, require a plan auditor to obtain a SOC 1 report to identify and assess risk. The first step to determine whether a SOC 1 report would be useful is to determine whether the services provided by the service organization are part of the plan's information system, including the related business processes relevant to financial reporting and communication. As previously stated, when a plan uses a service organization to process certain transactions or perform other functions on behalf of the plan, generally, the services provided by the service organization primarily affect the plan's control activities and information system, including the related business processes relevant to financial reporting and communication. When a service organization's services are part of the plan's information system, the auditor's understanding of the plan's internal control may need to include controls placed in operation by the service organization in addition to controls at the plan.

Paragraph .03 of AU-C section 402 states that a service organization's services are part of a user entity's information system, including related business processes, relevant to financial reporting if these services affect any of the following:

- The classes of transactions in the user entity's operations that are significant to the user entity's financial statements.
- The procedures within both IT and manual systems by which the user entity's transactions are initiated, authorized, recorded, processed, corrected as necessary, transferred to the general ledger, and reported in the financial statements.
- The related accounting records, supporting information, and specific accounts in the user entity's financial statements that are used to initiate, authorize, record, process, and report the user entity's transactions. This includes the correction of incorrect information and how information is transferred to the general ledger; the records may be in either manual or electronic form.
- How the user entity's information system captures events and conditions, other than transactions, that are significant to the financial statements.
- The financial reporting process used to prepare the user entity's financial statements, including significant accounting estimates and disclosures.
- Controls surrounding journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments.

Practice Pointer. Note that an employee benefit plan may not have a formal general ledger. However, the plan's statements, payroll ledgers, or other reports, and information that reflects the plan's day-to-day operations and are used to prepare the plan's financial statements, are applicable in the context of the guidance discussed in this practice aid.

The following are some examples of services that service organizations may provide to an employee benefit plan that would make the service organization's services part of the plan's information system:

- Processing of participant-level transactions, including the following:
  - — Contributions and distributions (benefit payments, new loans, and administrative expenses)
  - — Valuation of investments
  - — Execution of investment transactions
- Processing of new notes receivable from participants
- Processing of repayments of notes receivable from participants

- Recording and processing investment elections by participants or plan sponsors and changes to investment elections
- Claims processing
- Maintaining participant data records (for example, participant data)
- Purchasing or selling investment securities by an investment adviser or investment manager who has been authorized to initiate transactions on behalf of the plan without having to obtain authorization from the plan prior to each transaction
- Providing services that are ancillary to holding an entity's securities, such as the following:
    - Collecting dividend and interest income and distributing that income to the plan
    - Receiving notification of corporate actions
    - Receiving notification of security purchase and sale transactions
    - Receiving payments from purchasers and disbursing proceeds to sellers for investment security purchase and sale transactions
    - Maintaining records of securities transactions for the plan
- Providing the price of exchange traded investment securities through paper documents or electronic downloads that the plan uses to value its securities for transactions and financial statement reporting
- Facilitating security lending transactions in which the service organization provides collateral to the plan in exchange for the short-term use of certain securities
- Allocating investment income to participants
- Reconciling the participant's records to the plan's records
- Testing for compliance with ERISA, including discrimination testing
- Preparing the Form 5500 Annual Return/Report of Employee Benefit Plan

Thus, internal control of an employee benefit plan may consist of controls at both the plan and a service organization that performs functions that are likely to be relevant to the plan's internal control over financial reporting.

The plan auditor does not have to gain an understanding of controls at a service organization if the services provided by the service organization are limited to processing the plan's transactions that are specifically authorized by the plan, such as the processing of checking account transactions by a bank, or the processing of securities transactions by a broker (if the plan retains responsibility for authorizing the transactions and maintaining the related accountability). In these circumstances, the plan is not relying on controls at the bank or broker and is able to reconcile the information it has recorded in its books and records with statements from the bank or broker.

Understanding the Services Provided by a Service Organization

In accordance with the requirements of paragraph .09 of AU-C section 402, the plan auditor should obtain an understanding of how the plan uses the services of a service organization in its operations. This understanding includes the following:

- The nature of the services provided by the service organization and the significance of those services to the plan, including their effect on the plan's internal control
- The nature and materiality of the transactions processed or accounts or financial reporting processes affected by the service organization
- The degree of interaction between the activities of the service organization and those of the plan

- The nature of the relationship between the plan and the service organization, including the relevant contractual terms for the activities undertaken by the service organization

Obtaining Information About the Nature of the Services

As a rule, the plan auditor's first source of information about the nature and significance of the services provided by the service organization and their effect on the plan's internal control are (1) personnel at the employee benefit plan that would be in a position to have such knowledge, and (2) documentation at the plan that describes the services provided by the service organization. The following are examples of procedures the auditor may perform to obtain such information:

- Reading user manuals or other systems documentation (for example, system overviews and technical manuals) about the services provided
- Reading reports by service organizations, the plan's internal audit function, or regulatory authorities on controls at the service organization
- Inquiring of or observing personnel at the plan or at the service organization
- Reading the contract or service level agreement between the plan and the service organization
- Reading reports by the service auditor, if available

As indicated in paragraphs .A3–.A4 of AU-C section 402, a plan may use a service organization, such as one that processes transactions and maintains the related accountability for the plan, or records transactions and processes related data. Examples of service provided by a service organization that may be relevant to the audit include the following:

- Maintenance of the plan's accounting records
- Management of the plan's assets
- Initiating, authorizing, recording, or processing transactions as an agent of the plan

The Nature and Materiality of the Transactions

As indicated in paragraph .A6 of AU-C section 402, a service organization may establish policies and procedures (controls) that affect the plan's internal control. These controls are at least, in part, physically and operationally separate from the plan. The significance of the controls at the service organization to the plan's internal control depends on the nature of the services provided by the service organization, including the nature and materiality of the transactions it processes for the plan. In certain situations, the transactions processed and the accounts affected by the service organization may not appear to be material to the plan's financial statements, but the nature of the transactions processed may be significant, and the plan auditor may determine that an understanding of controls over the processing of those transactions is necessary in the circumstances.

Degree of Interaction

According to paragraph .A7 of AU-C section 402, the significance of the controls at the service organization to the plan's internal control also depends on the degree of interaction between the service organization's activities and those of the plan. The degree of interaction relates to the extent to which a plan is able to and elects to implement effective controls over the processing performed by the service organization, as follows:

- *High degree of interaction.* An example of a high degree of interaction between the activities of the plan and those at the service organization is when the plan authorizes transactions, and the service organization processes and accounts for those transactions. In these circumstances, it may be practicable for the plan to implement its own effective controls over those transactions.
- *Low degree of interaction.* When the service organization has been authorized to initiate transactions on behalf of the plan, or initially records, processes, and accounts for the user entity's transactions, a lower

degree of interaction exists between the plan and the service organization. In these circumstances, the plan may be unable to, or may elect not to, implement effective controls over these transactions at the plan and may rely on controls at the service organization.

As indicated in chapter 2, "A Brief Overview," the plan auditor's understanding of internal control assists the plan auditor in identifying types of potential misstatements and factors that affect the risks of material misstatement. The plan auditor's understanding of internal control also assists the plan auditor in designing the nature, timing, and extent of further audit procedures.

When gaining an understanding of internal control, it is important for the plan auditor to consider that not all of a service organization's controls are relevant to the audit. Paragraph .03 of AU-C section 402 states that services provided by a service organization are relevant to the audit of a user entity's financial statements when those services and the controls over them affect the user entity's information system, including related business processes relevant to financial reporting. Although most controls at the service organization are likely to relate to financial reporting, other controls also may be relevant to the audit, such as controls over the safeguarding of assets.

Nature of the Relationships

Paragraphs .A8–.A10 of AU-C section 402 indicate that the contract or service level agreement between the plan and the service organization may provide for matters such as the following:

- The information to be provided to the plan and the responsibilities for initiating transactions relating to the activities undertaken by the service organization
- Complying with the requirements of regulatory bodies concerning the form of records to be maintained or access to them
- Whether the service organization will provide a report on its controls and, if so, whether such a report will be a type 1 or type 2 report

A direct relationship exists between the service organization and the plan when the plan enters into an agreement with the service organization, and between the service organization and the service auditor when the service organization engages the service auditor. These relationships do not create a direct relationship between the plan auditor and the service auditor.

Communication between the plan auditor and the service auditor usually are conducted through the plan and the service organization. A plan auditor may request through the plan that a service auditor perform procedures for the benefit of the plan auditor.

Procedures When the Plan Auditor Cannot Obtain a Sufficient Understanding From the Employee Benefit Plan

If the plan auditor is unable to obtain the necessary information from the employee benefit plan, the plan auditor may obtain that understanding by performing one or more of the following procedures:

a. Obtaining and reading a type 1 or type 2 SOC 1 report, if available

b. Contacting the service organization, through the plan, to obtain specific information

c. Visiting the service organization and performing procedures that will provide the necessary information about the relevant controls at the service organization

d. Using another auditor to perform procedures at the service organization

Using a SOC 1 Report to Obtain an Understanding of the Services Provided to the Employee Benefit Plan

A service organization may engage a service auditor to perform a type 1 or type 2 SOC 1 engagement under AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*), with the objective of providing the resulting SOC 1 report to management of the service organization and user entities. Exhibit 3-2, "Summary of SOC 1 Reports," describes the features of type 1 and type 2 SOC 1 reports.

Exhibit 3-2

Summary of SOC 1 Reports

Title	*Contents*	*Relevance to Plan Auditors*
Management's description of a service organization's system and the service auditor's report on that description and on the suitability of the design of controls (Type 1 SOC 1 report)	*a.* Management's description of the service organization's system *b.* Management's written assertion about whether, based on the criteria, i. management's description of the service organization's system fairly presents the system that was designed and implemented as of a specified date ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed as of the specified date to achieve those control objectives *c.* A report by the service auditor that expresses an opinion on the matters in *b*(i)–(ii). *Note*: Management of the service organization is responsible for preparing the description of the service organization's system, including the control objectives and related controls that are likely to be relevant to the user entities' internal control over financial reporting.	Assists the plan auditor in obtaining a sufficient understanding of the nature and significance of the services provided by the service organization and their effect on the plan's internal control relevant to the audit. Enables the user auditor to identify and assess risks of material misstatement for financial statement assertions affected by the service organization's services
Management's description of a service organization's system and the service auditor's report on that description and on the suitability of the design and operating effectiveness of controls (Type 2 SOC 1 report)	*a.* Management's description of the service organization's system *b.* Management's written assertion about whether, based on the criteria, i. management's description of the service organization's system fairly presents the system that was designed and implemented as of a specified date ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives iii. the controls related to the control objectives stated in management's description of the service organization's system were operating effectively throughout the specified period to achieve those control objectives *c.* A report by the service auditor that i. expresses an opinion on the matters in *b*(i)–(iii) ii. includes a description of the tests of controls and the results thereof	Assists the plan auditor in obtaining a sufficient understanding of the nature and significance of the services provided by the service organization and their effect on the plan's internal control relevant to the audit Enables the plan auditor to identify and assess risks of material misstatement for the plan's financial statement assertions affected by the service organization's services Provides evidence about whether controls at the service organization were operating effectively to achieve the related control objectives stated in the description. Such evidence should enable the plan auditor to respond to assessed risk related to assertions in the plan's financial statements affected by the service organization's services

Evaluating a SOC 1 Report

If a plan auditor intends to use a type 1 or type 2 SOC 1 report as audit evidence to support the plan auditor's understanding about the design and implementation of controls at the service organization , the plan auditor should

a. evaluate whether the SOC 1 report addresses the services, functions, or applications that the employee benefit plan uses and that are relevant to the plan's internal control over financial reporting;

b. evaluate whether the type 1 report is as of a date, or in the case of a type 2 report, is for a period that is appropriate for the plan auditor's purposes (see chapter 5, "How to Use a SOC 1 Report," for more detail);

c. evaluate the sufficiency and appropriateness of the evidence provided by the report for the plan auditor's understanding of the employee benefit plan's internal control relevant to the audit; and

d. determine whether complementary user entity controls identified by the service organization are relevant in addressing the risks of material misstatement related to the relevant assertions in the employee benefit plan's financial statements and, if so, obtaining an understanding of whether the plan has designed and implemented such controls (see chapter 5 for more detail).

As stated in paragraph .13 of AU-C section 402, in determining the sufficiency and appropriateness of the audit evidence provided by a type 1 or type 2 report, the user auditor should be satisfied regarding the service auditor's professional competence and independence from the service organization, and the adequacy of the standards under which the type 1 or type 2 report was issued.

To obtain information about the service auditor's professional competence, paragraph .A21 of AU-C section 402 indicates that a user auditor may make inquiries of the service auditor's professional organization (for example, a state board of accountancy) or other practitioners and inquire about whether the service auditor is subject to regulatory oversight. With respect to the adequacy of the standards under which the type 1 or type 2 report was issued, paragraph .A21 of AU-C section 402 indicates that an example of a situation in which a user auditor may need such information is when the service auditor is practicing in a jurisdiction in which different standards are followed with respect to reports on controls at a service organization; in those circumstances, the user auditor may obtain information about the standards used by the service auditor from the standard-setting organization in that jurisdiction.

With respect to the service auditor's independence, paragraph .A22 of AU-C section 402 states that, unless evidence to the contrary comes to the user auditor's attention, a service auditor's report implies that the service auditor is independent of the service organization. Paragraph .A22 of AU-C section 402 also notes that a service auditor need not be independent of the user entities.

Practice Pointer. It has come to the AICPA's attention that, in some cases, SOC 1 engagements are being performed and reported on by consulting organizations that are not licensed CPA firms. AT-C section 320 is intended for use by licensed CPAs. For a plan auditor to use a SOC 1 report, it must be issued by a licensed CPA. Plan auditors may not use a report provided by an unlicensed individual or organization. It is important for plan auditors to be alert to the possibility that a SOC 1 report may not have been prepared by a licensed CPA and, if the organization is unfamiliar to the plan auditor, should consider contacting a representative of the organization to verify that the organization is properly licensed, peer reviewed, and able to provide its peer review report and letter of comments and response. If the organization is unlicensed, CPAs are advised to convey that finding to the state board of accountancy in the state in which the engagement was performed or to their own state board.

If the plan auditor is unable to obtain sufficient appropriate audit evidence regarding the services provided by the service organization relevant to the audit of the plan's financial statements, a scope limitation may exist. When a scope limitation exists because sufficient appropriate audit evidence is unavailable, the options are to issue a qualified opinion or a disclaimer of opinion, depending on the plan auditor's conclusion regarding

whether the possible effects on the plan's financial statements are material, pervasive, or both. The following AU-C sections (AICPA, *Professional Standards*) provide guidance for auditor's reports issued in connection with audited financial statements:

- AU-C section 700, *Forming an Opinion and Reporting on Financial Statements*
- AU-C section 705, *Modifications to the Opinion in the Independent Auditor's Report*
- AU-C section 706, *Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs in the Independent Auditor's Report*
- AU-C section 800, *Special Considerations—Audits of Financial Statements Prepared in Accordance With Special Purpose Frameworks*

Subservice Organizations

In some cases, a service organization may use the services of another service organization to perform some of the services provided to user entities that are relevant to those user entities' internal control over financial reporting. AU-C section 402 and AT-C section 320 use the *term subservice organization* to refer to these service organizations. A subservice organization may be a separate entity from the service organization or it may be related to the service organization. Common examples of services provided by a subservice organization include the following:

- Statement printing
- Investment pricing
- Custody of securities
- Hosting of IT general controls and applications

When a subservice organization is used to process a plan's transactions, the plan auditor may need to obtain information about controls at the subservice organization that are relevant to the audit of the plan's financial statements. In situations in which one or more subservice organizations are used, the interaction between the activities of the plan and those of the service organization is expanded to include the interaction between the plan, the service organization, and the subservice organizations. The degree of this interaction as well as the nature and materiality of the transactions processed by the service organization and the subservice organizations are the most important factors for the plan auditor to consider in determining the significance of the service organization's and subservice organization's controls to the plan's controls. It is important for the plan auditor to evaluate the significance of the subservice organization to the audit of the plan's financial statements.

If a service organization uses a subservice organization and the SOC 1 report excludes the subservice organization, this is known as the *carve-out method* of reporting. When the plan auditor plans to use a type 1 or type 2 SOC 1 report that carves out the subservice organization, and the services provided by the subservice organization are relevant to the audit of the plan's financial statements, paragraph .A41 of AU-C section 402 states that the user auditor is required to apply the requirements of AU-C section 402 with respect to the subservice organization. The nature and extent of the work to be performed by the plan auditor regarding the service provided by a subservice organization depend on the nature and significance of those services to the plan and the relevance of those services to the audit. Because a plan typically does not have any contractual relationship with the subservice organization, plan management should obtain available reports and information about the subservice organization from the service organization.

If the service organization provides a SOC 1 report, the description of the service organization's system will identify the services performed by the subservice organization and whether the inclusive method or the carve-out method was used. If a service organization does not provide a SOC 1 report, it is often challenging for a plan auditor to determine whether a service organization uses a subservice organization and whether a carve-out exists. Possible sources of this information include

a. discussions with plan management,

b. inquiry of the service organization,

c. reading the contract or service level agreement between the plan and the service organization, and

d. reading plan manuals and other documentation about the service organization's services.

Practice Pointer. For an ERISA limited-scope audit, as permitted by Title 29 U.S. *Code of Federal Regulations* Part 2520.103-8, Rules and Regulations for Reporting and Disclosure under ERISA, the auditor has no responsibility to obtain an understanding of the controls maintained by the certifying institution over assets or liabilities held and investment transactions executed by the institution (in other words, the certifying institution is only certifying the investment and investment activity). Therefore, in an ERISA limited-scope audit, to the extent that the service organization is only providing investment transaction services, a SOC 1 report is not necessary. However, if the service organization also provides services such as processing participant-level transactions, a report may be relevant if it covers these services.

Chapter 4
Responding to the Assessed Risks of Material Misstatement When the Plan Uses a Service Organization

After the plan auditor has assessed the risks of material misstatement for financial statements assertions affected by the service organization's services, paragraph .06 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained* (AICPA, *Professional Standards*), requires the plan auditor to design and perform further audit procedures whose nature, timing, and extent are based on, and are responsive to, the assessed risks of material misstatement at the relevant assertion level. In applying that requirement, paragraph .15 of AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), directs the auditor to

a. determine whether sufficient appropriate audit evidence concerning the relevant financial statement assertions is available from records held at the user entity and, if not

b. perform further audit procedures to obtain sufficient appropriate audit evidence or use another auditor to perform those procedures at the service organization on the user auditor's behalf.

Performing Further Procedures in Response to Assessed Risk

Procedures When a SOC 1 Report Is Not Available

Obtaining a SOC 1 report is not the only way for a plan auditor to respond to assessed risks. The following paragraphs provide information about other procedures the plan auditor may perform to obtain sufficient appropriate evidence that is responsive to assessed risks.

When a SOC 1 report is not available and the service organization maintains material elements of the plan's accounting records, direct access to those records may be necessary for the plan auditor to obtain sufficient appropriate audit evidence relating to the operation of controls over those records or to substantiate transactions and balances recorded in them. Such access may involve physical inspection of records at the service organization's premises or electronic interrogation of records. When direct access is achieved electronically, the plan auditor may also obtain evidence concerning the adequacy of the service organization's controls over the completeness and integrity of the plan's data for which the service organization is responsible.

In accordance with paragraph .A27 of AU-C section 402, when the service organization holds assets or processes transactions for the plan, the plan auditor may consider performing the following procedures:

- *Inspecting records and documents held by the plan*. The reliability of this source of evidence is determined by the nature and extent of the accounting records and supporting documentation retained by the plan. In some cases, the plan may not maintain independent detailed records or documentation of specific transactions undertaken on its behalf.
- *Inspecting records and documents held by the service organization*. The plan auditor's access to the records of the service organization may be established as part of the contractual arrangements between the plan and the service organization. The plan auditor may also use another auditor, on its behalf, to gain access to the plan's records maintained by the service organization or ask the service organization, through the plan, for access to the plan's records maintained by the service organization.
- *Obtaining confirmations of balances and transactions from the service organization*. When the plan maintains independent records of balances and transactions, confirmation from the service organization corroborating those records usually constitutes reliable audit evidence concerning the existence of the transactions and assets concerned. For example, when multiple service organizations are used, such

as an investment manager and a custodian, and these service organizations maintain independent records, the plan auditor may confirm balances with these organizations in order to compare this information with the plan's independent records. If the plan does not maintain independent records, information obtained in confirmations from the service organization is merely a statement of what is reflected in the records maintained by the service organization. Therefore, such confirmations do not, taken alone, constitute reliable audit evidence. In these circumstances, the plan auditor may consider whether an alternative source of independent evidence can be identified.

- *Performing analytical procedures on the records maintained by the plan or on the reports received from the service organization*. The effectiveness of analytical procedures is likely to vary by assertion and will be affected by the extent and detail of information available.

Paragraph .A29 of AU-C section 402 states that in certain circumstances, in particular when the plan outsources some or all of its finance functions to a service organization, the plan auditor may face a situation in which a significant portion of the audit evidence resides at the service organization. Substantive procedures may need to be performed at the service organization by the plan auditor or the service auditor on behalf of the plan auditor. A service auditor may provide a type 2 SOC 1 report and, in addition, may perform substantive procedures on behalf of the plan auditor.

Obtaining and Using a Type 2 SOC 1 Report

A SOC 1 report may be the most efficient means of obtaining an understanding of relevant controls at the service organization and responding to assessed risk. The plan auditor will need to read the entire report (the service auditor's report, the description of the service organization's system, and, in a type 2 report, the description of the service auditor's tests of controls and results). As previously stated, if the service organization provides a type 1 SOC 1 report, the plan auditor may use the report to identify and assess the risks of material misstatement of the financial statements assertions affected by the service organization's services. However, a type 1 report does not provide evidence of the operating effectiveness of controls at the service organization. If the plan auditor determines that assessed risks for financial statement assertions affected by the service organization's services warrant further audit evidence, and other procedures do not provide the necessary evidence, the plan auditor will need to obtain evidence of the operating effectiveness of controls at the service organization. A type 2 SOC 1 report is intended to provide such evidence because it includes a description of the service auditor's test of controls and the results of those tests, as well as the service auditor's opinion on the operating effectiveness of those controls.

If the plan auditor intends to use a type 2 SOC 1 report as audit evidence that controls at the service organization are operating effectively, it is important for the plan auditor to determine whether the report provides sufficient appropriate audit evidence about the operating effectiveness of the controls to support the plan auditor's risk assessment by

a. evaluating whether the type 2 SOC 1 report is for a period that is appropriate for the plan auditor's purposes;

b. determining whether complementary user entity's controls identified by the service organization are relevant in addressing the risks of material misstatement relating to the relevant assertions in the plan's financial statements and, if so, obtaining an understanding of whether the plan has designed and implemented such controls and, if so, testing their operating effectiveness;

c. evaluating the adequacy of the time period covered by the tests of controls and the time elapsed since the performance of the tests of controls; and

d. evaluating whether the tests of controls performed by the service auditor and the results of the tests, as described in the description of the service auditor's tests of controls and results, are relevant to the assertions in the plan's financial statements and provide sufficient appropriate audit evidence to support the plan auditor's risk assessment.

When using a SOC 1 report, it is important for the plan auditor to determine the link between individual controls at the service organization and the financial statement assertions to which they relate.

There are two basic approaches to establishing a link between controls and financial statement assertions. The first is a *financial statement-oriented* approach in which the plan auditor lists the major financial statement line items and the relevant assertions associated with those line items and then determines the transactions and processes that "feed" into each line item. In effect, general-ledger accounts are analyzed by identifying related major transactions and processes.

Because transactions, processes, and controls frequently affect multiple general-ledger accounts, using a financial statement-oriented approach often leads to confusion among audit team members and causes audit inefficiencies. This practice aid recommends that the plan auditor take a *transaction-* or *process-oriented* approach to linking controls with the relevant financial statement assertions.

Under the transaction or process-oriented approach, the plan auditor begins by identifying and describing the major transactions and processes of the plan, for example, adding new participants, allocating investment income, and making distributions. These processes are then analyzed by mapping them to the financial statement accounts to which they relate and the relevant financial statement assertions.

Planning Checklist for Audits of Employee Benefit Plans That Use a Service Organization

Exhibit A-2, "Planning Checklist for Audits of Employee Benefit Plans That Use a Service Organization," in appendix A, "Practice Tools," contains a checklist that, together with the accompanying instructions, is designed to help a plan auditor implement a transaction- or process-oriented approach.

SOC 1 Report Considerations in Planning an ERISA Limited-Scope Audit

When a plan administrator elects to limit the scope of the plan audit as permitted by Title 29 of the U.S. *Code of Federal Regulations* (CFR) Part 2520.103-8, Rules and Regulations for Reporting and Disclosure under the Employee Retirement Income Security Act of 1974 (ERISA limited-scope audit), the plan administrator is permitted to instruct the plan auditor not to perform any auditing procedures with respect to investment information prepared and certified by a bank or similar institution or by an insurance carrier that is regulated, supervised, and subject to periodic examination by a state or federal agency. The election is available, however, only if the trustee, custodian, or insurance company certifies both the accuracy and completeness of the investment information submitted. In practice, questions frequently arise about the requirements for obtaining and using a SOC 1 report when performing an ERISA limited-scope audit.

First, recognize that the ERISA limited-scope audit permitted by 29 CFR 2520.103-8 applies only to the investment information certified by the qualified certifying institution. Thus, in an ERISA limited-scope audit, to the extent that the service organization is only providing investment transaction services, a SOC 1 report may not be necessary. Plan investments not held by a qualified certifying institution, such as real estate, leases, mortgages, self-directed brokerage accounts, participant loans, and any other investment or assets not covered by such an entity's certification should be subject to appropriate audit procedures.

The ERISA limited-scope audit permitted by 29 CFR 2520.103-8 does not apply to plan and participant-level transactions such as the following:

- Plan set up
- Participant data
- Employer or employee contributions
- Benefit payments
- Plan allocations
- Other information, transactions, or processes (such as plan mergers)

Therefore, in accordance with paragraph .16 of AU-C section 402, plan auditors should obtain audit evidence about the operating effectiveness of the controls related to these transactions. Obtaining a SOC 1 report, if

available, may be useful under these circumstances. Paragraph 4.28 of the AICPA Audit and Accounting Guide *Employee Benefit Plans* provides additional information on the use of SOC 1 reports in an ERISA limited-scope audit of an employee benefit plan.

Frequently Asked Questions—How Does a Plan Auditor Obtain a SOC 1 Report?

Q. Who should the plan auditor contact to obtain a SOC 1 report?

A. Service organizations may have more than one SOC 1 report; therefore, it is important for the plan auditor to obtain the SOC 1 report directly from the plan sponsor who will be able to obtain the appropriate SOC 1 report for use in the audit of the plan's financial statements. Use of a type 1 SOC 1 report is restricted to management of the service organization, user entities of the service organization's system as of the end of the period covered by the SOC 1 report, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting. Use of a type 2 SOC 1 report is restricted to management of the service organization, user entities of the service organization's system during some or all of the period covered by the SOC 1 report, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting.

Chapter 5
How to Use a SOC 1 Report

This chapter describes some of the key considerations for an auditor of a plan's financial statements when using a SOC 1 report and determining its effect on the audit of the plan's financial statements. Considerations regarding evaluating the adequacy of a SOC 1 report are also addressed in chapter 4, "Responding to the Assessed Risks of Material Misstatement When the Plan Uses a Service Organization."

Type of SOC 1 Report

One of the first items to consider when using a SOC 1 report is whether the report is a type 1 or type 2 report. A type 1 SOC 1 report consists of management's description of a service organization's system and the service auditor's report on that description and on the suitability of the design of controls. A type 2 SOC 1 report consists of management's description of a service organization's system and the service auditor's report on that description and on the suitability of the design and operating effectiveness of controls.

Type 1 SOC 1 Reports

According to paragraph .08 of AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*), a type 1 SOC 1 report contains (note that the items in *italics* represent items different from a type 2 SOC 1 report)

a. management's description of the service organization's system, *as of a specified date*.

b. a written assertion by management of the service organization about whether, based on the criteria

  i. 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*, and

  ii. 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.

c. a report that expresses an opinion on the matters in *b*(i)–(ii).

As indicated in chapter 4, a type 1 or type 2 SOC 1 report may be used by the plan auditor to obtain a sufficient understanding of controls at the service organization that are relevant to the audit of the plan's financial statements. Both reports contain the service organization's description of its system and the service auditor's opinion on the fairness of the presentation of the service organization's description of its system and the suitability of the design of the controls included in the description.

Type 2 SOC 1 Reports

A type 2 SOC 1 report contains (note that the items in *italics* represent items in addition to or different from a type 1 SOC 1 report)

a. management's description of the service organization's system *throughout a specified period*.

b. a written assertion by management of the service organization about whether, based on the 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*;

ii. 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 *throughout the specified period*; and

iii. the controls related to the control objectives stated in management's description of the service organization's system operated effectively *throughout the specified period* to achieve those control objectives.

c. a report that

i. expresses an opinion on the matters in *b*(i)–(iii).

ii. includes a description of the test of controls and the results thereof.

Practice Pointer. AT-C section 320 requires the service auditor to request a written assertion about the matters covered by the service auditor's opinion. If management refuses to provide such an assertion, the service auditor should withdraw from the engagement.

Timing Considerations

In a type 1 SOC 1 report, the service organization's description of its system and the service auditor's report are as of a specified date. In a type 2 SOC 1 report, the service organization's description of its system and the service auditor's report are for a period of time, which is the same period covered by the service auditor's tests of controls. The as of date or period covered by the report are identified in the service auditor's report. The plan auditor should evaluate whether the type 1 SOC 1 report is as of a date, or in the case of a type 2 SOC 1 report, for a period that is appropriate for the plan auditor's purposes.

It is not unusual for a type 1 SOC 1 report to be as of a date that is different from the plan's fiscal year-end or for a type 2 SOC 1 report to cover a period that is different from the period covered by the plan's financial statements. However, such a report may be useful in obtaining a preliminary understanding of the controls implemented by the service organization if the report is supplemented by additional current information from other sources. If the date of the SOC 1 report is prior to the period under audit, the plan auditor may perform additional procedures such as

a. making inquiries of employee benefit plan personnel about any changes at the service organization. The employee benefit plan personnel who are consulted should be those who are in a position to know about such changes. These discussions may include inquiries relating to

i. changes in personnel at the service organization with whom plan personnel interact;

ii. changes in reports or other data received from the service organization;

iii. changes in contracts or service level agreements with the service organization; and

iv. errors identified in the service organization's processing, if any, and how they were corrected.

b. reading current documentation and correspondence from the service organization.

c. making inquiries of service organization personnel or of the service auditor (either through the plan or after obtaining approval from the plan to do so) regarding

i. changes to automated or manual systems, including related controls, that occurred outside of the period covered by the service auditor's report but during the period covered by the plan's financial statements;

ii. additional information concerning the reliability of the processing of financial information; and

iii. whether the service auditor would consider applying agreed-upon procedures to supplement the SOC 1 report, if necessary.

If there have been significant changes in the service organization's controls, it is important to gain an understanding of the changes and consider the effect of the changes on the audit of the plan's financial statements.

A type 2 SOC 1 report may cover a period that overlaps a portion of the plan's reporting period. In determining the audit evidence that such a report can provide, it is important for the plan auditor to consider that the longer the time elapsed since the performance of tests of controls, the less evidence the test may provide. When a type 2 SOC 1 report covers only a portion of the plan's reporting period, an additional type 2 SOC 1 report covering the gap period may provide additional audit evidence.

The plan auditor should consider the following relevant factors when determining the nature and the extent of the additional evidence that is needed to update a type 2 SOC 1 report:

- The significance of the assessed risks of material misstatement at the assertion level
- The specific controls that were tested during the period covered by the type 2 SOC 1 report and significant changes to them since they were tested, including changes in the information systems, processes, and personnel
- The degree to which audit evidence about the operating effectiveness of those controls was obtained
- The length of the remaining untested period
- The extent to which the plan auditor intends to reduce further substantive procedures by relying on the operating effectiveness of controls at the service organization
- The effectiveness of the control environment and related monitoring controls at the plan

If the period covered by the type 2 SOC 1 report is completely outside the period under audit, the plan auditor will be unable to rely on such tests to conclude that controls are operating effectively because such tests do not provide evidence of the operating effectiveness of controls during the period under audit. In accordance with paragraph .A34 of AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), when there is little or no overlap and another type 2 SOC 1 report is not available, the plan auditor may consider the need to perform, or use another auditor to perform, tests of controls at the service organization. If testing controls for the uncovered or gap period is not an effective or efficient approach for the auditor of the employee benefit plan's financial statements, management of the plan may consider requesting that the service organization have the service auditor perform the necessary testing.

The Service Auditor's Report

When reading the service auditor's report in a SOC 1 report, it is important for the plan auditor to consider whether the service auditor has modified the service auditor's opinion and, if so, the implications that the modification may have on the audit of the plan's financial statements. Modifications to the service auditor's opinion can be for deviations in the fairness of the presentation of the service organization's system, the suitability of the design of controls, or the operating effectiveness of controls. How the plan auditor analyzes and addresses such modifications is discussed in more detail in chapter 6, "Responding to Testing Exceptions and Control Deficiencies and Other SOC 1 Report Considerations."

Understanding the reason for the modification and whether it relates to controls that are relevant to the audit of the plan's financial statements are critical for the plan auditor to understand in determining the effect of the report on the audit of the plan's financial statements.

Description of the Service Organization's System

Both type 1 and type 2 SOC 1 reports contain management's description of the service organization's system. The service organization is responsible for the completeness, accuracy, and method of presentation of the description of the service organization's system.

Management's description of the service organization's system can be used by the plan auditor to obtain information about the controls implemented at the service organization that are relevant to the employee benefit

plan's internal control over financial reporting. Both type 1 and type 2 SOC 1 reports are intended to provide the plan auditor with information necessary to assess risk for assertions in the employee benefit plan's financial statements affected by the service organization's services. However, only a type 2 report provides plan auditors with a description of the service auditor's tests of controls and results of those tests, which is intended to enable the plan auditor to respond to the assessed risk.

The service organization's description presents how the service organization's system is designed and implemented and includes the following information based on the requirements in paragraph .15 of AT-C section 320:

- The types of services provided including, as appropriate, the classes of transactions processed
- The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities
- 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
- How the service organization's system captures and addresses significant events and conditions other than transactions
- The process used to prepare reports and other information for user entities
- The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls
- Other aspects of the service organization's control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to the services provided
- In the case of a type 2 SOC 1 report, whether management's description of the service organization's system includes relevant details of changes to the service organization's system during the period covered by the description
- Whether management's description of the service organization's system does not omit or distort information relevant to the service organization's system, while acknowledging that management's description of the service organization's system is prepared to meet the common needs of a broad range of user entities and their user auditors, and may not, therefore, include every aspect of the service organization's system that each individual user entity and its user auditor may consider important in its own particular environment

When reading management's description of the service organization's system, the plan auditor should determine that the information provided contains sufficient detail to enable the plan auditor to achieve his or her audit objectives relevant to financial statements assertions affected by the service organization's services.

The description should be presented at a level of detail that provides sufficient information for the broad range of user entities and their auditors to obtain an understanding of how the service organization's processing affects the plan's internal control. The degree of detail in the description would be expected to be equivalent to the degree of detail the plan auditor would require if a service organization was not used. However, it need not be so detailed that it potentially would allow a reader to compromise security or other controls. For example, it should describe the classes of transactions that are processed, but not necessarily each individual transaction type. It need not necessarily include every step in the processing of the transactions and may be presented in various formats, such as narratives, flowcharts, tables, and graphics. The description may also indicate the extent of the manual and computer processing used.

Control Objectives, Related Controls, and Assertions

Management's description of the service organization's system should include the control objectives and related controls that management of the service organization believes are likely to be relevant to user entities' internal control over financial reporting. Paragraph .16 of AT-C section 320 indicates that the minimum criteria for evaluating whether controls are suitably designed include whether

a. the risks that threaten the achievement of the control objectives stated in management's description of the service organization's system have been identified by management

b. the controls identified in management's description of the service organization's system would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

In reading the service auditor's report in the SOC 1 report as well as the description of the service organization's system, the plan auditor should determine whether the scope of the engagement covered by the SOC 1 report corresponds with the service, system(s), or aspects of the system used by the plan. It is important to carefully read this section of the report to be sure that the scope of the engagement addressed by the SOC 1 report is adequate for the plan auditor's purposes. Matters that are relevant in determining whether the SOC 1 report is adequate for the plan auditor's purposes include whether the service auditor's report and the description address

a. all significant transactions processed by the service organization for the plan that affect the plan's financial statements.

b. for each significant transaction processed by the service organization, the control objectives and related controls that are relevant to the financial statement assertions affected by the service organization's services.

Complementary User Entity Controls

As discussed previously, when a plan uses a service organization to process transactions, the plan's internal control consists of both

a. controls at the service organization that are relevant to the plan's internal control over financial reporting and

b. controls implemented by the plan.

Most service organizations design their controls with the assumption that certain additional controls will be implemented by the user entities (complementary user entity controls). If these controls are necessary to achieve the control objectives stated in management's description of the service organization's system, they are identified as such in the description. The plan auditor should determine whether complementary user entity controls identified by the service organization are relevant in addressing the risks of material misstatement relating to the relevant assertions in the plan's financial statements and, if so, should obtain an understanding of whether the plan has designed and implemented such controls. An example of a complementary user entity control is a control over passwords used by authorized plan personnel to electronically access the service organization's system. Such a control is designed to ensure that all input sent to the service organization is authorized.

It is important for the plan auditor to determine whether the key complementary user entity controls identified in the SOC 1 report have been suitably designed and implemented at the plan. If the plan auditor intends to use a type 2 SOC 1 report to obtain evidence of the operating effectiveness of controls at the service organization, the plan auditor should also test the operating effectiveness of the relevant complementary user entity controls.

Usually, the plan auditor determines whether the required complementary user entity controls have been designed and implemented by the plan when performing walkthroughs to gain an understanding of the plan and its internal control. In some cases, procedures performed in conjunction with such walkthroughs may also fulfill requirements related to testing the operating effectiveness of complementary user entity controls.

Tests of the Operating Effectiveness of Controls

After the plan auditor has assessed risks for assertions in the plan's financial statements that are affected by the service organization's services, the plan auditor should design and perform further audit procedures whose nature, timing, and extent are based on, and responsive to, the assessed risks of material misstatements at the relevant assertion level. Paragraph .16 of AU-C section 402 states that when the user auditor's risk assessment includes an expectation that controls at the service organization are operating effectively, the user auditor should obtain evidence about the operating effectiveness of those controls by performing one or more of the following procedures:

- Obtaining and reading a type 2 report, if available
- Performing appropriate tests of controls at the service organization
- Using another auditor to perform tests of controls at the service organization on behalf of the plan auditor

If the plan auditor has obtained a type 2 SOC 1 report, the plan auditor should evaluate the service auditor's description of tests of the operating effectiveness of controls and results of those tests by considering the following matters.

- Are the tests of controls that were performed by the service auditor and the results of those tests relevant to the assertions in the plan's financial statements for which the plan auditor intends to rely on the operating effectiveness of controls at the service organization? (To make this determination, the plan auditor evaluates whether the control objective has a direct bearing on the financial statement assertion being tested.)
- Do the results of the tests of controls performed support the risk assessment?

For example, suppose the service auditor performed tests of the operating effectiveness of controls at a trust organization. One of the services performed by the trust organization is recording the purchase and sale of securities and related income for the plan. The following exhibit summarizes certain information that might appear in a type 2 SOC 1 report and the questions that may be considered by the plan auditor relating to how this information affects the audit.

Exhibit 5-1

Information Obtained From a Type 2 SOC 1 Report Regarding Controls Over Transactions Involving the Purchase and Sale of Securities

Source: Type 2 SOC 1 Report		
Required Elements in the Description of Test of Controls	***Information Provided By the Service Auditor***	***Plan Auditor's Considerations***
Control objective	Security purchase and sale transactions are recorded at the appropriate amounts and in the appropriate periods.	• Does the control objective have a direct relationship to the plan's financial statement assertion? • If so, which ones?
Control policy or procedure	Reconciliations of trade activity processed on the trading system to settled cash are performed daily. Reconciling items are researched and resolved.	
Tests of control	Inspected a sample of daily reconciliations covering the audit period to determine whether they were reconciled and whether reconciling items were researched and resolved in a timely manner.	• Is the description of the tests sufficient to determine the nature, timing, and extent of the tests performed by the service auditor? • Are the nature, timing, and extent of the service auditor's test procedures capable of providing sufficient appropriate audit evidence about the operating effectiveness of the control?
Results of tests	Reconciling items for the reconciliations inspected appeared to result from normal processing and ranged from a few cents to several thousand dollars. Reconciling items were identified timely but were not always resolved in a timely manner.	Do the results of the tests support the plan auditor's risk assessment? Can the plan auditor rely on the operating effectiveness of the controls to reduce the extent of substantive procedures?

Frequently Asked Questions—Using SOC 1 Reports

Q. If a plan auditor is using a type 2 SOC 1 report that states that the service organization's controls over participant contributions were tested and no exceptions were found, could the type 2 SOC 1 report be relied on to eliminate the need for detailed substantive testing, or is more testing necessary?

A. Paragraph .18 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained* (AICPA, *Professional Standards*), states that irrespective of the assessed risks of material misstatement, the auditor should design and perform substantive procedures for all relevant assertions related to each material class of transactions, account balance, and disclosure. The service auditor's tests of controls alone are not sufficient to allow a plan auditor to completely eliminate substantive testing for financial statement assertions affected by these controls. In addition to the service auditor's tests of controls at the service organization, the plan auditor should also

- consider the design and, possibly, the operating effectiveness of complementary user entity controls maintained by the plan, and
- perform substantive tests of the account balance.

If a plan auditor can rely on the operating effectiveness of controls, he or she may be able to use that information in reducing the extent of substantive procedures to be performed.

Chapter 6
Responding to Testing Exceptions and Control Deficiencies and Other SOC 1 Report Considerations

When reading the service auditor's report on a SOC 1 engagement, one or more of the following conditions may be identified:

- Deviations in management's description of the service organization's system. (For example, controls included in the description have not been implemented, the description includes information that is not relevant to user entities' internal control over financial reporting, the description omits a relevant control objective, and, in a type 2 report, the description omits relevant information about changes to controls.)
- Deviations in the suitability of the design of controls. (This occurs when either a control necessary to meet a control objective is missing or an existing control is not suitably designed so that, even if the control operates as designed, the control objective would not be met.)
- Deviations in the operating effectiveness of controls identified during testing. (This occurs when a properly designed control at the service organization does not operate as designed or the person performing the control does not possess the necessary authority or competence to perform the control effectively.)

In all of these instances, it is important for the plan auditor to

a. evaluate the condition;

b. determine how it affects his or her ability to obtain an understanding of the plan's internal control;

c. determine how it affects the plan auditor's assessment of the risk of material misstatement of financial statement assertions affected by the service organization's services; and

d. develop an appropriate audit response, based on the preceding determinations.

Practice Pointer. AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), refers to the aforementioned instances as *deviations*. Such deviations are commonly referred to as *exceptions*.

Effect on the Plan Auditor

As discussed in chapter 4, "Responding to the Assessed Risks of Material Misstatement When the Plan Uses a Service Organization," any one, or a combination of, the preceding conditions may lead the service auditor to modify his or her report. A plan auditor is expected to evaluate the conditions that gave rise to the modification in the service auditor's report and to consider the effect of the condition(s) on the plan's internal control over financial reporting. The following sections are designed to provide the plan auditor with assistance in evaluating and responding to these conditions.

Other SOC 1 Report Considerations

When reading the description of the service organization's system, a plan auditor may conclude that the description is not adequate for his or her purposes. These shortcomings may include any of the following:

- Lack of sufficient detail, which prevents the plan auditor from gaining the knowledge needed to obtain an understanding of the plan's internal control or assess the risks of material misstatement of the financial statements assertions affected by the service organization's services
- Lack of sufficient scope (for example, the report does not include information about a particular service used by the employee benefit plan)
- For a type 1 SOC 1 report, lack of synchronicity between the as of date of the type 1 SOC 1 report and the as of date of the plan's statement of net assets available for benefits (for example, the as of date for the description of the service organization's system does not coincide with the plan's year-end)
- For a type 2 SOC 1 report, lack of synchronicity between the period covered by the type 2 SOC 1 report and the period covered by the plan's financial statements (for example, the period covered by the service auditor's tests of controls does not coincide with the plan's reporting period)

If the SOC 1 report does not provide the plan auditor with the necessary information to assess risk for assertions in the plan's financial statements affected by the service organization's services, and the plan auditor is unable to obtain that information from the plan itself, as described in the "Obtaining Information About the Nature of the Services" section in chapter 3, "Using the Services of a Service Organization," the plan auditor should obtain the necessary information from one or more of the following procedures:

- Contacting the service organization, through the plan, to obtain specific information.
- Visiting the service organization and performing procedures that will provide the necessary information about the relevant controls at the service organization.
- Using another auditor to perform procedures at the service organization.

If performing these other procedures still does not enable the plan auditor to obtain a sufficient understanding of the plan's internal control, then he or she will need to consider modifying his or her opinion or disclaiming an opinion because of a scope limitation.

Deviations in the Results of Tests

Paragraph .A39 of AU-C section 402 indicates that the service auditor's report in a type 2 SOC 1 report identifies results of tests, including deviations, and other information that could affect the plan auditor's conclusions. Deviations noted by the service auditor or a modified opinion in the service auditor's report do not automatically mean that the SOC 1 report will not be useful for the audit of the plan's financial statements in assessing the risks of material misstatement. Rather, the deviations and the matter giving rise to a modified opinion in the service auditor's report are considered in the plan auditor's assessment of the results of tests of controls performed by the service auditor. In considering the deviations and matters giving rise to a modified opinion, the plan auditor may discuss such matters with the service auditor. Such communication is dependent upon the plan contacting the service organization and obtaining the service organization's approval for the communication to take place.

Deviation in IT and Non-IT Controls

A service organization's controls generally consist of IT controls and non-IT controls, and deviations may be identified in either type of control. The following are areas in which deviations in IT controls may occur and examples of those deviations:

- *Information security*. Controls over physical access to computer hardware or logical access to computer applications.

  - — Improper level of access is granted to employees based on the employee's job description.
  - — Access privileges are not removed timely for terminated employees or employees whose job responsibilities have changed such that access is no longer required.
  - — Password policies are not enforced or are not in place.
- *Change management*. Controls over changes to existing system software or the implementation of new system software.
  - — Changes are not approved by designated individuals or are not approved timely.
  - — Changes are not adequately tested in accordance with prescribed testing procedures.
  - — Changes are not documented in accordance with requirements, including documentation of approvals or of test results.

The following are examples of non-IT deviations:

- Improper set-up of plan provisions
- Inaccurate processing of enrollment information
- Inaccurate computation of vesting for distributions
- Participant data changes processed without proper authorization

The following language illustrates a service auditor's description of the results of tests when an exception has occurred:

Example 1: For 1 of 45 unscheduled changes, there was no evidence of required approvals.

Example 2: For 2 of the 15 selected dates, the reconciliation between the trust system and recordkeeping system was not performed timely.

When evaluating the significance of exceptions or deviations, be sure to fully understand the situation described by the service auditor and whether any of the following apply:

- The service auditor obtained evidence that the control was not performed.
- The service auditor was unable to obtain any evidence relating to the performance of the control because of a scope limitation. (For example, there was a change in controls during the period covered by the service auditor's report and the service auditor was unable to test the control that was superseded, documentation has been destroyed in a fire, or electronic records were inadvertently deleted). If this is the case, the significance of the procedures that the service auditor was unable to perform due to the scope limitation should be considered. For example, if the service auditor was unable to review evidence for 1 transaction out of the 40 selected, it is important for the plan auditor to evaluate the service auditor's observations, determine their effect on assessed risks, and, possibly, reassess risk. As part of this process, it is important for the plan auditor to consider the following questions:
  - — Which accounts or assertions in the plan's financial statements could be misstated if the control failed and there were no other controls in place to prevent, or detect and correct, a misstatement?
  - — How significant would the misstatement be to the plan's financial statements?
  - — Considering the significance of the deviation plus the operation of other controls that address the same control objective, what is the likelihood that a misstatement to the plan's financial statements could occur?
  - — Does the plan or the service organization have controls in place to mitigate the effect of the nonperforming control?

— Did management of the service organization provide a response to the exception(s) noted, and did the service auditor test management's responses to mitigate the effect of the exceptions?

— Has the service organization provided additional information that could be considered by the plan auditor?

— Did the service auditor test additional items (such as expanded testing of the control) or perform additional procedures, the results of which mitigate the effect of the exception?

— Given the type of misstatement that could occur, its significance to the plan's financial statements, and the likelihood of a misstatement happening, are the plan auditor's planned audit procedures sufficient? For example, the deviations in the operation of the controls at the service organization may result in the need to revise

  - the nature of the planned procedures (for example, calling participants to confirm balances, rather than sending confirmations).
  - the extent of the planned procedures (for example, performing more of the same planned substantive procedure [sending additional confirmations]).
  - the timing of the planned procedures (for example, performing substantive tests closer to the plan's year-end).

If the plan auditor had planned on relying on the operating effectiveness of a control to reduce substantive tests, deviations in the operation of the control at the service organization may preclude the plan auditor from doing so.

Paragraph .20 of AU-C section 402 indicates that the plan auditor should modify the opinion in the plan auditor's report in accordance with AU-C section 705, *Modifications to the Opinion in the Independent Auditor's Report* (AICPA, *Professional Standards*), if the plan auditor is unable to obtain sufficient appropriate audit evidence regarding the service provided by the service organization relevant to the audit of the plan's financial statements.

Finally, it is important for the plan auditor to consider whether deviations in the operation of the control at the service organization represents a significant deficiency or a material weakness in the plan's internal control over financial reporting that should be communicated to management and those charged with governance of the plan. Paragraph .A40 of AU-C section 402 indicates that the plan auditor is required by AU-C section 265, *Communicating Internal Control Related Matters Identified in an Audit* (AICPA, *Professional Standards*), to communicate in writing to management and those charged with governance significant deficiencies and material weaknesses identified during the audit. When applying the guidance in AU-C section 265, it is important for the plan auditor to evaluate whether matters related to the use of a service organization, such as the following, represent significant deficiencies or material weaknesses that should be communicated to management and those charged with governance of the plan.

- Monitoring controls that may be implemented by the plan to mitigate weaknesses in the service organization's controls have not been implemented.
- Complementary user entity controls identified in a SOC 1 report have not been implemented at the plan.
- Controls that may be needed at the service organization do not appear to have been implemented or were implemented, but are not operating effectively.

In addition to communicating significant deficiencies and material weaknesses to plan management or those charged with governance, the plan auditor is not precluded from communicating other matters or recommendations, related to the use of the service organization.

Glossary

The following definitions are from paragraph .08 of AU-C section 402, *Auditing Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*).

complementary user entity controls. Controls that management of the service organization assumes, in the design of its service, 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.

service auditor. A practitioner who reports on controls of a service organization.

service organization. An organization or segment of an organization that provides services to user entities that are relevant to those user entities' internal control over financial reporting.

service organization's system. 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. Management's description of the service organization's system identifies the services covered, the period to which the description relates (or in the case of a type 1 report, the date to which the description relates), the control objectives specified by management or an outside party, the party specifying the control objectives (if not specified by management), and the related controls.

subservice organization. A service organization used by another service organization to perform some of the services provided to user entities that are relevant to those user entities' internal control over financial reporting.

user auditor. An auditor who audits and reports on the financial statements of a user entity.

user entity. An entity that uses a service organization and whose financial statements are being audited.

Appendix A
Practice Tools

These practice tools are designed to assist the auditor of an employee benefit plan's financial statements in applying the requirements in AU-C section 402, *Audit Consideration Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), for (*a*) considering an employee benefit plan's use of a service organization when obtaining an understanding of the plan's internal control and assessing the risks of material misstatement of financial statement assertions affected by the service organization's services, and (*b*) documenting the procedures performed and findings. These practice tools incorporate the nonauthoritative suggestions contained in this publication. The following is a list of the practice tools contained in this appendix.

- Exhibit A-1, "Audit Program: Auditing the Financial Statements of an Employee Benefit Plan That Uses A Service Organization"
- Exhibit A-2, "Planning Checklist for Audits of Employee Benefit Plans That Use a Service Organization"
- Exhibit A-3, "Documenting the Use of a Type 2 Service Auditor's Report In an Audit of an Employee Benefit Plan's Financial Statements"

These tools have not been peer reviewed or subjected to any other form of quality assurance. Before using them in an engagement, the plan auditor should determine whether they are suitable for his or her purposes. Reports on controls at a service organization that are relevant to a user entity's internal control over financial reporting have been designated SOC 1 reports.[1] These reports are issued under AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*). See appendix B, "An Overview of SOC 1, 2, and 3 Reports," for a discussion of all three types of SOC reports.

Exhibit A-1—Audit Program: Auditing the Financial Statements of an Employee Benefit Plan That Uses a Service Organization

Effect of an Employee Benefit Plan's Use of a Service Organization on the Audit of the Plan's Financial Statements

Page _____ of _____

Name of Employee Benefit Plan: _____

As of Date of Statement of Net Assets Available for Benefits: _____

Audit Objectives:

1. Determine whether information about controls at the service organization is needed in order to
   a. obtain an understanding of the employee benefit plan's internal control over financial reporting as it relates to assertions in the plan's financial statements affected by the service organization's services (applicable to all audits of plan's that use a service organization).
   b. assess the risk of material misstatement for those assertions (applicable to all audits of plans that use a service organization).

[1] The fact that an employee benefit plan uses a service organization does not always require that the plan auditor obtain a service auditor's report (SOC 1 report). For example, a user entity may implement effective controls over the data or other information it receives from the service organization, in which case the plan auditor would most likely focus on the plan's controls. The plan auditor also might visit the service organization and perform procedures there to obtain an understanding of controls at the service organization that affect assertions in the plan's financial statements and to determine if those controls are suitably designed. If the plan auditor needs a basis for reducing assessed risk for those financial statement assertions, the plan auditor could test the operating effectiveness of the controls at the service organization.

c. obtain an understanding of the design of controls relevant to those financial statement assertions and whether they have been implemented. These controls may be implemented by the service organization or by the employee benefit plan (applicable to all audits of plans that use a service organization).

d. if the plan auditor's risk assessment includes an expectation that controls are operating effectively or if substantive procedures alone do not provide sufficient appropriate audit evidence, obtain evidence about the operating effectiveness of controls at the service organization that may enable the plan auditor to reduce assessed risk for relevant financial statement assertions.

2. If a SOC 1 report is available, read the SOC 1 report to

a. obtain an understanding of how the service organization's services and controls affect the plan's financial statements and the types of potential misstatements that could occur.

b. obtain an understanding of controls at the service organization in order to assess the risks of material misstatement of the plan's financial statements.

c. obtain an understanding of the design of controls at the service organization that are relevant to the audit of the plan's financial statements and how those controls are linked to assertions in the plan's financial statements.

d. evaluate the suitability of the design of those controls and determine whether they have been implemented.

e. assess the risk of material misstatement for assertions in the plan's financial statements affected by the service organization's services.

f. design the nature, timing, and extent of further audit procedures.

Audit Objective	*Audit Procedure for Consideration*	*Performed By*	*Working Paper Index*
	Planning (See exhibit A-2, "Planning Checklist for Audits of Employee Benefit Plans That Use a Service Organization") 1. Identify plan transactions that are processed by the service organization. 2. Link the transactions identified in step 1 to the relevant assertions in the plan's financial statements. 3. If a SOC 1 report is available, obtain the SOC 1 report from the plan sponsor. Determine whether the report addresses each of the transactions identified in step 1. If a SOC 1 report does not address the transactions in step 1 or is unavailable, then do either of the following: *a.* Perform alternative procedures to obtain the information necessary to obtain an understanding of the services provided by the service organization and how those services affect assertions in the plan's financial statements. Then, assess the risk of material misstatement for those assertions. *b.* Modify the plan auditor's opinion for a scope limitation. Controls at the service organization may be designed with the expectation that complementary user entity controls will be implemented by the plan.		

Audit Objective	*Audit Procedure for Consideration*	*Performed By*	*Working Paper Index*
	Read the SOC 1 Report and Assess Implications for the Audit 4. Read the SOC 1 report and assess its implications for the audit of the plan's financial statements, including *a.* whether the SOC 1 report is a type 1 or a type 2 report. *b.* the nature of the opinions in the SOC 1 report (unmodified, modified, or disclaimer), the reason for the opinion (if other than an unmodified opinion) and, for a type 2 SOC 1 report, whether the service auditor has identified exceptions or deviations in his or her tests of controls. *c.* for a type 1 report, compare the as of date of the service organization's description of its system and the service auditor's report to the as of date of the plan's financial statements. *d.* for a type 2 report, compare the period covered by the description of the service organization's system, the service auditor's report, and the service auditor's tests of the operating effectiveness of controls to the period covered by the plan's financial statements. *e.* if the report is as of a date or for a period that precedes the beginning of the period under audit, consider performing procedures to update the information, such as the following: i. Discuss changes at the service organization with plan personnel who would be in a position to know of such changes ii. Review current documentation and correspondence issued by the service organization iii. Discuss changes with service organization personnel 5. Read management's description of the service organization's system and evaluate the effect of the following on the audit of the plan's financial statements: *a.* Whether management's description of the service organization's system includes the services provided by the service organization that are significant to the plan's financial statements.		

(continued)

Audit Objective	*Audit Procedure for Consideration*	*Performed By*	*Working Paper Index*
	b. Whether the description includes the aspects of the five components[2] of the service organization's internal control that may be relevant to the plan's financial statement assertions. *c.* Whether the description is sufficiently detailed to enable the plan auditor to obtain an understanding of how the service organization's processing or other service affect the plan's financial statements. *d.* In a type 2 report, whether management's description of the service organization's system identifies changes to the system during the period covered by the report. *e.* Whether the description of the service organization's system is adequate to provide the plan auditor with an understanding of those elements of the plan's information system that are maintained by the service organization. 6. Determine whether the complementary user entity controls identified in the SOC 1 report that the service auditor assumes will be implemented by the user entities are relevant to addressing the risks of material misstatement of relevant assertions in the plan's financial statements, and *a.* list those complementary user entity controls. *b.* obtain an understanding of the design of the relevant complementary user entity controls and whether they have been implemented. *c.* if the plan auditor plans to use a type 2 SOC 1 report as audit evidence that controls at the service organization are operating effectively, test the operating effectiveness of the relevant complementary user entity controls.		

[2] The five interrelated components of internal control are control environment; the entity's risk assessment process; the information system, including the related business processes relevant to financial reporting and communication; control activities relevant to the audit; and monitoring of controls.

Audit Objective	*Audit Procedure for Consideration*	*Performed By*	*Working Paper Index*
	Tests of Operating Effectiveness, If Applicable 7. Read the service auditor's description of tests of controls and results and assess whether the information is satisfactory for the plan auditor's purposes. Consider the following: *a.* The scope of the SOC 1 report (the services provided and the system[s] or aspects of the system covered by the service auditor's report) and whether that scope corresponds with the service, system(s), or aspects of the system used by the employee benefit plan. *b.* The link between the plan's financial statement assertions, the control objectives, and the controls tested. *c.* The nature, timing, and extent of tests performed as they relate to the assertions that are significant to the plan's financial statements. 8. Evaluate the results of the tests of controls and determine whether they support the plan auditor's risk assessment.		

Exhibit A-2—Planning Checklist for Audits of Employee Benefit Plans That Use a Service Organization

Instructions for Use

This checklist is designed to assist the plan auditor in identifying the service organizations that provide services to the employee benefit plan that affect the plan's financial statements. (See chapter 3, "Using the Services of a Service Organization," for guidance on using this planning checklist.) The following are the definitions of the column headings that appear in the checklist.

Column	*Information to Be Documented*
1	Tasks or functions that employee benefit plans commonly outsource to a service organization. Chapter 3 contains an illustrative list of such tasks or functions that serves as a good starting point for identifying service organizations, but ultimately, the information in the checklist should be tailored to the employee benefit plan that is being audited.
2	The financial statement line items affected by each task or function listed in column 1.
3	The financial statement assertions affected by each task or function listed in column 1.
4	The plan auditor's risk assessment (H, M, L) for the financial statement assertions in column 3.
5	Whether the process identified in column 1 is performed by a service organization. (A *No* response indicates that the function is performed by the employee benefit plan.)

(continued)

Column	*Information to Be Documented*
6	The auditor's conclusion about whether a SOC 1 report is needed to obtain an understanding of internal control and assess risk for assertions in the plan's financial statements affected by the service provided by the service organization (see exhibit 3-1, "Considering a Service Organization in an Employee Benefit Plan Audit"). The fact that a service organization is part of the plan's information system does not necessarily mean that the auditor needs to obtain a SOC 1 report. The plan auditor may be able to achieve his or her audit objectives related to obtaining an understanding of the plan's internal control and assessing risk through other means, for example, by focusing on relevant controls implemented by the user entity or by performing procedures at the service organization. The suggestions provided in exhibit 3-1 help the auditor to determine whether a SOC 1 report is needed for the plan auditor to assess risk for assertions in the plan's financial statements affected by the services provided by the service organization as they relate to each of the tasks or functions in column 1.
7	The auditor's conclusion about whether the SOC 1 report provided by the service organization meets the plan auditor's needs. Matters to be considered are the services, business units, functions, or applications covered by the report; whether the SOC 1 report is as of a date, or in the case of a type 2 report, for a period that is appropriate for the plan auditor's purposes, and whether the SOC 1 report provides sufficient information to enable the plan auditor to obtain an understanding of the plan's internal control as it is affected by the services provided by the service organization.
8	The name of the service organization that performs the task or function identified in column 1, if applicable.

1	2	3	4	5	6	7	8
Tasks or Functions That May Be Performed By a Service Organization	*Financial Statement Line Items and Assertions Affected by the Service Organization's Services*		*Plan Auditor's Risk Assessment (High, Medium, or Low)*	*Is the Task or Functions in Column 1 Performed by a Service Organization?*	*Is a SOC 1 Report Needed?*	*If a SOC 1 Report is Needed, Should the Available Report be Used?*	*Name of Service Organization*
	Line Items	***Assertions***					
Plan set-up			H M L	Y N	Y N	Y N	
New participants and enrollments			H M L	Y N	Y N	Y N	
Investment elections and changes			H M L	Y N	Y N	Y N	
Deferral rate elections and changes			H M L	Y N	Y N	Y N	
Participant data and changes			H M L	Y N	Y N	Y N	
Reconciliation of the participants' records (trust vs. record-keeping)			H M L	Y N	Y N	Y N	

1	2	3	4	5	6	7	8
Tasks or Functions That May Be Performed By a Service Organization	*Financial Statement Line Items and Assertions Affected by the Service Organization's Services*		*Plan Auditor's Risk Assessment (High, Medium, or Low)*	*Is the Task or Functions in Column 1 Performed by a Service Organization?*	*Is a SOC 1 Report Needed?*	*If a SOC 1 Report is Needed, Should the Available Report be Used?*	*Name of Service Organization*
	Line Items	***Assertions***					
Participant loans			H M L	Y N	Y N	Y N	
Employer contributions received and receivable			H M L	Y N	Y N	Y N	
Participant contributions received and receivable			H M L	Y N	Y N	Y N	
Benefit payments			H M L	Y N	Y N	Y N	
Contracts with insurance companies and similar contracts			H M L	Y N	Y N	Y N	
Purchase and sale of securities			H M L	Y N	Y N	Y N	
Allocation of investment income			H M L	Y N	Y N	Y N	
Other participant-level transactions			H M L	Y N	Y N	Y N	
Services ancillary to holding equity securities			H M L	Y N	Y N	Y N	
Pricing of derivatives and securities			H M L	Y N	Y N	Y N	
Security lending transactions			H M L	Y N	Y N	Y N	
Payroll			H M L	Y N	Y N	Y N	

(continued)

1	2	3	4	5	6	7	8
Tasks or Functions That May Be Performed By a Service Organization	*Financial Statement Line Items and Assertions Affected by the Service Organization's Services*		*Plan Auditor's Risk Assessment (High, Medium, or Low)*	*Is the Task or Functions in Column 1 Performed by a Service Organization?*	*Is a SOC 1 Report Needed?*	*If a SOC 1 Report is Needed, Should the Available Report be Used?*	*Name of Service Organization*
Compliance With the Employee Retirement Income Security Act			H M L	Y N	Y N	Y N	
Preparation of Form 5500			H M L	Y N	Y N	Y N	

Exhibit A-3—Documentation of Use of a Type 2 Service Auditor's Report in an Audit of an Employee Benefit Plan's Financial Statements

To help CPAs meet the challenges of performing quality audits in the unique and complex employee benefit plan area (plan), the Employee Benefit Plan Audit Quality Center (EBPAQC) has assembled a wide variety of resources and tools.

Among the many tools, the EBPAQC has prepared the following tool to assist members in documenting procedures and findings related to controls at a service organization that are likely to be relevant to the plan's internal control over financial reporting. It focuses on the plan auditor's use of a type 2 report.

Documentation of Use of a Type 2 Service Auditor's Report in an Audit of an Employee Benefit Plan's Financial Statements

Plan Information

PLAN NAME:	CLIENT NUMBER:
PLAN YEAR END:	SCOPE OF PLAN AUDIT: LIMITED ___ FULL ____

Note: *This nonauthoritative tool is intended to assist CPAs auditing the financial statements of employee benefit plans that use one or more service organizations (plan auditors). It is designed to assist plan auditors in documenting their procedures and findings related to controls at a service organization that are likely to be relevant to the employee benefit plan's internal control over financial reporting. It focuses on the plan auditor's use of a* management of a service organization's description of its system and the service auditor's report on that description and on the suitability of the design and operating effectiveness of controls*" (a type 2 report). Both a type 1 report and a type 2 report provide a plan auditor with information about the design and implementation of controls at a service organization that are likely to be relevant to a plan's internal control over financial reporting. Such information is intended to provide the plan auditor with a basis for identifying and assessing the risks of material misstatement in the employee benefit plan's financial statements related to the services provided by the service organization. A type 2 report also includes a description of the service auditor's tests of the operating effectiveness of controls and the results of those tests. That information should enable the plan auditor to determine whether he or she can rely on the operating effectiveness of the controls that were tested for the purpose of determining the nature, timing, and extent of substantive procedures to be performed on related account balances, classes of transactions, and disclosures in the employee benefit plan's financial statements.*

The AICPA has introduced a series of three SOC reports. Service auditors' reports that address controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting are referred to as SOC 1 reports*; for example, management's description of a service organization's system and a service auditor's report on that description and on the suitability of the design and operating effectiveness of controls is referred to as a* type 2 SOC 1 report*. SOC 1 engagements are performed under AT-C section 320,* Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting *(AICPA,* Professional Standards*), and the related reports are referred to as SOC 1 reports.*

This tool is not intended to be used as an audit program or to provide authoritative guidance and should be tailored to the audit firm's employee benefit plan audit practice and the circumstances of the individual plan audit. Certain sections of this tool may be completed by the firm's reviewer (if applicable) to document the use of a type 2 SOC 1 report in an audit of an employee benefit plan's financial statements, whereas other sections may be prepared by the engagement team to document procedures performed to evaluate controls at a service organization. For purposes of this tool, the plan auditor is the user auditor.

Section I—Type 2 SOC 1 Report General Information

NAME OF SERVICE ORGANIZATION
NAME OF SERVICE AUDITOR
SERVICES PROVIDED BY THE SERVICE ORGANIZATION
LOCATIONS COVERED (IF APPLICABLE)
PERIOD COVERED BY THE TYPE 2 SOC 1 REPORT

Section II—Service Auditor's Opinion

What type of opinion did the service auditor express in the type 2 SOC 1 report?

_____ Unmodified

_____ Modified

If modified, document the nature of the modification(s) and any potential effect it may have on the risk of material misstatement in the employee benefit plan's financial statements in the box provided. (*Note*: A modification may affect a single control objective (for example, controls related to enrollment) or may affect several control objectives (for example, IT general controls over logical access).

Section III—Period Covered by the Type 2 SOC 1 Report

Does the type 2 SOC 1 report cover the period covered by the plan's financial statements that are being audited?

_____ Yes (skip to Section IV)

_____ No

If the type 2 SOC 1 report does not cover a significant portion of the period covered by the plan's financial statements, was evidence about the operating effectiveness of controls obtained for the period that is not covered by the type 2 SOC 1 report by performing additional procedures?

Examples of procedures that may be performed include the following:

- Making inquiries of the service organization about any major changes in the controls or processes, any noted issues, or any changes in programs or software at the service organization since the period covered by the service auditor's type 2 SOC 1 report.

(*Note*: Some service organizations provide a "gap letter" that addresses the period from the date of the service auditor's report through the most recent calendar year-end.)

Name of service organization representative contacted: _____

Telephone number: _____

Date contacted: _____

Contacted by: _____

Results:_____

- Reviewing documentation and correspondence issued by the service organization to management of the plan regarding changes to the programs, software, or controls or any noted issues.
- Obtaining additional audit evidence regarding the operating effectiveness of controls at the service organization for the portion of the period that is not covered by the type 2 SOC 1 report. If the plan auditor believes it is necessary, he or she may request that the plan contact the service organization to request that the service auditor perform agreed-upon procedures at the service organization, or the plan auditor may perform such procedures.

Conclusion:

Document the plan auditor's conclusion and any procedures performed, as applicable, and include any supporting documentation.

Section IV—Service Auditor's Professional Reputation

If the plan auditor is unfamiliar with or has no experience with the service auditor that issued the type 2 SOC 1 report, the plan auditor should perform procedures concerning the service auditor's professional competence. Examples of procedures include reviewing online sources of such information, such as the PCAOB website, which includes registration listings and inspection reports; the AICPA's website from which peer review reports and peer review acceptance letters can be accessed; and the website of the applicable state accountancy board. If no information can be found, document that fact, and determine the effect on the audit.

Was the service auditor's report prepared by a CPA firm with whom the plan auditor is familiar?

_____ Yes (skip to Section V)

_____ No

Document procedures performed and include any supporting documentation.

Section V—Use of Subservice Organizations/Carve-Outs

Did the service organization outsource any functions relevant to the plan's internal control over financial reporting to another service organization (a subservice organization), and was the subservice organization carved out of the type 2 SOC 1 report?

_____ Yes

_____ No (skip to Section VI)

If yes, in the following table, list the name(s) of the subservice organization(s) and the functions performed by the subservice organization(s) identified in the service auditor's report, which is included in the type 2 SOC 1 report (and also in management's description of the service organization's system). (If the service organization uses the carve-out method to present its description, the functions performed by the service organizations will be provided, but the names of the subservice organizations may not be provided.) If the functions performed by the subservice organization are significant and relevant to the plan's internal control over financial reporting, the plan auditor may consider obtaining additional information about the subservice organization's controls.

Such information may be available from user manuals, system overviews, technical manuals, the contract between the plan and the service organization, and reports on the subservice organization's controls, prepared by other service auditors, internal auditors, or a regulatory authority.

Complete column 3 to document or reference work performed to address the carved-out subservice organization(s). If the controls and functions performed by the subservice organization are not deemed relevant or significant to the plan's internal control over financial reporting, indicate N/A.

NAME OF SUBSERVICE ORGANIZATION	FUNCTIONS PERFORMED	WORK PERFORMED TO ADDRESS CARVED-OUT SUBSERVICE ORGANIZATION

Section VI—Identification of Control Objectives and Deviations Noted

In this section, the plan auditor will begin to note the control objectives to determine what is present and what is not, and any noted deviations identified in the results of tests of controls that may affect the nature, timing, and extent of the audit procedures in an employee benefit plan audit. List the control objectives included in the description of the service organization's system.

CONTROL OBJECTIVES INCLUDED IN THE SERVICE ORGANIZATION'S DESCRIPTION OF ITS SYSTEM		WERE DEVIATIONS NOTED IN THE SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS?		PAGE(S) # IN SERVICE ORGANIZATION'S DESCRIPTION OR SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS WHERE CONTROL OBJECTIVE IS LOCATED
CONTROLS PROVIDE REASONABLE ASSURANCE THAT:		YES*	NO	
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
* For any *Yes* answers, complete the table that follows.				

In the following table, summarize the service organization's and plan auditor's responses (if any) to any deviations identified by the service auditor in the description of tests of controls and results. *Note:* Deviations in the results of tests of controls should be considered individually and in the aggregate to determine their effect, if any, on audit procedures to be performed.

CONTROL OBJECTIVE # (FROM PRECEDING TABLE)	DEVIATION(S) NOTED	SERVICE ORGANIZATION'S RESPONSE INCLUDED IN THE DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM (SUCH RESPONSES ARE NOT COVERED BY THE SERVICE AUDITOR'S OPINION)	PLAN AUDITOR'S RESPONSES (SEE NOTE THAT FOLLOWS)

Note: Consider any mitigating controls in place at the plan sponsor, or consider designing procedures to address the risks related to the deviations identified in the preceding table.

Conclusion:

_____Deviations were noted as documented previously; however, we have concluded that they would not significantly affect the nature, timing, and extent of our procedures in the audit of the employee benefit plan.

_____Although the deviations did not result in a qualification of the service auditor's opinion on the operating effectiveness of the controls to achieve the control objective, the following procedures were completed by the plan auditor to address and evaluate the effect of the deviations on the audit.

Document procedures performed and include any supporting documentation.

Section VII—Complementary User Entity Controls

Summarize any complementary user entity control considerations identified in the service organization's description of its system.

NO.	COMPLEMENTARY USER ENTITY CONTROL CONSIDERATIONS IDENTIFIED IN THE SERVICE ORGANIZATION'S DESCRIPTION	ARE THE COMPLEMENTARY USER ENTITY CONTROL CONSIDERATIONS IDENTIFIED IN THE SERVICE ORGANIZATION'S DESCRIPTION RELEVANT TO THE PLAN? IF NO, DOCUMENT IN THE SPACE THAT FOLLOWS. IF YES, DOCUMENT OR REFERENCE WORK PERFORMED TO ENSURE COMPLEMENTARY USER ENTITY CONTROLS ARE IN PLACE.	WORKING PAPER REFERENCE (SEE NOTE)
1.			
2.			
3.			

NO.	COMPLEMENTARY USER ENTITY CONTROL CONSIDERATIONS IDENTIFIED IN THE SERVICE ORGANIZATION'S DESCRIPTION	ARE THE COMPLEMENTARY USER ENTITY CONTROL CONSIDERATIONS IDENTIFIED IN THE SERVICE ORGANIZATION'S DESCRIPTION RELEVANT TO THE PLAN? IF NO, DOCUMENT IN THE SPACE THAT FOLLOWS. IF YES, DOCUMENT OR REFERENCE WORK PERFORMED TO ENSURE COMPLEMENTARY USER ENTITY CONTROLS ARE IN PLACE.	WORKING PAPER REFERENCE (SEE NOTE)
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Note: Consider completing the evaluation of the plan sponsor and plan's controls first. For controls already reviewed and evaluated by the plan auditor, insert the working paper reference where that work is documented. If the plan or plan sponsor has not implemented complementary user entity controls then that should be documented, as well as the effect on the nature, timing, and extent of audit procedures.

Section VIII—Documentation of Evaluation of the Control Objectives

If the type 2 SOC 1 report covers only the payroll process, skip Section VIII and go to Section IX.

In the following section, the reviewer or plan auditor can begin to evaluate whether the service organization's description of its system contains controls and control objectives relevant to the assertions included in the employee benefit plan's financial statements. (These are documented in columns 1 and 2 in the following table). In addition, the plan auditor will need to evaluate whether the tests of controls performed by the service auditor and the results of those tests provide sufficient appropriate evidence of the operating effectiveness of the controls to support the auditor's risk assessment. The plan auditor should consider the following factors in making that evaluation:

- The nature, timing, and extent of the testing (for example, when testing controls, the service auditor should perform procedures in addition to inquiry, as required by related risk assessment standards)
- Results of the tests of controls (for example, any noted deviations)

Evaluation of the Control Objectives

Page # in the service organization's description of its system or service auditor's tests of controls where control objective is listed (from Section VI)	Control objective as listed in the description (from Section VI)	Do the descriptions of the controls and the control objectives enable the plan auditor to evaluate the design and confirm the implementation of relevant controls and assess risk? (Yes/No)	Do the tests of operating effectiveness and results of those tests support the achievement of the stated control objective? (Yes/No) Note: Consider the effect of any deviations identified in the preceding table in Section VI	Reference from Section VII to applicable complementary user entity controls identified in the description that are in place to support the plan auditor's risk assessment
IT General Controls/Control Objectives—Logical Access and Program Change Management				
Controls/Control Objectives Related to New Plan Set-Up—Plan Provisions				
Controls/Control Objectives Related to New Plan Set-Up—Participant Level Data/Accounts and Investments				
Controls/Control Objectives Related to Eligibility, Enrollment, and Participant Data				
Controls/Control Objectives Related to Contributions—Plan Level				
Controls/Control Objectives Related to Contributions—Participant Level				
Controls/Control Objectives Related to Participant Account Income/Expense Allocations				
Controls/Control Objectives Related to Distributions to Participants/Beneficiaries				
Controls/Control Objectives Related to Distributions—Plan Expenses				
Controls/Control Objectives Related to Marketable Securities Held—Safekeeping & Valuation				
Controls/Control Objectives Related to Non-Readily Marketable Securities Held—Safekeeping & Valuation				
Controls/Control Objectives Related to Investment Transactions—Purchases/Sales (including realized gain/loss)				
Controls/Control Objectives Related to Investment Income—Plan Level				
Controls/Control Objectives Related to Report Processing—Plan Level				

Page # in the service organization's description of its system or service auditor's tests of controls where control objective is listed (from Section VI)	Control objective as listed in the description (from Section VI)	Do the descriptions of the controls and the control objectives enable the plan auditor to evaluate the design and confirm the implementation of relevant controls and assess risk? (Yes/No)	Do the tests of operating effectiveness and results of those tests support the achievement of the stated control objective? (Yes/No) Note: Consider the effect of any deviations identified in the preceding table in Section VI	Reference from Section VII to applicable complementary user entity controls identified in the description that are in place to support the plan auditor's risk assessment
Controls/Control Objectives Related to Report Processing—Participant Level				
DEFINED CONTRIBUTION PLANS ONLY				
Controls/Control Objectives Related to Participant Loans (Authorization, Calculation, and Recording)				
Controls/Control Objectives Related to Participant Loan Repayments—Plan Level				
Controls/Control Objectives Related to Participant Loan Repayments—Participant Level				
Controls/Control Objectives Related to Investment Election Changes and Transfers				
DEFINED BENEFIT AND HEALTH & WELFARE PLANS				
Controls/Control Objectives Related to Participant Census Data				
Controls/Control Objectives Related to Plan Obligations				
HEALTH & WELFARE PLANS ONLY				
Controls/Control Objectives Related to Claims Processing				

Section IX—Payroll Processing Service Organizations

Most large payroll processors provide a type 1 or type 2 report, but such reports vary widely regarding what services are covered. In addition, some payroll processors issue several reports that cover different locations, services, or markets. Plan sponsors may contract with different payroll processors to provide different services. Plan sponsors are expected by the payroll processors to have controls in place to ensure accurate input and submission of data to the payroll processors (complementary user entity controls). Once the plan auditor has obtained the proper type 2 reports, the plan auditor can complete the following sections.

Documentation of the Evaluation of Payroll Reports

In the following section, the reviewer or plan auditor can begin to evaluate whether the report contains controls and control objectives relevant to the assertions included in the employee benefit plan's financial statements. (These are documented in columns 1 and 2 in the following table). In addition, the plan auditor will need to evaluate whether the tests of controls performed by the service auditor and the results of those tests provide sufficient appropriate evidence of the operating effectiveness of the controls to support the auditor's risk assessment. The auditor should consider the following factors in making that evaluation:

- The nature, timing, and extent of the testing (for example, when testing controls, the service auditor should perform procedures in addition to inquiry, as required by related risk assessment standards)
- Results of the tests of controls (for example, any noted deviations?)

Page # in the service organization's description or service auditor's description of tests of controls where control objective is listed (from Section VI)	Control objective as listed in the description (from Section VI)	Do the descriptions of the controls and control objectives enable the plan auditor to evaluate the design and confirm the implementation of relevant controls and assess risk? (Yes/No)	Do the tests of operating effectiveness and results of those tests support the achievement of the stated control objective? (Yes/No) Note: Consider the effect of any deviations identified in the preceding table in Section VI	Reference from Section VII to applicable complementary user entity controls identified in the description that are in place to support the plan auditor's risk assessment
Controls/Control Objectives Related to Set Up of New Employees (demographic data, pay rates, withholding amounts)				
Controls/Control Objectives Related to Computation of Payroll Amounts Based on Rates (Salary, Hourly)				
Controls/Control Objectives Related to Computation of withholdings (401(k), H&W, and so on)				
Controls/Control Objectives Related to Reporting of Payroll Amounts Paid and Remitted				
Controls/Control Objectives Related to Termination of Employees and Removal From Payroll Records				

Section X—Conclusion

Has the plan auditor obtained a sufficient understanding of the control objectives and related controls at the service organization that are relevant to the plan's internal control over financial reporting in order to assess the risks of material misstatement and to design the nature, timing, and extent of further audit procedures?

_____ Yes

_____ No

Note: If the plan auditor concludes that information is not available to obtain a sufficient understanding to assess the risks of material misstatement, he or she may consider contacting the service organization to obtain

specific information or request that a service auditor be engaged to perform procedures that will provide the necessary information, or the plan auditor may visit the service organization and perform such procedures.

Include any additional comments.

Prepared by: _____ Date: _____

Reviewed by: _____ Date: _____

Appendix B
An Overview of SOC 1, 2, and 3 Reports

AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*), provides guidance to practitioners engaged to report on controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. A practitioner may be engaged to examine and report on controls at a service organization relevant to subject matter other than user entities' internal control over financial reporting, for example, controls that affect the privacy of information processed for the customers of user entities. The applicable attestation standard for such engagements may vary depending on the subject matter. To make practitioners aware of the various professional standards and guides available to them for examining and reporting on controls at a service organization and to help practitioners select the appropriate standard or guide for a particular engagement, the AICPA has introduced the term *service organization control reports*® (or *SOC reports*). The following are designations for three such engagements and the source of the guidance for performing and reporting on them:

- SOC 1: AT-C section 320 and the AICPA Guide *Service Organizations: Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*
- SOC 2: The AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*
- SOC 3: TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*)

The following table identifies the difference between SOC 1, SOC 2, and SOC 3 engagements and the related reports.

	SOC 1 Engagements	SOC 2 Engagements	SOC 3 Engagements
Under what professional standard and interpretive publications is the engagement performed?	AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*) The AICPA Guide *Service Organizations: Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*	AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*) The AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*	AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*) TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*), provides the criteria for evaluating the design and operating effectiveness of controls in these engagements.

(continued)

	SOC 1 Engagements	SOC 2 Engagements	SOC 3 Engagements
What are the criteria for the engagement?	Paragraph .15 of AT-C section 320 contains the minimum criteria for the description of the service organization's system. Paragraph .16 of AT-C section 320 provides the criteria for evaluating the suitability of the design of controls. Paragraph .17 of AT-C section 320 contains the criteria for evaluating the operating effectiveness of controls.	Paragraphs 1.26–.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2 ®)* contain the criteria for the description of the service organization's system. TSP section 100 contains the criteria for evaluating the design and operating effectiveness of controls.	TSP section 100 contains the criteria for evaluating the design and operating effectiveness of controls.
What is the subject matter of the engagement?	Controls at a service organization relevant to user entities' internal control over financial reporting	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy
What is the purpose of the report?	To provide management of the service organization, user entities, and the independent auditor of the user entity's financial statements with information and a service auditor's opinion about controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. It enables the plan auditor to perform risk assessment procedures and, if a type 2 report is provided, to use the report as audit evidence that controls at the service organization are operating effectively.	To provide management of a service organization, user entities, and other specified parties with information and a service auditor's opinion about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy.	To provide interested parties with a service auditor's opinion about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy.
What are the components of the report?	**Components of a Type 1 Report** *a.* Management's description of the service organization's system *b.* A written assertion by management of the service organization about whether, based on the criteria i. management's description of the service organization's system fairly presents	A description of the service organization's system A written assertion by management of the service organization regarding the description of the service organization's system; the suitability of the design of the controls; and in a type 2 report, the operating effectiveness of the controls in meeting the applicable trust services criteria	A description of the system and its boundaries[1] or, in the case of a report that addresses the privacy principle, a copy of the service organization's privacy notice A written assertion by management of the service organization regarding the effectiveness of controls in meeting the applicable trust services criteria

[1] These descriptions are typically less detailed than the descriptions in SOC 1 or SOC 2 reports and are not covered by the practitioner's opinion.

	SOC 1 Engagements	SOC 2 Engagements	SOC 3 Engagements
	the service organization'su system that was designed and implemented as of a specified date ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed and implemented as of the specified date **Components of a Type 2 Report** *a.* Management's description of the service organization's system *b.* A written assertion by management of the service organization about whether, based on the 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 ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives iii. the controls related to the control objectives stated in management's description of the service organization's system operated effectively	A service auditor's report that contains an opinion on the fairness of the presentation of the description of the service organization's system; the suitability of the design of the controls to meet the applicable trust services criteria; and in a type 2 report, the operating effectiveness of those controls In a type 2 report, a description of the service auditor's tests of controls and results of the tests	A service auditor's report on whether the entity maintained effective controls over its system as it relates to the principle being reported on (that is, security, availability, processing integrity, confidentiality, or privacy), based on the applicable trust services criteria

(continued)

	SOC 1 Engagements	SOC 2 Engagements	SOC 3 Engagements
	throughout the specified period to achieve those control objectives *c.* A service auditor's report that i. expresses an opinion on the matters in *b*(i)–(iii) ii. includes a description of the test of controls and the results thereof		
Who are the intended users of the report?	Management of the service organization; user entities during some or all of the period covered by the report (for type 2 reports) and user entities as of a specified date (for type 1 reports); and auditors of the user entities' financial statements	Management of the service organization and other specified parties who have sufficient knowledge and understanding of the following: • The nature of the service provided by the service organization • How the service organization's system interacts with user entities, subservice organizations, and other parties • Internal control and its limitations • User entity responsibilities: complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria • The applicable trust services criteria • The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks	Anyone