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.