

University of Mississippi

eGrove

Guides, Handbooks and Manuals

American Institute of Certified Public Accountants (AICPA) Historical Collection

2013

Using a SOC 1sm report in a financial statement audit; Practice Aid Series

American Institute of Certified Public Accountants (AICPA)

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_guides



Part of the [Accounting Commons](#)

Recommended Citation

American Institute of Certified Public Accountants (AICPA), "Using a SOC 1sm report in a financial statement audit; Practice Aid Series" (2013). *Guides, Handbooks and Manuals*. 1671.

https://egrove.olemiss.edu/aicpa_guides/1671

This Book is brought to you for free and open access by the American Institute of Certified Public Accountants (AICPA) Historical Collection at eGrove. It has been accepted for inclusion in Guides, Handbooks and Manuals by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.

REF

HF

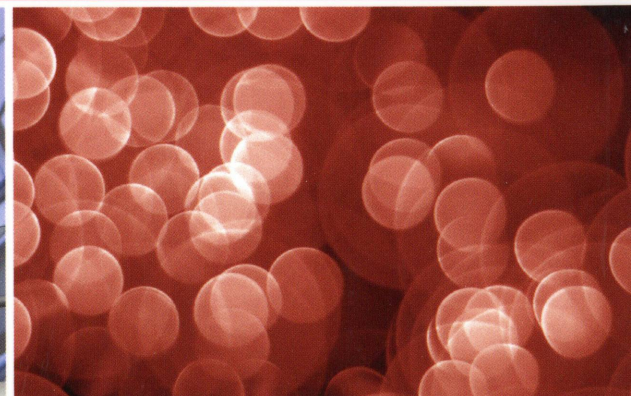
5667

.U87

2013

P R A C T I C E A I D S E R I E S

Using a SOC 1SM Report in a Financial Statement Audit



AICPA[®]

SOC1SM

P R A C T I C E A I D S E R I E S

Using a SOC 1SM Report in a Financial Statement Audit

13638-359

Copyright © 2013 by
American Institute of Certified Public Accountants, Inc.
New York, NY 10036-8775

All rights reserved. For information about the procedure for requesting permission to make copies of any part of this work, please e-mail copyright@aicpa.org with your request. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, 220 Leigh Farm Road, Durham, NC 27707-8110.

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

ISBN 978-1-94023-529-5

Notice to Readers

This practice aid, *Using a SOC 1SM Report in a Financial Statement Audit*, has been developed to provide guidance to user auditors when auditing the financial statements of an entity that uses a service organization (user entity).

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.

Recognition

AICPA Staff

Diana Krupica, CPA
Technical Manager
A&A Content Development

Standards Considered In This Edition

The following references were used in preparing this practice aid:

- ▶ AT section 801, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*) (Effective for service auditor's reports for periods ending on or after June 15, 2011.)

-
-
- ▶ AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*) (Effective for audits of financial statements for periods ending on or after December 15, 2012.)
 - ▶ AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* (AICPA, *Professional Standards*)
 - ▶ AICPA Alert *Service Organization Control Reports*[®]: *Considerations for User and Service Auditors—2013*

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	1
Purpose of This Practice Aid	1
Background.....	2
Types of SOC 1 Reports	3
Applicability to User Entities.....	5
Chapter 2: A Brief Overview	7
Risk Assessment Procedures and Related Activities.....	7
The Auditor’s Understanding of the Entity and Its Environment, Including Its Internal Control	8
Understanding the Entity and Its Environment.....	8
Understanding the Entity’s Internal Control	8
Control Activities and the Information System, Including the Accounting System.....	10
Identifying and Assessing the Risks of Material Misstatement	11
Risk Assessment and an Entity’s Use of IT	12
Chapter 3: Using the Services of a Service Organization	15
Determining Whether the Service Organization Is Part of the User Entity’s Information System.....	18
Understanding the Services Provided By a Service Organization	20

Obtaining Information About The Nature of the Services.....	20
The Nature and Materiality of the Transactions.....	21
Degree of Interaction	21
Nature of the Relationships.....	22
Procedures When the User Auditor Cannot Obtain a Sufficient Understanding from the User Entity	23
Using a SOC 1 Report to Obtain an Understanding of the Services Provided to the User Entity.....	23
Evaluating a SOC 1 Report.....	24
Subservice Organizations.....	27
Chapter 4: Responding to the Assessed Risks of Material Misstatement When the User Entity Uses a Service Organization.....	29
Performing Further Procedures in Response to Assessed Risk When a SOC 1 Report Is Not Available.....	29
Obtaining and Using a Type 2 SOC 1 Report	31
Frequently Asked Questions—How a User Auditor Obtains a SOC 1 Report	32
Chapter 5: How to Use a SOC 1 Report	35
Type of SOC 1 Report.....	35
Type 1 SOC 1 Reports.....	35
Type 2 SOC 1 Reports.....	36
Timing Considerations.....	37

The Service Auditor’s Report	39
Description of the Service Organization’s System.....	40
Control Objectives, Related Controls, and Assertions	42
Complementary User Entity Controls.....	42
Tests of the Operating Effectiveness of Controls	43
Frequently Asked Questions—Using SOC 1 Reports.....	45
Chapter 6: Responding to Testing Exceptions and Control Deficiencies and Other SOC 1 Report Considerations	47
Effect on the User Auditor	48
Other SOC 1 Report Considerations	48
Deviations in the Results of Tests.....	49
Deviation in IT and Non-IT Controls	49
Common User Auditor Issues Related to SOC 1 Reports.....	53
SOC 1 Report Does Not Address All of the Services Provided By the Service Organization	53
Period Covered by the SOC 1 Type 2 Report is Not Sufficient for the User Auditor’s Purposes	53
An Inclusive Subservice Organization’s Assertion Does Not Address all of the Minimum Criteria	54
The SOC 1 Report Carves Out Subservice Organizations.....	55
Service Auditor Expresses a Qualified Opinion Because of Deviations Identified in Tests of Controls.....	55

User Auditor Determines the Type 1 or Type 2 Report is Not Sufficient for His or Her Needs.....	56
Service Auditor Expresses a Qualified Opinion Regarding the Design or Operating Effectiveness of Controls	56
Glossary	57
Appendix A: An Overview of SOC 1, 2, and 3 Reports	59

Chapter 1

Introduction

Purpose of This Practice Aid

This practice aid provides guidance on

- a. how the auditor of the financial statements of an entity that uses a service organization (user entity) uses a report prepared under AT section 801, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*), in the audit of the user entity'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 the auditor of a user entity's financial statements (user auditor) should apply to the information in a report issued under AT section 801.

Hereinafter a report issued under AT section 801 is referred to as a SOC 1SM report.

The glossary of this practice aid contains definitions of technical terms used in AT section 801 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 better understanding the practice aid.

Service auditor. A practitioner¹ 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 relevant to those user entities' internal control over financial reporting. (Examples of service organizations that are commonly used by entities include payroll service providers, custodian of investments, software as a service providers, data center and colocation providers, third party administrators, and investment advisers.)

1. In the attestation standards, a CPA performing an attestation engagement ordinarily is referred to as a *practitioner*. AT section 801, *Reporting on Controls at a Service Organization* (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.

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.

Background

AU-C section 402 addresses the user auditor's responsibility for obtaining sufficient appropriate audit evidence in an audit of the financial statements of a user entity. When planning to use a SOC 1 report in a financial statement audit, AU-C section 402 expands on how the user auditor applies AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, and AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained* (AICPA, *Professional Standards*), in obtaining an understanding of the user entity, including internal control relevant to the audit, sufficient to identify and assess the risks of material misstatement and in designing and performing further audit procedures responsive to those risks.

Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*) has been codified in the attestation standards as AT section 801 and establishes the requirements and guidance for reporting on controls at a service organization relevant to user entities' internal control over financial reporting. The controls addressed in AT section 801 are those that a service organization implements to prevent, or detect and correct, errors or omissions in the information it provides to user entities. A service organization's controls are relevant to a user entity's internal control over financial reporting when they are part of the user entity's information and communication systems maintained by the service organization.

The service organizations addressed by AT section 801 are those that generate 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 (SOC 2SM reports) 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 section 801 is not applicable to such engagements.

However, AT section 101, *Attest Engagements* (AICPA, *Professional Standards*), may be used 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 has introduced a series of SOC reports. This series encompasses

- a. SOC 1 reports for engagements performed under AT section 801; 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 or the confidentiality or privacy of the information processed by that system; and
- c. SOC 3SM 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 A, "An Overview of SOC 1, 2, and 3 Reports."

Types of SOC 1 Reports

SOC 1 reports are intended to meet the needs of user 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 .07 of AT section 801 identifies and defines the two types of SOC 1 reports:

- ▶ *Type 1 report.* A report that contains (a) management's description of the service organization's system,² (b) management's written assertion about the fairness of the presentation of the description and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date, and (c) the service auditor's report. The service auditor's report contains the service auditor's opinion on
 - the fairness of the presentation of management's description of the service organization's system, and

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 section 801.

-
-
- the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

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 end of the period covered by the SOC 1 report, and the auditors of those user entities.

- ▶ *Type 2 report.* A report that contains (a) management's description of the service organization's system, (b) management's written assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period, (c) the service auditor's report, and (d) a description of the service auditor's tests of the operating effectiveness of controls and the results of those tests. The service auditor's report contains the service auditor's opinion on

- the fairness of the presentation of management's description of the service organization's system,
- the suitability of the design of the service organization's controls to achieve the related control objectives included in the description throughout a specified period, and
- the operating effectiveness of the service organization's controls to achieve the related control objectives included in the description throughout a specified period.

Use of a type 2 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 the auditors of those user entities.

Both type 1 and type 2 SOC 1 reports are intended to provide user auditors with information that will enable them to obtain an understanding of the entity, including its internal control, so that the user 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 user auditors with a description of the service auditor's tests of controls and results of those tests, which is intended to enable the user 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 User Entities

Paragraph .02 of AU-C section 402 states that many entities outsource aspects of their business activities to organizations that provide services ranging from performing a specific task under the direction of the entity to replacing entire business units or functions of the entity. Many of the services provided by such organizations are integral to the user entity's business operations; however, not all of those services are relevant to the audit of the user entity's financial statements. Examples of service organizations that provide services that may be relevant to the audit include payroll service providers, bank trust departments, mortgage servicers, insurance companies, call centers, medical claims processors, application service providers, and data centers.

AU-C section 315 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 the user entity uses a service organization to process transactions or perform other functions, questions may arise about how the user auditor should obtain the necessary understanding related to controls at the service organization. One way a user auditor may obtain this understanding is to obtain a SOC 1 report from the user entity, which is described in the section "Using a SOC 1 Report to Obtain an Understanding of the Services Provided to the User Entity" in chapter 3.

One of the objectives of this practice aid is to help user auditors determine how a SOC 1 report should be considered in an audit 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.* audit implications when a service organization uses a subservice organization.
- b.* determining whether a user auditor should obtain a SOC 1 report, if available, and whether a type 1 or type 2 report is applicable in the circumstances.
- c.* how to read and understand a SOC 1 report, including the procedures a user auditor may perform to
 - i.* determine whether the scope of the SOC 1 report is adequate for the purposes of a particular audit;
 - ii.* evaluate the results of tests of controls; and
 - iii.* respond to identified testing exceptions, and determine whether such exceptions represent deficiencies in the user entity's internal control.

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 guidance contained therein.

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 a user entity's use of a service organization affects an audit of the user entity's financial statements, this chapter presents a summary of the procedures the user 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 entity 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 .A6–.A11 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.

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

Understanding 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.
- ▶ 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

Paragraph .13 of AU-C section 315 requires the auditor to obtain an understanding of the entity's internal control relevant to the audit. 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. 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 relevant to the audit
 5. Monitoring of controls

Although most controls relevant to the audit are likely to relate to financial reporting, other controls also may be relevant to the audit, such as controls over the safeguarding of assets. Also, 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.

Paragraph .14 of AU-C section 315 states that when obtaining an understanding of controls that are relevant to the audit, the auditor should 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. Implementation of a control means that the control exists and that the entity is using it. 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.

AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), tells the user auditor how to apply AU-C section 315 and AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained* (AICPA, *Professional Standards*), when auditing the financial statements of an entity that uses a service organization. Paragraph .10 of AU-C 402 states, in part, that the user auditor should evaluate the design and confirm the implementation of 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 the user auditor is unable to obtain a sufficient understanding from the user entity of controls over the services provided by the service organization to assess risk for assertions in the user.

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 a user entity 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 user entity's internal control:

- ▶ *Control activities.* Paragraphs .A91–.A92 of AU-C section 315 state that control activities¹ are the policies and procedures that help ensure that management directives are carried out. Paragraphs .21–.22 of AU-C section 315 require the auditor to 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

.....
1. The terms *controls* and *control activities* are used interchangeably.

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. 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 .A84 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 statements 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 an Entity’s Use of IT

As indicated in paragraph .A53 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 to the further audit procedures the auditor performs to respond to assessed risk. In addition, when obtaining an understanding of internal control, it is important for the auditor to consider how an entity’s use of IT and manual procedures may affect controls relevant to the audit. As stated in paragraph .A54 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 an entity'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 an entity's risk of material misstatement, particularly if the entity itself does not possess the expertise necessary to undertake particular activities, or does not have adequate resources to properly implement a function in-house.



Chapter 3

Using the Services of a Service Organization

Many entities use service organizations to process certain transactions or perform other functions on behalf of the user entity. In these circumstances, the user entity's internal control may consist of the controls at the user entity 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 states that the user 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 its effect on the user entity'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 .A42 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 user auditor regarding the services provided by a service organization depend on the nature of the services, their significance to the user entity, and the relevance of those services to the audit (discussed in more detail later).

A user entity may use a service organization to perform a wide variety of services. Examples of service organizations and the services they provide include

- a. transfer agents that issue, transfer, redeem, and account for a fund's capital shares.
- b. payroll processors, that , prepare paychecks or make direct deposits, prepare payroll tax returns, withhold employee contributions, make payments to governmental entities and other third parties, and maintain the related records.
- c. claims processors that process claims for health insurers.

-
-
- d.* investment managers that execute investment transactions and maintain the related accountability.
 - e.* third-party pricing services that calculate prices for investments that are valued at fair value in situations in which there are no observable inputs.
 - f.* student loan administrators for a university.
 - g.* bank custodians responsible for maintaining investment securities and all related banking transactions.
 - h.* cash receipts processors that record cash and checks received, forward payments to the appropriate parties, and apply the payments to customer accounts. This may be performed via a lock box arrangement with a financial institution.
 - i.* fund underwriters , also known as *fund distributors*, that act as an agent or a principal that sells a fund's shares as a wholesaler through independent dealers or as a retailer through its own sales network.

Exhibit 3-1, "Considering a Service Organization in a Financial Statement Audit," provides an overview of the key questions that are important for the user auditor to consider when auditing the financial statements of an entity that uses a service organization.

Exhibit 3-1—Considering a Service Organization in a Financial Statement Audit

<p>1. Is the service provided by the service organization part of the user entity’s information system including the related business process relevant to financial reporting and communication?</p> <p style="text-align: center;">Yes</p>	<p>No</p> <hr style="width: 100%;"/>	<p>No action is necessary because the service organization is not considered part of the user entity’s information system. The guidance for user auditors in AU-C section 402, <i>Audit Considerations Relating to an Entity Using a Service Organization</i> (AICPA, <i>Professional Standards</i>), is not applicable.</p>
<p>2. Can the user entity provide the user auditor with information about the services provided by the service organization that is sufficient to identify and assess the risks of material misstatement?</p> <p style="text-align: center;">No</p>	<p>Yes</p> <hr style="width: 100%;"/>	<p>Obtain the necessary information from the user entity.</p>
<p>3. Does the service organization provide a SOC 1 report?</p> <p style="text-align: center;">No</p>	<p>Yes</p> <hr style="width: 100%;"/>	<p>Use the SOC 1 report to identify and assess risk.</p>
<p>4. Is the user auditor able to obtain the information necessary to identify and assess the risk of material misstatement by performing one or more of the following procedures:</p> <ul style="list-style-type: none"> • Contacting the service organization through the user entity to obtain specific information • Visiting the service organization and perform the procedures there to obtain the necessary information • Using another auditor to perform procedures at the service organization to obtain the necessary information <p style="text-align: center;">No</p>	<p>Yes</p> <hr style="width: 100%;"/>	<p>Use the information obtained to identify and assess risk.</p>
<p>Modify the user auditor’s opinion in accordance with AU-C section 705, <i>Modifications to the Opinion in the Independent Auditor’s Report</i> (AICPA, <i>Professional Standards</i>).</p>		

See chapter 1, “Introduction,” for a brief overview of SOC 1 reports. Chapters 3–5 provide a more detailed discussion of SOC 1 reports. The following sections discuss the flow-chart in exhibit 3-1.

Determining Whether the Service Organization Is Part of the User Entity’s Information System

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

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.

The following are some examples of services that service organizations may provide to user entities that would make the service organization's services part of the user entity's information system:

- ▶ Purchasing or selling investment securities by an investment adviser or investment manager who has been authorized to initiate transactions on behalf of the user entity without having to obtain authorization from the user entity prior to each transaction. Recording those transactions and providing user entities with a record of the activity in the account and value of the securities as of a specified date.
- ▶ Providing services that are ancillary to holding a user entity's securities, such as the following:
 - Collecting dividend and interest income and distributing that income to the user entity.
 - 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 user entity.
- ▶ Providing the price of exchange traded investment securities through paper documents or electronic downloads that the user entity uses to value its securities for transactions and financial statement reporting.
- ▶ Facilitating security lending transactions in which the service organization provides collateral to the user entity in exchange for the short-term use of certain securities.

When a service organization's services are part of a user entity's information system, the user auditor's understanding of the user entity's internal control may need to include controls placed in operation by the service organization as well as controls at the user entity.

The user 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 user entity's transactions that are specifically authorized by the user entity, such as the processing of checking account transactions by a bank, or the processing of securities

transactions by a broker (if the user entity retains responsibility for authorizing the transactions and maintaining the related accountability). In these circumstances, the user entity 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 user auditor should obtain an understanding of how the user entity 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 user entity, including their effect on the user entity'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 user entity
- ▶ The nature of the relationship between the user entity 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 user auditor's first source of information about the nature and significance of the services provided by the service organization and their effect on the user entity's internal control are (1) personnel at the user entity that would be in a position to have such knowledge, and (2) documentation that describes the services provided by the service organization. The following are examples of procedures the auditor performs to obtain such information:

- ▶ Reading user manuals or other systems documentation (for example, system overviews and technical manuals) about the services provided
- ▶ Reading reports of the service organization, its internal auditors, or regulatory authorities on the service organization's controls
- ▶ Inquiring of or observing personnel at the user entity or at the service organization

-
-
- ▶ Reading the contract or service level agreement between the user entity and the service organization

Knowledge obtained through the user auditor's experience with the service organization (for example, experience during prior audit engagements) may also be helpful when obtaining an understanding of the nature of the service provided by the service organization. This may be particularly helpful if those services and controls over those services are highly standardized.

As stated in paragraphs .A3–.A4 of AU-C section 402, a user entity may use a service organization, such as one that processes transactions and maintains the related accountability for the user entity, 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:

- ▶ Maintaining the user entity's accounting records
- ▶ Managing the user entity's assets
- ▶ Initiating, authorizing, recording, or processing transactions as an agent of the user entity

The Nature and Materiality of the Transactions

As stated in paragraph .A6 of AU-C section 402, a service organization may establish policies and procedures (controls) that affect the user entity's internal control. These controls are at least in part physically and operationally separate from the user entity. The significance of the controls at the service organization to the user entity'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 user entity. In certain situations, the transactions processed and the accounts affected by the service organization may not appear to be material to the user entity's financial statements, but the nature of the transactions processed may be significant and the user 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 user entity's internal control also depends on the degree of interaction between the service organization's activities and those of the user entity. The degree of interaction relates to the extent to which a user entity 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 user entity and those at the service organization is when the user entity authorizes transactions and the service organization processes and accounts for those transactions. In these circumstances, it may be practicable for the user entity 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 user entity, or initially records, processes, and accounts for the user entity's transactions, a lower degree of interaction exists between the user entity and the service organization. In these circumstances, the user entity may be unable to, or may elect not to, implement effective controls over these transactions at the user entity and may rely on controls at the service organization.

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

Nature of the Relationships

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

- ▶ The information to be provided to the user entity 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 user entity when the user entity 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 user auditor and the service auditor.

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

Procedures When the User Auditor Cannot Obtain a Sufficient Understanding from the User Entity

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

- a.* Obtain and read a type 1 or type 2 SOC 1 report, if available.
- b.* Contact the service organization, through the user entity, to obtain specific information.
- c.* Visit the service organization and perform procedures that will provide the necessary information about the relevant controls at the service organization.
- d.* Use another auditor to perform procedures at the service organization.

Using a SOC 1 Report to Obtain an Understanding of the Services Provided to the User Entity

A service organization may engage a service auditor to perform a type 1 or type 2 SOC 1 engagement under AT section 801, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*), with the objective of providing the resulting SOC 1 report to user entities. Exhibit 3-2, “Summary of Type 1 and Type 2 SOC 1 Reports,” describes the features of type 1 and type 2 SOC 1 reports.

Exhibit 3-2—Summary of Type 1 and Type 2 SOC 1 Reports

<i>Title</i>	<i>Contents</i>	<i>Relevance to User Auditors</i>
<p>Report on management’s description of a service organization’s system and the suitability of the design of controls (Type 1 SOC 1 report)</p>	<ul style="list-style-type: none"> • Management’s description of the service organization’s system. • Management’s written assertion about whether the description is fairly presented and whether the controls included in the description are suitably designed to achieve the related control objectives. • A report by the service auditor that includes the service auditor’s opinion on whether the description is fairly presented and the related controls are suitably designed to achieve the specified control objectives included in the description, as of a specified date. <p>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.</p>	<ul style="list-style-type: none"> • Assists the user auditor in obtaining a sufficient 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. Enables the service auditor to identify and assess risks of material misstatement for financial statement assertions affected by the service organization’s services.
<p>Report on management’s description of a service organization’s system and the suitability of the design and operating effectiveness of controls (Type 2 SOC 1 report)</p>	<ul style="list-style-type: none"> • Includes all of the elements of a type 1 SOC 1 report and also includes a description of the service auditor’s tests of controls and results of those tests. • In addition to the opinion expressed in a type 1 SOC 1 report, the service auditor expresses an opinion on whether the controls were operating effectively to achieve the related control objectives included in the description throughout a specified period. 	<ul style="list-style-type: none"> • Has the same utility as a type 1 SOC 1 report and also provides evidence about whether controls at the service organization were operating effectively to achieve the related control objectives included in the description. Such evidence should enable the user auditor to respond to assessed risk related to assertions in the user entity’s financial statements affected by the service organization’s services.

Evaluating a SOC 1 Report

If a user auditor intends to use a type 1 or type 2 SOC 1 report as audit evidence to support the user auditor’s risk assessment for financial statement assertions affected by the

service organization's services, the user auditor should determine whether the SOC 1 report provides sufficient appropriate audit evidence to support the user auditor's risk assessment by


- a.* evaluating whether the SOC 1 report addresses the services, functions, or applications that the user entity uses and that are relevant to the user entity's internal control over financial reporting;
- b.* evaluating whether the type 1 report is as of a date, or in the case of a type 2 report, for a period that is appropriate for the user auditor's purposes (see chapter 5, "How to Use a SOC 1 Report," for more detail);
- c.* evaluating the sufficiency and appropriateness of the evidence provided by the report for the user auditor's understanding of the user entity's internal control relevant to the audit; and
- d.* determining 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 user entity's financial statements and, if so, obtaining an understanding of whether the user entity 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 SOC 1 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 of 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 section 801 is intended for use by licensed CPAs. For a user auditor to use a SOC 1 report, it must be issued by a licensed CPA. User auditors may not use a report provided by an unlicensed individual or entity. It is important for user auditors to be alert to the possibility that a SOC 1 report may not have been prepared by a licensed CPA and, if the user auditor is unfamiliar with the organization, the user 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, the user auditor is 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.

A scope limitation may exist if the user auditor is unable to obtain sufficient appropriate audit evidence regarding the services provided by the service organization relevant to the audit of the user entity's financial statements. 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 user auditor's conclusion regarding whether the possible effects on the user entity'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, including the financial statements of entities that use a service organization:

- ▶ 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 section 801 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
- ▶ Maintaining custody of securities
- ▶ Hosting IT general controls and applications

When a subservice organization is used to process a user entity's transactions, the user auditor may need to obtain information about controls at the subservice organization that are relevant to the user entity's internal control over financial reporting. In situations in which one or more subservice organizations are used, the interaction between the activities of the user entity and those of the service organization is expanded to include the interaction between the user entity, 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 user auditor to consider in determining the significance of the service organization's and subservice organization's controls to the user entity's controls. It is important for the user auditor to evaluate the significance of the subservice organization to the user entity's financial statements audit.

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 user 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 user entity'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 work to be performed by the user auditor regarding the service provided by a subservice organization depend on the nature and significance of those services to the user entity and the relevance of those services to the audit. Because a user entity typically does not have any contractual relationship with the

subservice organization, the user entity 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 user 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 user entity management,
- b.* inquiry of the service organization,
- c.* reading the contract or service level agreement between the user entity and the service organization, and
- d.* reading user manuals and other documentation about the service organization's services.

Chapter 4

Responding to the Assessed Risks of Material Misstatement When the User Entity Uses a Service Organization

After the user 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 user 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 When a SOC 1 Report Is Not Available

Obtaining a SOC 1 report is not the only way for a user auditor to respond to assessed risks. The following paragraphs provide information about other procedures the user 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 accounting records of the user entity, direct access to those records may be necessary for the user 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 user auditor may also obtain evidence concerning the adequacy of the service organization's controls over the completeness and integrity of the user entity'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 user entity, the user auditor may consider performing the following procedures:

- ▶ *Inspecting records and documents held by the user entity.* The reliability of this source of evidence is determined by the nature and extent of the accounting records and supporting documentation retained by the user entity. In some cases, the user entity 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 user auditor's access to the records of the service organization may be established as part of the contractual arrangements between the user entity and the service organization. The user auditor may also use another auditor, on its behalf, to gain access to the user entity's records maintained by the service organization, or ask the service organization through the user entity for access to the user entity's records maintained by the service organization.
- ▶ *Obtaining confirmations of balances and transactions from the service organization.* When the user entity 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 user auditor may confirm balances with these organizations in order to compare this information with the user entity's independent records. If the user entity 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 user auditor may consider whether an alternative source of independent evidence can be identified.
- ▶ *Performing analytical procedures on the records maintained by the user entity 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 user entity outsources some or all of its finance functions to a service organization, the user 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 user auditor or the service auditor on behalf of the user auditor. A service auditor may provide a type 2 SOC 1 report and, in addition, may perform substantive procedures on behalf of the user 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 user auditor will need to read the entire SOC 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 user 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 user 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 user 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 user 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 user auditor to determine whether the report provides sufficient appropriate audit evidence about the operating effectiveness of the controls to support the user auditor's risk assessment by

- a.* evaluating whether the type 2 SOC 1 report is for a period that is appropriate for the user 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 user entity's financial statements and, if so, obtaining an understanding of whether the user entity 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 user entity's financial statements and provide sufficient appropriate audit evidence to support the user auditor's risk assessment.

When using a SOC 1 report, it is important for the user 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 user 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 suggests taking a *transaction- or process-oriented* approach to linking controls with the relevant financial statement assertions.

Under the transaction or process-oriented approach, the user auditor begins by identifying and describing the major transactions and processes of the user entity. These processes then are analyzed by mapping them to the financial statement accounts to which they relate and the relevant financial statement assertions.

Frequently Asked Questions—How a User Auditor Obtains a SOC 1 Report

Q. Who should the user auditor contact to obtain a service organization's SOC 1 report?

A. It is important for the user auditor to obtain the SOC 1 report from the user entity. Because service organizations may have more than one SOC 1 report, obtaining the SOC 1 report directly from the user entity ensures that the correct SOC 1 report is used in the audit of the user entity. 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 type 1 SOC 1 report, and the auditors of those user entities. 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 type 2 SOC 1 report, and the auditors of those user entities.



Chapter 5

How to Use a SOC 1 Report

This chapter describes some of the key considerations for an auditor of a user entity's financial statements when using a SOC 1 report, including determining the effect of that report on the audit of the user entity'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 User Entity 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 is a report on management's description of a service organization's system and the suitability of the design of controls. A type 2 SOC 1 report is a report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls.

Type 1 SOC 1 Reports

According to paragraph .07 of AT section 801, *Reporting on Controls at a Service Organization* (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, in all material respects, and based on suitable criteria,
 - i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented *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 service auditor's report that expresses an opinion on whether
 - 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.

As indicated in chapter 4, a type 1 or type 2 SOC 1 report may be used by the user auditor to obtain a sufficient understanding of controls at the service organization that are likely to be relevant to the user entity's internal control over financial reporting. 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, in all material respects, and based on suitable criteria,
 - i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented *throughout the specified period*;
 - 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 service auditor's report that expresses an opinion on whether
 - 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 were operating effectively to achieve those control objectives *throughout the specified period*.
- d. a description of the service auditor's tests of controls and the results of those tests.



Practice Pointer. AT section 801 requires that management provide a written assertion about the matters covered by the service auditor's opinion.

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 user 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 user 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 user entity'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 user entity'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 user auditor may perform additional procedures such as

- a. making inquiries of user entity personnel about any changes at the service organization. The user entity 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 user entity 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 user entity or after obtaining approval from the user entity 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 user entity'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 user entity's financial statements.

A type 2 SOC 1 report may cover a period that overlaps a portion of the user entity's reporting period. In determining the audit evidence that such a report can provide, it is important for the user 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 user entity's reporting period, an additional type 2 SOC 1 report covering the gap period may provide additional audit evidence.

The user 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 user 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 user entity

If the period covered by the type 2 SOC 1 report is completely outside the period under audit, the user 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 .15 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 user 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 user entity's financial statements, management of the user entity may consider requesting that the service organization have the service auditor perform the necessary testing.

The Service Auditor's Report

When reading a SOC 1 report, it is important for the user 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 financial statements of the user entity. 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 user 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 the controls that are relevant to the user entity's financial statements will assist the user auditor in determining the effect of the report on the audit of the user entity'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 user auditor to obtain information about the controls implemented at the service organization that are relevant to the user entity's internal control over financial reporting. Both type 1 and type 2 SOC 1 reports are intended to provide the user auditor with information necessary to assess risk for assertions in the user entity's financial statements affected by the service organization's services. However, only a type 2 report provides user auditors with a description of the service auditor's tests of controls and results of those tests, which is intended to enable the user 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 .14 of AT section 801:


- ▶ 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 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 contemplated 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 user auditor should determine that the information provided contains sufficient detail to enable the user 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 user entities internal control. The degree of detail in the description would be expected to be equivalent to the degree of detail the user 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.

 **Practice Pointer.** One of the changes required by AT section 801 is that the description of the service organization’s system in a type 2 SOC 1 report covers a period—the same period as the period covered by the service auditor’s tests of the operating effectiveness of controls.

Control Objectives, Related Controls, and Assertions

Management's description of the service organization's system should include a discussion of the service organization's control objectives and related controls. In forming his or her opinion on the suitability of the design of controls, the service auditor determines which of the controls at the service organization are necessary to achieve the control objectives stated in management's description of the service organization's system and whether those controls were suitably designed to achieve the control objectives by

- a.* identifying the risks that threaten the achievement of the control objectives stated in management's description of the service organization's system, and
- b.* evaluating the linkage of the controls identified in management's description of the service organization's system with those risks.

In reading the service auditor's SOC 1 report as well as the description of the service organization's system, the user auditor determines the scope of the engagement covered by the report and whether that scope corresponds with the service, system(s), or aspects of the system used by the user entity. 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 needs of the user auditor. To be adequate for the user auditor's purposes, the service auditor's report and the description should address

- a.* all significant transactions processed by the service organization for the user entity that affect the user entity'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 previously discussed, when a user entity uses a service organization to process transactions, the user entity's internal control consists of both

- a.* controls at the service organization that are relevant to the user entity's internal control over financial reporting and
- b.* controls implemented by the user entity.

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 user 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 user entity's financial statements and, if so, should obtain an understanding of whether the user entity has designed and implemented such controls. An example of a complementary user entity control is a control over passwords used by specified user entity 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 user auditor to determine whether the complementary user entity controls identified in the SOC 1 report have been suitably designed and implemented at the user entity. If the user auditor intends to use a type 2 SOC 1 report to obtain evidence of the operating effectiveness of controls at the service organization, the user auditor should also test the operating effectiveness of the relevant complementary user entity controls.

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

Tests of the Operating Effectiveness of Controls

After the user auditor has assessed risks for assertions in the user entity's financial statements that are affected by the service organization's services, the user 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 user auditor

If the user auditor has obtained a type 2 SOC 1 report, the user 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 user entity’s financial statements for which the user auditor intends to rely on the operating effectiveness of controls at the service organization? (To make this determination, the user 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 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 user entity. 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 user auditor relating to how this information affects the audit of the user entity’s financial statements.

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

<i>Required Elements in the Description of the Service Auditor’s Test of Controls</i>	<i>Control Objective</i>	<i>Control Policy or Procedure</i>	<i>Description of the Tests of Controls Performed by the Service Auditor</i>	<i>Results of the Tests</i>
Information Provided By the Service Auditor	Security purchase and sale transactions are recorded at the appropriate amounts and in the appropriate periods.	Reconciliations of trade activity processed on the trading system to settled cash are performed daily. Reconciling items are researched and resolved.	Inspected a sample of XX daily reconciliations covering the audit period to determine whether they were reconciled and whether reconciling items were researched and resolved in a timely manner.	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 the reconciliations for April, May and June 20XX ² contained items that were not resolved in a timely manner.

1. Paragraph 520(ii) of AT section 801, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*), indicates that if deviations have been identified in the operation of controls included in the description, the description should include the extent of testing performed by the service auditor that led to the identification of the deviations (including the number of items tested), and the number and nature of the deviations noted (even if, on the basis of tests performed, the service auditor concludes that the related control objective was achieved).

2. See footnote 1.

<i>Required Elements in the Description of the Service Auditor's Test of Controls</i>	<i>Control Objective</i>	<i>Control Policy or Procedure</i>	<i>Description of the Tests of Controls Performed by the Service Auditor</i>	<i>Results of the Tests</i>
User Auditor's Considerations	Does the control objective have a direct relationship to the user entity's financial statement assertion? If so, which ones?		Is the description of the tests sufficient to determine the nature, timing, and extent of the tests performed by the service auditor? Does the nature, timing, and extent of the service auditor's tests provide sufficient appropriate audit evidence about the operating effectiveness of the control?	Do the results of the tests support the user auditor's risk assessment? Can the user 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 user auditor is using a type 2 SOC 1 report that states that controls over payroll processing 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 user 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 user auditor also should

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

If a user 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 a 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 user auditor to

- a. evaluate the condition;
- b. determine how it affects his or her ability to obtain an understanding of the user entity's internal control;
- c. determine how it affects the user 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 User Auditor

As discussed in chapter 4, “Assessing and Responding to Risks of Material Misstatement When the User Entity 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 user 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 user entity’s internal control over financial reporting. The following sections are designed to provide the user 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 user 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 user auditor from gaining the knowledge needed to obtain an understanding of the user entity’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 user entity)
- ▶ 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 user entity’s balance sheet (for example, the as of date for the description of the service organization’s system does not coincide with the user entity’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 user entity’s financial statements (for example, the period covered by the service auditor’s tests of controls does not coincide with the user entity’s reporting period)

If the SOC 1 report does not provide the user auditor with the necessary information to assess risk for assertions in the user entity's financial statements affected by the service organization's services and the user auditor is unable to obtain that information from the user entity 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 user auditor will need to

- a. contact the service organization, through the user entity, to obtain specific information;
- b. request that a service auditor be engaged to perform procedures that will supply the necessary information; and
- c. visit the service organization and perform procedures.

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

Deviations in the Results of Tests

Paragraph .A39 of AU-C section 402 indicates that a service auditor's type 2 SOC 1 report identifies the results of tests, including deviations, and other information that could affect the user auditor's conclusions. Deviations in tests of controls noted by the service auditor or a modified opinion in the service auditor's report do not automatically mean that the service auditor's report will not be useful in assessing the risks of material misstatement in an audit of the user entity's financial statements. Rather, the deviations and the matter giving rise to a modified opinion in the service auditor's type 2 SOC 1 report are considered in the user 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 user auditor may discuss such matters with the service auditor. Such communication is dependent upon the user entity 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; deviations may be identified in either type of control. The following list provides 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, including the following:
 - 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 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, including the following:
 - Changes are not approved by designated individuals or 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 deviations in non-IT controls:

- ▶ Improper set-up of an employee
- ▶ Inaccurate processing of payroll information
- ▶ Inaccurate computation of withholding for employees
- ▶ Employee data changes, such as employee salary, processed without proper authorization

The following is an example of how the service auditor would describe 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 trust system and recordkeeping system was not performed timely.

When evaluating the significance of exceptions or deviations, the user auditor needs 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 user 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 user auditor to consider the following questions:
- Which accounts or assertions in the user entity’s financial statements could be misstated if the control failed and there were no other controls in place to prevent or detect a misstatement?
 - How significant would the misstatement be to the user entity’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 user entity’s financial statements could occur?
 - Does the user entity 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 if the response had a mitigating effect on the exception(s), did the service auditor test management’s response?
 - Has the service organization provided additional information that could be considered by the user 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 user entity’s financial statements, and the likelihood of a misstatement happening, are the 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 employees to confirm their retirement account balance 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 user entity's year-end).

If the user 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 user auditor from doing so.

Paragraph .20 of AU-C section 402 states that the user auditor should modify the opinion in the 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 user auditor is unable to obtain sufficient appropriate audit evidence regarding the service provided by the service organization relevant to the audit of the user entity's financial statements.

Finally, it is important for the user 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 user entity's internal control over financial reporting that should be communicated to management and those charged with governance of the user entity. Paragraph .A40 of AU-C section 402 states that the user 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 user 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 user entity:

- ▶ The user entity has not implemented monitoring controls that are needed to mitigate the effect of deficiencies in the service organization's controls.
- ▶ The user entity has not implemented the complementary user entity controls identified in the SOC 1 report.
- ▶ Controls that are needed for the user entity's internal control to be suitably designed and operating effectively do not appear to have been implemented by the service organization or were implemented, but are not operating effectively.

In addition to communicating significant deficiencies and material weaknesses to management of the user entity or those charged with governance, the user auditor is not precluded

from communicating other matters or recommendations, related to the use of the service organization.

Common User Auditor Issues Related to SOC 1 Reports

SOC 1 Report Does Not Address All of the Services Provided By the Service Organization

A service organization may provide multiple services but may not provide a SOC 1 report for all of those services. For that reason, it is particularly important for the user auditor to determine which services are covered by a particular report.

For services that are not covered by the SOC 1 report and for which the user auditor is unable to obtain a sufficient understanding, from the user entity, of the nature and significance of the services provided by the service organization and their effect on the user entity's internal control, paragraph .12 of AU-C section 402 requires the user auditor to obtain that understanding from one or more of the following procedures:

- ▶ Contacting the service organization, through the user entity, 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 that will provide the necessary information about the relevant controls at the service organization

Period Covered by the SOC 1 Type 2 Report is Not Sufficient for the User Auditor's Purposes

The period addressed by a type 2 SOC 1 report usually will not be identical to the financial statement period of the user entity. When the periods are not identical, the user auditor should consider whether the report provides sufficient appropriate evidence to reduce audit risk to an appropriate level. In many instances in which the period addressed by the SOC 1 report and the financial statement audit period differ, the difference in periods is sufficiently small, therefore the user auditor may be able to reduce audit risk to an appropriate level by testing only user entity controls, if such controls exist. In evaluating whether the difference in the periods, it is important for the user auditor to consider AT section 801, which indicates that a type 2 SOC 1 report that covers a period that is less than six months is unlikely to be useful to user entities and their auditors. However, the

user auditor may determine that a report covering more than six months is necessary to reduce audit risk to an appropriate level. If the user auditor concludes that the period of coverage is insufficient, and sufficient additional evidence is not available from the user entity, the user 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 user auditor, management of the user entity may consider requesting that the service organization obtain an additional type 2 SOC 1 report that addresses the portion of the financial statement period that is not covered by the initial report.
- ▶ visiting the service organization and performing procedures.
- ▶ using another auditor to perform the additional procedures in an examination engagement or agreed-upon procedures engagement performed in accordance with the attestation standards.

An Inclusive Subservice Organization's Assertion Does Not Address all of the Minimum Criteria

Paragraph .14 of AT section 801 instructs the service auditor to determine whether the criteria used by management to prepare its description include, at a minimum, the matters listed in paragraph .14. All of the criteria in paragraph .14 are to be used for all descriptions, unless specified criteria are not applicable. When a SOC 1 report is prepared using the inclusive method, the included subservice organization is responsible only for that portion of the description and controls related to the subservice organization's services. That responsibility will vary by the nature of the service provided to the service organization, as well as the effect of those services on the user entities. For example, a subservice organization would be responsible for the fairness of the presentation of the description of the services it provides to the service organization and for the operating effectiveness of controls designed by the service organization. In these instances, the description will include the design of the controls at the subservice organization. However, the criteria in the subservice organization's assertion will not address the suitability of the design of the controls; the criteria in the service organization's assertion will address the suitability of the design of the controls and the service organization will take responsibility for the design of those controls in its assertion. On the other hand, a subservice organization providing IT outsourcing services may include all the criteria in paragraph .14 in its assertion because it provides its own description of the services it provides, specifies its own control objectives, identifies the risks that threaten the achievement of those control objectives, and designs and operates the controls addressing those risks.

The SOC 1 Report Carves Out Subservice Organizations

The service organization may elect to carve out from its description, and from the engagement, controls at the subservice organization that are necessary for the service organization to achieve its control objectives. In these situations, the user auditor may be able to obtain a SOC 1 report from the subservice organizations. Paragraph .A64 of AT section 801 indicates that if the service provided by the subservice organization is relevant to a user entity's internal control over financial reporting, the user entity and, by analogy, the user auditor are intended users of the subservice organization's SOC 1 report. In certain situations, a SOC 1 report for a subservice organization may not be available to the user auditor. In those circumstances, the user auditor determines whether the user entity has implemented effective controls over the services provided by the subservice organization, in which case the user auditor would not need to obtain evidence about the operating effectiveness of relevant controls at the subservice organization.

For example, a service organization may use a subservice organization to provide securities pricing information, but the user entity compares prices reported by the service organization to prices obtained from a separate service. In such a situation, the user entity is not dependent on controls at the subservice organization to obtain accurate securities pricing information because it has implemented its own controls to achieve that control objective.

If the user auditor determines that the user entity has not implemented controls over the services provided by the subservice organization, and those services are relevant to the user entity's internal control over financial reporting, the user auditor should apply the guidance in paragraph .15 of AT section 801. If the user auditor is unable to obtain additional evidence, the user auditor considers the effect of this limitation on his or her opinion of the user entity's financial statements.

Service Auditor Expresses a Qualified Opinion Because of Deviations Identified in Tests of Controls

Deviations identified by the service auditor, or a modified opinion in the service auditor's report, do not automatically mean that the service auditor's report will not be useful to the user auditor in assessing the risks of material misstatement. Rather, the user auditor uses that information to determine the effect of the service organization's controls that were not operating effectively, if any, on the user entity's financial statements as a basis for assessing risk.

User Auditor Determines the Type 1 or Type 2 Report is Not Sufficient for His or Her Needs

Generally, a SOC 1 report is intended to meet the common needs of a broad range of user entities. However, the needs of each user entity may differ. When reading a SOC 1 report, it is important for a user auditor to consider whether the description of the service organization's system includes enough detail to address the particular facts and circumstances of the user entity's internal control and whether the controls tested in the SOC 1 report address all of the relevant risks of material misstatement of the user entity's financial statements. For example, materiality for a user entity experiencing large operating losses may be significantly below materiality for the broad range of user entities. As a result, a certain class of transactions that is immaterial for the broad range of user entities may be material for the particular user entity. In this situation, the SOC 1 report might not cover that specific class of transactions. For example, amounts generated by a service organization that serves as a third-party administrator for employee benefit plans may be immaterial for a broad range of user entities, but material for a smaller entity.

Service Auditor Expresses a Qualified Opinion Regarding the Design or Operating Effectiveness of Controls

If the service auditor has identified deficiencies in the design or operating effectiveness of controls at the service organization that prevent the service organization from achieving its controls objectives, it is important for the user auditor to consider the effect of those deficiencies on the user entity's financial statements. In certain situations, the deficiencies may not be relevant to the user entity's financial statements. For example, if the service auditor identifies deficiencies at a custodian related to investment valuation services, they may not be relevant to a particular user entity because the user entity uses an independent service organization for asset valuation services.

In considering the deviations and matters giving rise to a modified opinion in the service auditor's report, the user auditor may contact the service auditor through the user entity to discuss the particular facts leading to the modification of the opinion.

When the deficiencies are relevant to the user entity, the user auditor may be able to identify controls at the user entity that address the specific risks related to those deficiencies. If the user auditor is unable to obtain sufficient appropriate evidence regarding the user entity's financial statement assertion, the user auditor should modify the opinion on the financial statement in accordance with AU-C section 705.

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

An Overview of SOC 1, 2, and 3 Reports

AT section 801, *Reporting on Controls at a Service Organization* (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 user entities' customers. 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 section 801 and the AICPA Guide *Service Organizations: Reporting on 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, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*)

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

	<i>SOC 1 Engagements</i>	<i>SOC 2 Engagements</i>	<i>SOC 3 Engagements</i>
Under what professional standard is the engagement performed?	AT section 801, <i>Reporting on Controls at a Service Organization</i> (AICPA, <i>Professional Standards</i>). Other resource: The AICPA Guide <i>Service Organizations: Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting</i> .	AT section 101, <i>Attest Engagements</i> (AICPA, <i>Professional Standards</i>). Other resource: The AICPA Guide <i>Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)</i> .	AT section 101. Other resource: TSP section 100, <i>Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy</i> (AICPA, <i>Technical Practice Aids</i>), provides the criteria for evaluating the design and operating effectiveness of controls in these engagements, as well as the criteria for the content of a privacy notice.
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. If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices.	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. If the report addresses the privacy principle, the service organization's compliance with the commitments in its privacy notice. ¹

1. Entities that collect personal information generally establish and document their policies regarding the nature of the information they collect and how that information will be used, retained, disclosed, and disposed of or anonymized. These policies and the entity's commitment to adhere to them when included in a written communication to individuals about whom personal information is collected (sometimes referred to as *data subjects*) are referred to as a *privacy notice*. A privacy notice also includes information about such matters as the purpose of collecting the information; the choices individuals have related to their personal information; the security of such information; and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

When a service organization is involved in any of the phases of the personal information life cycle, it may or may not be responsible for providing a privacy notice to the individuals about whom information is collected. If the user entity is responsible for providing the privacy notice, the service organization provides a statement of privacy practices to the user entities that includes the same types of policies and commitments as would be included in a privacy notice, but the statement is written from the perspective of the service organization communicating its privacy-related policies and commitments to the user entities. The statement of privacy practices provides a basis for the user entities to prepare a privacy notice to be sent to individuals or for ensuring that the service organization has appropriate practices for meeting the existing privacy commitments of user entities.

	<i>SOC 1 Engagements</i>	<i>SOC 2 Engagements</i>	<i>SOC 3 Engagements</i>
What is the purpose of the report?	To provide the auditor of a user entity's financial statements with information and a CPA's opinion about controls at a service organization that may be relevant to a user entity's internal control over financial reporting. It enables the user 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 CPA's opinion about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy. A type 2 report that addresses the privacy principle also provides information and a CPA's opinion about the service organization's compliance with the commitments in its statement of privacy practices.	To provide interested parties with a CPA's opinion about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy. A report that addresses the privacy principle also provides a CPA's opinion about the service organization's compliance with the commitments in its privacy notice.
What are the components of the report?	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 achieving the specified control objectives. 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 achieve specified control objectives; and in a type 2 report, the operating effectiveness of those controls.	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. If the report addresses the privacy principle, the assertion also covers the service organization's compliance with the commitments in its statement of privacy practices. A service auditor's report that contains an opinion on the fairness of the presentation of the description of the service organization's system;	A description of the system and its boundaries ² 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 and, if the report addresses the privacy principle, compliance with the commitments in the service organization's privacy notice.

(continued)

2. 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.

	<i>SOC 1 Engagements</i>	<i>SOC 2 Engagements</i>	<i>SOC 3 Engagements</i>
	In a type 2 report, a description of the service auditor's tests of the controls and the results of the tests.	<p>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.</p> <p>If the report addresses the privacy principle, the service auditor's opinion on whether the service organization complied with the commitments in its statement of privacy practices.</p> <p>In a type 2 report, a description of the service auditor's tests of controls and the results of the tests.</p> <p>In a type 2 report that addresses the privacy principle, a description of the service auditor's tests of the service organization's compliance with the commitments in its statement of privacy practices and the results of those tests.</p>	<p>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.</p> <p>If the report addresses the privacy principle, the service auditor's opinion on whether the service organization complied with the commitments in its privacy notice.</p>
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.	<p>Management of the service organization and other specified parties who have sufficient knowledge and understanding of the following:</p> <ul style="list-style-type: none"> • 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. 	Anyone.

SOC 1 Engagements

SOC 2 Engagements

SOC 3 Engagements

- 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.





Using a SOC 1SM Report in a Financial Statement Audit

ISBN 978-1-94023-529-5



9 781940 235295

APASSAE13P