2005

SAS no. 70 reports and employee benefit plans; Statement on auditing standards, 021

Michael J. Ramos
Linda C. Delahanty

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

Part of the Accounting Commons, and the Taxation Commons

Recommended Citation
Ramos, Michael J. and Delahanty, Linda C., "SAS no. 70 reports and employee benefit plans; Statement on auditing standards, 021" (2005). Statements on Auditing Standards. 3.
https://egrove.olemiss.edu/aicpa_sas/3

This Article 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 Statements on Auditing Standards by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.
SAS No. 70 Reports and Employee Benefit Plans
SAS No. 70 Reports and Employee Benefit Plans

Written by Michael Ramos
Edited by Linda Delahanty
Technical Manager Accounting and Auditing Publications
Notice to Readers

This publication, SAS No. 70 Reports and Employee Benefit Plans, is a Practice Aid that provides guidance to CPAs about the use of SAS No. 70 reports in the audits of employee benefit plans. This publication is not intended to provide guidance to public accounting firms registered with the Public Company Accounting Oversight Board (PCAOB) and their associated persons in connection with their audits of issuers as defined by the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley), and other entities when prescribed by the rules of the Securities and Exchange Commission (SEC). Publicly held companies and other issuers are subject to the provisions of Sarbanes-Oxley and the related SEC regulations that implement this legislation. Their outside auditors are also subject to the provisions of Sarbanes-Oxley and to the rules and standards issued by the PCAOB. Generally, plans that are required to file Form 11-K would be considered issuers.

This Practice Aid is an Other Auditing Publication as defined in Statement on Auditing Standards (SAS) No. 95, Generally Accepted Auditing Standards (AICPA, Professional Standards, vol. 1, AU sec. 150). Other Auditing Publications have no authoritative status; however, they may help the accountant understand and apply the SAS.

If you apply the guidance included in an Other Auditing Publication, you should be satisfied that, in your judgment, it is both appropriate and relevant to the circumstances of your audit. 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 a senior technical committee of the AICPA.
Acknowledgments

In response to continued questions about the use of SAS No. 70 reports, the 2004 AICPA National Conference on Employee Benefit Plans featured a presentation on the topic. The speakers are experts in the review of SAS No. 70 reports in conjunction with an audit performed in accordance with generally accepted auditing standards (GAAS), and over the course of their careers have addressed many of the issues that confront auditors of employee benefit plans. The enthusiastic response to the conference presentation inspired Linda Delahanty, of the AICPA’s publication team, to suggest the writing of this book. Linda championed the project and later edited the manuscript.

The conference presentation, together with the questions submitted by the participants during the conference, provided a solid foundation for the preparation of these materials. To build on this foundation, we relied on the guidance contained in:

- AICPA Audit Guide *Employee Benefit Plans*
- AICPA Audit Guide *Service Organizations: Applying SAS No. 70, As Amended*

We are indebted to all those who contributed to this publication and those who contributed to the development of the authoritative literature.
# Table of Contents

**Purpose of This Publication** ......................................................................................................... vii
**How This Publication Is Organized** ............................................................................................ viii

## Chapter 1: A Brief Review of SAS No. 55
- Sufficient to Plan the Audit ........................................................................................................... 2
- Reducing Control Risk Below the Maximum ................................................................................... 2
- Control Activities and the Accounting Information System ............................................................. 3

## Chapter 2: Use of a Service Organization
- Determining Whether the Service Organization Is Part of the Plan’s Information System ............. 7
- Obtaining Necessary Information Without a SAS No. 70 Report .................................................... 9
- The Service Organization and SAS No. 70 Reports ........................................................................ 11
- Subservicing .................................................................................................................................... 11
- When the Necessary Information Is Not Available ........................................................................ 12
- Frequently Asked Questions—SAS No. 70 Applicability ................................................................. 12

## Chapter 3: Audit Planning When the Plan Uses a Service Organization
- SAS No. 70 Planning Checklist ....................................................................................................... 16
- Obtaining the Information Necessary to Complete the Planning Checklist ......................................... 16
- SAS No.70 Considerations in the Planning of a Limited-Scope Audit ............................................... 16
- Frequently Asked Questions—Audit Planning .................................................................................. 17

## Chapter 4: How to Review a SAS No. 70 Report
- The Service Auditor’s Report .......................................................................................................... 19
  - Timing Considerations ................................................................................................................... 20
- Description of the Service Organization’s Controls .......................................................................... 21
- Control Objectives, Related Controls, and Assertions ...................................................................... 23
- Complementary User Organization Controls .................................................................................... 23
- Tests of Operating Effectiveness ........................................................................................................ 24
- Frequently Asked Questions—Reviewing SAS No. 70 Report .......................................................... 26
Chapter 5: Responding to Testing Exceptions, Control Deficiencies, or SAS No. 70 Report Inadequacies ............................................ 27

Instances of Noncompliance .................................................................................................................. 28

Glossary .......................................................................................................................... 31

Practice Aids .................................................................................................................. 33

Audit Program: Considering Service Organization Controls .......................................................... 34

SAS No. 70 Planning Checklist ................................................................................................... 37

SAS No. 70 Report Review Checklist ...................................................................................... 39

Appendix A: Excerpts From Audit And Accounting Guide Employee Benefit Plans ........ 45

Appendix B: Illustrative Control Objectives for Various Service Organizations ............ 53
Purpose of This Publication

It is common for an employee benefit plan administrator to use a third-party administrator or service organization to process certain transactions on behalf of the plan. These third parties may include bank trustees, custodians, insurance companies, or contract administrators.

In any audit, the auditor is required to obtain a sufficient understanding of internal control necessary to plan the audit. When the audited entity uses a service organization to process transactions, issues may arise relating to how the auditor is to obtain the necessary understanding of internal controls located at the service organization. In these situations, it is common for the auditor to obtain a service auditor’s report or SAS No. 70 report, based on Statement on Auditing Standards (SAS) No. 70, Service Organizations (AICPA, Professional Standards, vol. 1, AU sec. 324), as amended, that describes the service organization’s internal control.

In practice, auditors of employee benefit plans have continued to raise questions about how SAS No. 70 reports should be considered in their audits and which auditing procedures should be applied to these reports to increase their reliability as audit evidence.

This publication is written to help auditors of employee benefit plans. Its purpose is to provide guidance on the use of SAS No. 70 reports in your audits performed in accordance with generally accepted auditing standards (GAAS). Specifically, this publication is designed to address issues relating to:

• The circumstances under which a SAS No. 70 report should be obtained, including when each of the two different types of reports is appropriate
• How SAS No. 70 reports should be considered in a limited-scope audit
• The implications of subservice arrangements
• How to read and understand how a SAS No. 70 report affects your audit, including:
  — The procedures you should perform to understand the scope of the service auditor’s work and whether that scope is adequate for your purpose
  — The procedures you should perform to evaluate the results of tests of controls

1 This publication is not intended to provide guidance to public accounting firms registered with the Public Company Accounting Oversight Board (PCAOB) and their associated persons in connection with their audits of issuers as defined by the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley), and other entities when prescribed by the rules of the Securities and Exchange Commission (SEC). Generally, plans that are required to file Form 11-K would be considered issuers.
• How to develop an appropriate audit response for identified testing exceptions and control deficiencies

Paragraphs 6.04 through 6.17 of the AICPA Audit and Accounting Guide *Employee Benefit Plans*, with conforming changes as of March 1, 2005, (the EBP Guide) provide authoritative guidance on how the plan’s use of a service organization affects your audit. For your convenience, those paragraphs have been reproduced as Appendix A, “Excerpts From Audit and Accounting Guide *Employee Benefit Plans*,” to this publication. Additionally, the AICPA has published the Audit Guide *Service Organizations: Applying SAS No. 70, As Amended*, which provides detailed guidance for auditors on the use of SAS No. 70 reports.

This publication also includes several forms and checklists you may use to implement the suggestions provided.

**HOW THIS PUBLICATION IS ORGANIZED**

This publication considers SAS No. 70 reports within the context of the entire audit engagement. Thus, after a brief introduction summarizing the auditor’s overall requirements for obtaining an understanding of internal control, the publication describes how the auditor considers the SAS No. 70 report when:

• Planning the audit

• Obtaining an understanding of internal control

• Obtaining audit evidence to support an assessment of control risk below the maximum (if that is the audit strategy)

• Planning and performing further audit procedures in response to the audit evidence obtained from the SAS No. 70 report
Before considering how an employee benefit plan’s use of a service organization will affect your audit, it is helpful to review some of the key requirements relating to your understanding of internal control in a financial statement audit.

Statement on Auditing Standards (SAS) No. 55, *Consideration of Internal Control in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 319), as amended, provides the definitive guidance on your consideration of the plan’s internal control in an audit of their financial statements. AU Section 319.25 of the standard describes your overall responsibility for obtaining an understanding of internal control.

In *all audits*, the auditor should obtain an understanding of *each of the five components* of internal control sufficient to plan the audit. A sufficient understanding is obtained by performing procedures to understand the design of internal controls relevant to an audit of financial statements and determining whether they have been placed in operation. *Emphasis added*

In reviewing the requirements, note that:

• You should apply these requirements to all audits, even those for which you plan to assess control risk at the maximum and perform a completely substantive audit.

• You are required to obtain an understanding of each of the five components of internal control, as defined by the internal control framework of COSO, the Committee of Sponsoring Organizations of the Treadway Commission, the National Commission of Fraudulent Financial Reporting (sponsored jointly by the AICPA, the American Accounting Association, Financial Executives Institute, Institute of Internal Auditors, and Institute of Management Accountants) and SAS No. 55. These components are:
  
  — The control environment
  — Risk assessment
  — Control activities
  — Information and communication
  — Monitoring

• You are required to understand the design of internal control. Generally, internal control design encompasses considerations such as:

  — The types of financial statement misstatement that could occur and how these relate to the relevant assertions of individual financial statement accounts, e.g., What could go wrong?
— Control objectives and the individual control procedures that address potential misstate-
ments
— How accounting data and information is captured, recorded, processed, and included in the
financial statements; and the points in this process at which errors could be introduced

• On all audits, you are required to determine whether controls have been “placed in operation,”
  which means that the entity “is using them.”

When obtaining your understanding of internal control, you also consider how the plan’s use of
information technology (IT) and manual procedures may affect controls relevant to the audit.

SUFFICIENT TO PLAN THE AUDIT

Your overall requirements to understand internal control are placed in the context of audit plan-
ing. In planning your audit, your knowledge of internal control should be adequate to allow you to:

• Identify types of potential misstatements.
• Consider factors that affect the risk of material misstatement.
• Design substantive tests.

REDUCING CONTROL RISK BELOW THE MAXIMUM

For some audits, you may choose or be required to assess control risk below the maximum. For
example:

• You may determine that assessing control risk below the maximum for certain assertions may
  be more effective and more efficient than performing a purely substantive audit, or

• In situations in which a significant amount of information supporting one or more financial
  statement assertions is electronically initiated, recorded, processed, or reported, you may de-
termine that it is not possible to design effective substantive tests that, by themselves, would
provide sufficient evidence that the assertions are not materially misstated. For example, if all
information relating to plan participant contributions or the allocation of income was captured,
stored, and processed automatically, it may not be possible to come to a conclusion about the
financial statements without testing the operating effectiveness of relevant controls.

To assess control risk below the maximum level, you will need to perform procedures that go
beyond those necessary to plan the audit. Specifically, you will be required to:
• Identify specific controls relevant to specific assertions.

• Perform tests of controls to determine the effectiveness of the controls.

• Conclude on the assessed level of control risk.

**CONTROL ACTIVITIES AND THE ACCOUNTING INFORMATION SYSTEM**

When a plan uses a service organization to process certain transactions, that service organization will have the most direct effect on two components of internal control, namely, control activities and the accounting information system, which is a part of the information and communication component:

• **Control Activities.** On all audits, you should obtain an understanding of those control activities relevant to planning the audit. This understanding includes an understanding of how IT affects control activities that are relevant to planning the audit. *Ordinarily*, audit planning does not require you to obtain an understanding of the control activities related to each account balance and every relevant assertion. Normally, your understanding of control activities is limited to obtaining an understanding of control activities for the most significant accounts and assertions. However, you will need to obtain an understanding and then test controls related to the specific assertions for which you will assess control risk below the maximum.

• **Information System.** SAS No. 55, AU Section 319.49, requires you to obtain sufficient knowledge of the accounting information system to understand:

  — The classes of transactions in the plan’s operations that are significant to the financial statements

  — The procedures, both automated and manual, by which transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements

  — The related accounting records, whether electronic or manual, supporting information, and specific accounts in the financial statements involved in initiating, recording, processing, and reporting transactions

  — How the information system captures other events and conditions 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
CHAPTER 2: USE OF A SERVICE ORGANIZATION

When an entity uses a third-party service organization to process a number of its transactions, a portion of that entity’s internal control resides outside the entity. The procedures that auditors perform to satisfy the requirements of SAS No. 55, *Consideration of Internal Control in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 319), as amended, must be designed to take this fact into account.

An employee benefit plan may use a service organization to perform a wide variety of services related to its financial reporting. These services may include acting as a:

• Recordkeeper for participant accounts, which includes processing participant-level activity and maintaining their accounts

• Trustee or custodian, which includes maintaining custody of plan investment assets; reporting of income, prices, and investment shares; executing trades; and preparing checks

• Payroll provider, which includes processing payroll, withholding employee contributions, and maintaining related records

• Claims processor, which includes processing claims for health and welfare benefit plans

When a plan uses a service organization to process its transactions, those transactions are subject to the service organization’s controls. This situation raises the issue of the nature and extent of understanding you should obtain about the controls in place at the service organization. Exhibit 2-1, “Considering a Service Organization,” provides an overview of the key questions you should consider when a client uses a service organization.
Exhibit 2-1 Considering a Service Organization

Is the service organization part of the plan’s information system?

- Yes
- No

Can you obtain the necessary information about internal control without a SAS No. 70 report?

- Yes
- No

Does the service entity provide a SAS No. 70 report?

- Yes
- No

Either:
- Perform the procedures at service organization, or
- Modify auditor’s report.

SAS No. 70 does not apply. Information about service organization controls is not necessary to plan and perform the audit.

Obtain information necessary to plan and perform the audit.

Use SAS No. 70 report to plan and perform the audit.

The following pages discuss this flowchart in more detail.
Determining Whether the Service Organization Is Part of the Plan’s Information System

An entity’s use of a service organization in some capacity does not, in and of itself, compel you to obtain a SAS No. 70 report to plan the audit. The first step in assessing whether a SAS No. 70 report is necessary is to determine whether the service organization is part of the plan’s information system. When a service organization is part of the plan’s information system, your understanding of controls may include the controls placed in operation by the service organization as well as those at the plan administrator.

Paragraph 6.04 of the EBP Guide states that a service organization’s services are part of a plan’s information system if they affect any of the following:

- The classes of transactions in the plan’s operations that are significant to the plan’s financial statements
- The procedures, both automated and manual, by which the plan’s transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the plan’s financial statements involved in initiating, recording, processing, and reporting the plan’s transactions
- How the plan’s information system captures other events and conditions that are significant to the financial statements
- The financial reporting process used to prepare the plan’s financial statements, including significant accounting estimates and disclosures

The following are examples (not all-inclusive) of the kinds of services that service organizations may provide to an employee benefit plan that would make the service organization part of the plan’s information system:

- Processing of participant-level transactions, including:
  - Contributions and distributions (benefit payments, loans, and administrative expenses)
  - Investment custody and valuation
  - Execution of investment transactions
  - Processing of new participant loans
  - Loan repayments by participants and employer
  - Investment elections by participants or plan sponsors and changes in elections
• The initiation of the purchase or sale of equity securities by a service organization acting as investment adviser or manager

• Services that are ancillary to holding an entity’s securities, such as:
  — Collecting dividend and interest income and distributing that income to the entity
  — Receiving notification of corporate actions
  — Receiving notification of security purchase and sale transactions
  — Receiving payments from purchasers and disbursing proceeds to sellers for security purchase and sale transactions
  — Maintaining records of securities transactions for the entity

• A pricing service providing fair values of derivatives and securities through paper documents or electronic downloads that the entity uses to value its derivatives and securities for financial statement reporting

• Security lending transactions in which the service organization provides collateral to the plan in exchange for the short-term use of certain securities

• Allocation of investment income

• Reconciliation of the participants records to the trust

• Employee Retirement Income Security Act of 1974 (ERISA) compliance, including performance of discrimination testing

• Preparation of the Form 5500 Annual Return/Report of Employee Benefit Plan (Form 5500)

You do not have to gain an understanding of the controls related to services that are not part of the plan’s information system. Examples of a service organization’s services that may not be part of a plan’s information system are the following:

• The execution by a securities broker of trades that are initiated by either the plan or its investment adviser

• The holding of an entity’s securities

Thus, internal control of an employee benefit plan consists of controls at both:

• The plan

• Service organizations that perform significant plan functions
Chapter 2: Use of a Service Organization

Obtaining Necessary Information Without a SAS No. 70 Report

Once you have determined whether the service organization’s services are part of the plan’s information system, you should assess the relative significance of those services before deciding to gain an understanding of the controls in place at the service organization. As the significance of the service organization’s services increases, your understanding of service organization controls will need to be more thorough in order to properly plan the audit. To assess the relative significance of service organization services and determine whether or not you need a SAS No. 70 report, you should consider:

- **The nature of the transactions.** Complex transactions processing by the service organization will increase the significance of the organization to the plan.

- **The materiality of the transactions.** The more material the transactions are to the plan’s financial statements, the more significant the service organization.

- **The degree of interaction between the service organization and the plan.** The degree of interaction relates to the amount of control the plan retains over the initiation and processing of transactions, as follows:

  — **High degree of interaction.** Paragraph 6.05 of the EBP Guide provides the following guidance on situations in which there is a high degree of interaction between the service organization and the plan:

    If a service organization executes and processes transactions initiated by the plan, there may be a high degree of interaction between the activities at the plan and those at the service organization and, in these circumstances, it may be practicable for the plan to implement effective controls for those transactions. Accordingly, the plan may be able to maintain *independent records* of transactions authorized and executed by the service organization. In those circumstances, the auditor may be able to obtain a sufficient understanding of internal control relevant to transactions executed by the service organization to *plan the audit* and to determine the nature, timing, and extent of tests to be performed *without considering those components of internal control maintained by the service organization*. An example of such a service organization is a bank trust department that invests and services assets for a plan under a nondiscretionary or directed trust arrangement. However, even in such circumstances, the auditor may still find it more efficient to seek a reduction in the assessed level of control risk for assertions related to transactions executed by the service organization by considering internal control maintained by the service organization. [emphasis added]

  — **Low degree of interaction.** Paragraph 6.06 of the EBP Guide provides the following guidance on situations in which there is a low degree of interaction between the service organization and the plan:

    If the service organization is authorized by the plan to initiate, execute, and account for the processing of transactions without specific authorization of individual
transactions, there is a lower degree of interaction and it may not be practicable for the plan to implement effective controls for those transactions. The plan therefore may not have independent records of the transactions executed by the service organization. In those circumstances, the auditor may not be able to obtain an understanding of the components of internal control, relevant to such transactions, sufficient to plan the audit and to determine the nature, timing, and extent of tests to be performed without considering those components of internal control maintained by the service organization. [emphasis added]

If you need information about the nature of a service organization’s services or its controls, you are not required to obtain a SAS No. 70 report. The information necessary to plan the audit may be gathered in other ways, including:

- Read the user manuals or other systems documentation about the services provided.
- Read the reports of the internal auditors or regulatory authorities on the service organization’s controls.
- Inquire of or observe the personnel at the client or at the service organization.
- Read the contracts for the services.

Your previous experience with the service organization also may be helpful in planning the audit, but only when the services provided to the plan and the service organization’s controls over those services are highly standardized.

As indicated earlier, your understanding of controls, should be sufficient to (1) identify types of potential misstatements, (2) consider factors that affect the risk of material misstatement, and (3) design substantive tests.

Not all of a service organization’s controls are relevant for planning and performing your audit. In determining which service organization controls are relevant, you should consider:

- The relevant assertions in the plan’s financial statements
- The control objectives of the service organization related to those assertions
- The controls in place to meet those control objectives

In order to plan the audit, you should focus only on the relevant controls and whether they have been placed in operation. If you plan to assess control risk below the maximum for certain assertions, then the operating effectiveness of the controls related to those assertions must be tested and audit evidence gathered to support that assessed level of control risk.
Chapter 2: Use of a Service Organization

THE SERVICE ORGANIZATION AND SAS NO. 70 REPORTS

A service organization may engage an auditor (the service auditor) to perform procedures relating to its controls for the benefit of user organization auditors. Exhibit 2-2, “Summary of Service Auditor Reports,” explains the two types of reports that might be issued by a service auditor. Paragraph 6.08 of the EBP Guide provides a more detailed description of these reports. (See Appendix A, “Excerpts From Audit and Accounting Guide Employee Benefit Plans.”)

Exhibit 2-2 Summary of Service Auditor Reports

<table>
<thead>
<tr>
<th>Title</th>
<th>Contents</th>
<th>Relevance to User Auditors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports on Controls Placed in Operation (Type 1 Report)</td>
<td>• Describes controls and whether they are suitably designed to achieve specified control objectives&lt;br&gt;• States whether controls had been placed in operation as of a specified date&lt;br&gt;• Includes all elements of the Report on Controls Placed in Operation</td>
<td>• Helps the auditor gain an understanding of the controls necessary to plan the audit&lt;br&gt;• Does not provide a basis for reducing control risk below the maximum&lt;br&gt;• Has the same utility as a Type 1 report&lt;br&gt;• Provides a basis for reducing control risk below the maximum for specified assertions</td>
</tr>
<tr>
<td>Report on Controls Placed in Operation and Tests of Operating Effectiveness (Type 2 Report)</td>
<td>• Opines on whether the controls that were tested were operating effectively for a period of time</td>
<td></td>
</tr>
</tbody>
</table>

Practice Pointer. It has come to the AICPA’s attention that, in some cases, service auditors’ engagements are being performed and reported on by consulting organizations that are not licensed CPA firms. SAS No. 70, which is part of GAAS, is intended for use by licensed CPAs. For a user auditor to use a service auditor’s report, it must be issued by a licensed CPA. CPAs may not use a report provided by an unlicensed individual or entity. User auditors should be alert to the possibility that a service auditor’s report may not have been prepared by a licensed CPA and should consider contacting a representative of an unfamiliar organization to verify that the organization is properly licensed, peer reviewed, and able to provide its peer review report and letter of comments and response. If the organization is unlicensed, CPAs are advised to convey that finding to the state board of accountancy in the state in which the engagement was performed or to their own state board.

SUBSERVICING

In some cases, a service organization may use the services of another service organization to perform its data processing. When such a subservice organization is used to process a plan’s transactions, you should consider the need to obtain information about controls at the subservice organization. The process for considering the nature and type of information required from a subservice organization is similar to that used for considering the information required from a ser-
vice organization. In other words, you should consider the effect of the subservice organization on the internal control of the plan as follows:

- The degree of interaction, as well as the nature and materiality of the transactions processed by the service organization and the subservice organization.
- The available information about the service organization’s and subservice organization’s controls, including:
  - Information in the plan management’s possession, such as user manuals, system overviews, technical manuals, and the contract between the plan and the service organization
  - Reports on the service organization’s and subservice organization’s controls, such as reports by service auditors, internal auditors, or regulatory authorities
- Because a plan typically does not have any contractual relationship with the subservice organization, the plan should obtain available reports and information about the subservice organization from the service organization.

**When the Necessary Information Is Not Available**

In the rare circumstance in which the necessary information about the service or subservice organization’s controls is not available, your will have to either:

- Perform the procedures at the service or subservice organization necessary to plan and perform the audit, or, if this is not possible,
- Disclaim an opinion or issue a qualified opinion on the plan’s financial statements.

Note that, historically, the Department of Labor (DOL) has rejected Form 5500 filings that contain either qualified opinions, adverse opinions, or disclaimers of an opinion, except those issued in connection with a limited-scope audit.

---

**Frequently Asked Questions—SAS No. 70 Applicability**

Q. If we plan on assessing control risk at the maximum and performing a purely substantive audit, do we still need to obtain and review a SAS No. 70 report?

A. The question suggests a cause-and-effect relationship between the planned assessment of control risk and the need to review a SAS No. 70 report. In fact, there is no direct link between the two; they are two independent judgments.

First, on all audits—even those for which you plan to assess control risk at the maximum—you are required to obtain an understanding of all five components of internal control, and this understanding should encompass the design of controls and whether they have been placed in operation. If the plan uses a service organization to process certain transactions, and if the service organization is deter-
mined to be a part of the plan’s information system, then you are required to obtain an understanding of the controls related to the transactions processed by the service organization.

To obtain this understanding, you are not required to obtain and review a SAS No. 70 report. It is possible to obtain the required understanding of internal control without a SAS No. 70 report depending on:

- The nature of the services performed by the service organization
- The relationship (e.g., the degree of interaction) between the service organization and the plan
- The existence and nature of independent records and controls maintained by the plan
- The existence of user manuals, contracts, and other documentation
- Other factors

However, you may determine that the most effective and efficient way to obtain the required understanding of internal controls is by reviewing a SAS No. 70 report. If so, you should obtain and review a SAS No. 70 report even though you are planning a purely substantive audit.

Q. What should we do if we determine that we need a SAS No. 70 report, and the service organization does not provide one?

A. First, make sure that you have exhausted all possibilities for obtaining the information you need to obtain the required understanding of internal control. Consider any of the following:

- Read user manuals or other systems documentation about the services provided.
- Inquire of or observe personnel at the entity or at the service organization.
- Read the contracts for the services.

After considering these other procedures and sources of information about controls at the service organization, you may determine that a SAS No. 70 report is necessary for you to obtain the required understanding of internal control. If the service organization does not provide a SAS No. 70 report, then your options are to:

- Perform the procedures at the service organization necessary to plan and perform the audit, or, if this is not possible,
- Modify your audit report for a scope limitation. When a scope limitation is imposed by circumstances (and not by the client) your options are to issue a qualified (“except for”) opinion or disclaim an opinion, depending on the importance of the omitted procedures on your ability to form an opinion on the financial statements.
CHAPTER 3: AUDIT PLANNING WHEN THE PLAN USES A SERVICE ORGANIZATION

As discussed previously, the overall objectives of obtaining an understanding of internal control to plan your audit are to:

- Identify types of potential misstatements.
- Consider factors that affect the risk of material misstatement.
- Design substantive tests.

On some engagements, you may set an additional objective of assessing internal control operating effectiveness, in order to perform a more efficient or effective audit.

To best achieve these audit objectives, you should establish a link between individual controls and the financial statement assertions to which they relate. Thus, an important step in planning an employee benefit plan audit is to establish the link between the controls pertaining to transactions processed by service organizations and the relevant financial statement assertions.

Articulating this link between controls and assertions will allow you to better:

- Understand the effectiveness of the design of internal control, which includes both plan controls and those at the service organization.
- Assess the adequacy of a SAS No. 70 report.
- Design and perform tests of user controls that may be necessary to achieve your overall audit objectives.
- Evaluate the significance of any control test exceptions or control deficiencies.

There are two basic approaches to establishing a link between controls and financial statement assertions. The first is a financial statement-oriented approach that lists the major financial statement line items and the relevant assertions and then determines the transactions and processes that “feed” into the account. In effect, you analyze general-ledger accounts by breaking them down into major transactions and processes.

In the author’s experience, 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 audit inefficiencies. This publication and the related practice aids suggest you take a transaction- or process-oriented approach to linking controls with the relevant financial statement assertions.
Under this approach, you begin by identifying and describing the major transactions and processes of the plan. You then analyze these processes by mapping them to the financial statement accounts to which they relate.

**SAS No. 70 Planning Checklist**

Included in the section of this book entitled “Practice Aids” is the “SAS No. 70 Planning Checklist.” This checklist, together with the accompanying instructions, will help you implement this transaction-oriented approach.

**Obtaining the Information Necessary to Complete the Planning Checklist**

In order to successfully complete the “SAS No. 70 Planning Checklist,” you will need to gather information about the plan’s transactions that are processed by service organizations and the nature of the relationship between the client and the service organization. That information may be obtained through:

- Inquiry of plan personnel
- Review of contracts, user manuals, and other documentation about the service organization’s services
- Knowledge gained from previous audits or other engagements

**SAS No. 70 Considerations in the Planning of a Limited-Scope Audit**

When you are engaged to perform a limited-scope audit of an employee benefit plan, you are not required to perform any auditing procedures with respect to investment information that is prepared and certified by a qualified trustee or custodian. In practice, questions frequently arise about the requirements for obtaining and testing a SAS No. 70 report when performing a limited-scope audit.

First, recognize that the limited-scope exemption applies *only to the investment information* certified by the qualified trustee or custodian. Thus, in a limited-scope engagement, to the extent that the service organization is *only* providing investment transaction services, no SAS No. 70 report is required.
However, the limited-scope exemption does not apply to participant-level transactions such as:

- Participant data
- Contributions
- Benefit payments
- Other information, transactions, or processes

Therefore, you are required to obtain information about controls related to these transactions, which may require you to obtain and review a SAS No. 70 report.

Paragraph 6.12 of the EBP Guide provides definitive guidance on the use of SAS No. 70 reports in a limited-scope audit of an employee benefit plan. (This paragraph is included in Appendix A, “Excerpts From Audit and Accounting Guide Employee Benefit Plans.”)

Frequently Asked Questions—Audit Planning

Q. From whom should the auditor obtain the SAS No. 70 report?

A. The service organization is responsible for determining whether it will engage a service auditor to perform a service auditor engagement and issue a SAS No. 70 report. The use of a SAS No. 70 report is restricted to the service organization, its current customers (your client) and those customers’ auditors (you). You may obtain the SAS No. 70 report either directly from the service organization or from your client.
CHAPTER 4: HOW TO REVIEW A SAS NO. 70 REPORT

This chapter describes what you should consider when reviewing a SAS No. 70 report to assess its adequacy and its impact on your audit of the plan’s financial statements. Included in the “Practice Aids” section of this book is the “SAS No. 70 Report Review Checklist,” which you can use to help you implement the suggestions that follow.

The review of a SAS No. 70 report generally requires you to read and evaluate the following:

- The service auditor’s report
- The service organization’s description of service organization controls
- Control objectives and the related control procedures
- Complementary user organization controls
- Tests of operating effectiveness (only if you plan on assessing control risk below the maximum)
- Testing exceptions, instances of noncompliance with documented control procedures, or control deficiencies

**The Service Auditor’s Report**

In a Type 1 SAS No. 70 report, the service auditor issues a report on a description of controls that has been prepared by management. The service auditor performs a variety of procedures that allow him or her to express an opinion on whether the:

- Description of the service organization’s controls presents fairly, in all material respects, the relevant aspects of the service organization’s controls that had been placed in operation as of a specified date.

- Controls were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those controls were complied with satisfactorily.

In a Type 2 SAS No. 70 engagement, the service auditor performs the same procedures as in a Type 1 engagement and, in addition, performs tests of specific controls to evaluate their operating effectiveness. The service auditor’s report includes the same opinions as a Type 1 report, plus an opinion as to whether the controls tested were operating with sufficient effectiveness to provide reasonable but not absolute assurance that the related control objectives were achieved during the period specified.
Exhibit 4-1, “Service Auditor’s Opinions Included in Type 1 and Type 2 Service Auditors’ Reports,” summarizes the auditor’s opinions that are included in a SAS No. 70 report.

### Exhibit 4-1 Service Auditor’s Opinions Included in Type 1 and Type 2 Service Auditors’ Reports

<table>
<thead>
<tr>
<th>Opinion</th>
<th>Type 1 Report</th>
<th>Type 2 Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whether the service organization’s description of its controls presents fairly, in all material respects, the relevant aspects of the service organization’s controls that had been placed in operation as of a specific date</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Whether the controls were suitably designed to achieve specified control objectives</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Whether the controls that were tested were operating with sufficient effectiveness to provide reasonable but not absolute assurance that the control objectives were achieved during the period specified</td>
<td>Not included</td>
<td>Included</td>
</tr>
</tbody>
</table>

Start your review of the SAS No. 70 report by reading the service auditor’s report. Consider whether the:

- Report is a Type 1 or Type 2 report and whether that report type is adequate for your needs for the audit of the plan’s financial statements.
- Service auditor has modified the standard report, and, if so, the implications that modifications will have on your audit of the plan’s financial statements.

### Timing Considerations

The service organization’s description of controls is as of a specified date for both Type 1 and Type 2 reports. In a Type 2 report, the service auditor’s tests of control operating effectiveness will cover a *period of time*. Both of these timing considerations will be stated in the service auditor’s report, usually in the last paragraph. You should note these dates and evaluate how the timing of the service auditor’s engagement affects your audit.

It is not unusual for the SAS No. 70 report to cover a different reporting period than the plan’s fiscal year or for the description of controls to be as of a date that is different from the plan’s fiscal year-end. In those situations, you should make inquiries of the service organization or its auditor to determine whether there were changes in the service organization’s controls during the period not covered by the SAS No. 70 report.

---

1 This exhibit originally appeared as Table 2.1 in the AICPA Audit and Accounting Guide *Service Organizations: Applying SAS No. 70.*
If the period not covered is significant or there have been changes in the controls, you should gain an understanding of the service organization’s controls relating to the plan’s transactions during the period not covered by the SAS No. 70 report. The procedures performed to update the information in a service auditor’s report may include:

- Discussions with the client personnel who would be in a position to know about changes at the service organization. These discussions may include inquiries relating to:
  - Changes to application systems and control activities
  - Processing problems encountered during the audit period and how they were resolved
  - Changes in the reliability of the processing of financial information
- A review of current documentation and correspondence issued by the service organization.
- Discussions with service organization personnel or with the service auditor about matters such as:
  - Changes to the application system or related control activities outside the period covered by the report
  - Additional information concerning the reliability of the processing of financial information
  - The basis for determining the period covered by the report
  - Whether the service auditor would consider applying agreed-upon procedures to supplement the SAS No. 70 report

If there have been significant changes in the service organization’s controls, you should attempt to gain an understanding of the changes and consider the effect of the changes on the audit of the plan’s financial statements.

**Description of the Service Organization’s Controls**

Both Type 1 and Type 2 SAS No. 70 reports are required to provide a description of the service organization’s controls, which generally is prepared by the service organization. The service organization is responsible for the completeness, accuracy, and method of presentation of the description of controls. The service auditor is responsible for reading the service organization’s description of controls and performing additional procedures to determine whether the description is a fair presentation of controls that had been placed in operation.

The service organization’s description of controls should be presented at a level of detail that provides you with the information you need to plan the audit. The description of controls, by itself, is not adequate to allow you to assess control risk below the maximum for any assertion.
The service organization’s description of controls generally should contain the following information:

- Aspects of the service organization’s control environment; risk assessment; information and communication; and monitoring that may affect the services provided to user organizations, as it relates to an audit of financial statements
- Control objectives and related controls
- Changes to controls since the later of the date of the last report or within the last 12 months

When reading the service organization’s description of controls, you should satisfy yourself that the information provided is of sufficient detail to allow you to achieve your audit objectives. Paragraph 2.29 of the AICPA Audit Guide *Service Organizations: Applying SAS No. 70* provides the following guidance on the level of detail required in a service organization’s description of controls:

The service organization’s description of controls should provide sufficient information for user auditors to understand how the service organization’s processing affects the [five components of internal control]. The degree of detail of the description should be equivalent to the degree of detail a user auditor would require if a service organization were not used. However, it need not be so detailed as to potentially 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 also should indicate the extent of the manual and computer processing used.

With regard to the information aspect of the information and communication component of internal control, the service organization’s description of controls should allow you to understand:

- The classes of transactions in the plan’s operations that are significant to the financial statements
- The procedures, both automated and manual, by which transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements
- The related accounting records, whether electronic or manual; supporting information; and specific accounts in the financial statements involved in initiating, recording, processing, and reporting transactions
- How the information system captures other events and conditions that are significant to the financial statements
- The financial reporting process used to prepare the plan’s financial statements, including significant accounting estimates and disclosures
Note that not all of the above will be applicable for every service organization. For example, the services performed by the service organization may not be related to the plan’s financial reporting process or the preparation of accounting estimates or disclosures.

**CONTROL OBJECTIVES, RELATED CONTROLS, AND ASSERTIONS**

The service organization’s description of controls should include a discussion of control objectives and related controls. This discussion also may link the control objectives to the financial statement assertions to which they are likely to relate. In forming their opinion on the design of controls, the service auditor will evaluate the description of the control objective by considering:

- The link between control procedures and objectives
- The ability of the controls to prevent or detect errors related to the control objectives

In reading a SAS No. 70 report, your primary concern should be to assess the scope of the work described in the report. You should read this section of the report carefully to be sure that the controls included in the description are adequate for your needs as the auditor of the plan’s financial statements. To be adequate:

- All significant transactions, processes, or computer applications that you previously identified (see the section entitled “Audit Planning When the Plan Uses a Service Organization”), as affecting the plan’s financial statements should be described in the report.
- For each significant transaction, process, or computer application, control objectives should be identified for all assertions that are relevant to the financial statement accounts affected by the transactions.

**COMPLEMENTARY USER ORGANIZATION CONTROLS**

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

- Service organization controls, and
- Controls administered by the client (user organization controls)

The service auditor, when performing an engagement at the service organization, may observe instances in which the service organization’s service was designed with the assumption that certain controls would be implemented by the client. Such controls are called *complementary user organization controls*. Examples of complementary user organization controls include controls at the client:
• Over passwords needed to access the service organization’s application through remote terminals or over the Internet
• To ensure that all input sent to the service organization is complete, accurate, and authorized
• To ensure that all required output is received from the service organization and reconciled to the input sent to the service organization

These complementary user organization controls are required to be included in the service organization’s description of controls. (If they are not, then the service auditor will describe them in the service auditor’s report.)

You should make note of the complementary user controls identified in the SAS No. 70 report and determine that they have been properly included within the scope of your audit, for example, whether you have:

• Performed audit procedures to determine that the required complementary user controls have been suitably designed and placed in operation by the client.
• Tested the operating effectiveness of the required complementary user controls, whenever you plan to assess control risk below the maximum.

**Tests of Operating Effectiveness**

If you plan to assess control risk below the maximum for some financial statement assertions, then you need to obtain evidence about the operating effectiveness of the related controls. For controls located at a service organization, this evidence may be provided by a Type 2 SAS No. 70 report.

When evaluating the service auditor’s description of the tests of operating controls, you should consider the following:

• Were the controls tested related to the assertions for which you plan to assess control risk below the maximum? To make this determination, the service auditor should link the control procedure to an identified control objective, and you should satisfy yourself that this control objective has a direct bearing on the financial statement assertion you will be testing.

• Were the nature, timing, and extent of the tests performed sufficient to allow you to draw a conclusion about control risk for the purposes of performing your audit of the plan’s financial statements?

• Do the results of the tests performed support an assessment of control risk below the maximum?
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 the recording of transactions for the client. The following table summarizes certain information that might appear in a Type 2 SAS No. 70 report and the questions you should consider relating to how this information affects your audit.

Exhibit 4-2 Information Obtained From Type 2 SAS No. 70 Reports

<table>
<thead>
<tr>
<th>Required Element</th>
<th>Information Provided by Service Auditor</th>
<th>Auditor’s Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control objective</td>
<td>Controls provide reasonable assurance that security purchase and sale transactions are recorded at the appropriate amounts and in the appropriate periods.</td>
<td>• Does the control objective have a direct relationship to a financial statement assertion?</td>
</tr>
<tr>
<td></td>
<td>Reconciliations are performed daily and reconciling items are identified and resolved within ten days and before the issuance of customer statements.</td>
<td>• If so, which one?</td>
</tr>
<tr>
<td>Tests of control</td>
<td>The service auditor inspected a sample of x reconciliations covering the test period.</td>
<td>• Is the control procedure directly linked to the stated control objective? That is, would the procedure, if designed and operating effectively, help achieve the control objective?</td>
</tr>
<tr>
<td></td>
<td>Reconciling items for the reconciliations inspected appeared to result from normal processing and ranged from a few cents to several thousand dollars. Reconciling items were identified timely but were not always resolved before the issuance of customer statements.</td>
<td>• Are the nature, timing, and extent of the service auditor’s test procedures capable of providing sufficient and adequate evidence about the operating effectiveness of the control?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do the results of the tests support an assessment of control risk below the maximum?</td>
</tr>
</tbody>
</table>
If you have a Type 2 SAS No. 70 report that states income allocation and/or participant contributions were tested and no exceptions were found, would you rely on this or do more testing?

A. It depends on the nature, timing, and extent of the tests of controls performed by the service auditor. Ask yourself, if no service organization was involved and you were testing the operating effectiveness of the controls in question, would you:

• Perform the same types of tests as the service auditor?
• Test the same number of items?
• Perform the tests as of the same date?

If the answer to these questions is yes, then you should be able to rely on the service auditor's tests and the results of those tests to support control risk below the maximum. If you answer no to one or more of these questions, you should supplement the service auditor’s work with additional procedures of your own. Alternatively, you can assess control risk at maximum and design your substantive tests accordingly.

You also should keep in mind that the service auditor’s tests alone are not sufficient to allow you to completely support a control risk assessment below maximum or to conclude on the fairness of the financial statements. In addition to the service auditor’s tests of controls at the service organization you also should:

• Consider the design and, possibly, the operating effectiveness of complementary controls maintained by the client, and
• Perform substantive tests on the account balance. However, if you can assess control risk below the maximum, you can reduce the amount of your substantive testing.
Your reading of the SAS No. 70 report may lead you to identify one or more of the following:

- Inadequacies in the report itself
- Instances of noncompliance with stated controls
- Control deficiencies at the service organization

In all of these instances you should:

- Evaluate the condition.
- Determine how it affects your ability to plan the audit and your assessment of control risk.
- Based on your determination, develop an appropriate audit response.

**Report Inadequacies**

Your reading of the SAS No. 70 report may lead you to conclude that it is not adequate for your purposes. These shortcomings may include:

- Lack of sufficient detail, which prevents you from gaining the knowledge you need to plan the audit or assess control risk
- Lack of sufficient scope (For example, the report does not include information about transactions, control objectives, or individual controls.)
- Lack of synchronicity between the timing of the service auditor’s engagement and your audit of the plan (For example, the “as of” date for the service organization’s description of controls does not coincide with the plan’s year-end, or the period of time covered by the service auditor’s tests of controls does not coincide with the plan’s reporting period.)

If you determine that the SAS No. 70 report does not provide you with the information you need to determine the design of internal controls and whether they have been placed in operation, you should perform procedures to obtain the necessary information from other sources. As discussed previously in this publication (specifically, the section entitled “Obtaining Necessary Information Without a SAS No. 70 Report”), those procedures include the reading of relevant documentation and inquiries of client or service organization personnel.
If performing these other procedures still does not allow you to obtain a sufficient understanding of internal control, you will need to either perform the necessary procedures yourself at the service organization, or consider a scope limitation on your audit of the plan’s financial statements. (See the section entitled “When the Necessary Information Is Not Available.”)

**Instances of Noncompliance**

The SAS No. 70 report may identify instances in which the controls of the service organization were not followed. The service auditor also may note instances in which evidence of performance of the control was not maintained; and therefore, the service auditor could not determine whether the control had been placed in operation. For example, the service auditor may note:

> For one contribution tested, we could not review evidence of the comparison of deferral and match amounts, sent from the plan sponsor, to amounts imported into the records

When evaluating the significance of noncompliance, be sure to fully understand the situation noted by the service auditor and whether any of the following apply:

- The service auditor obtained evidence that failed to indicate that the control was performed.
- The service auditor was unable to obtain any evidence relating to the performance of the control. If this is the case, you should consider the significance of the procedures that the service auditor was unable to perform due to the missing documentation or other evidence. For example, if the service auditor was unable to review evidence for one transaction out of the 40 selected, you probably still have enough information to plan the audit, and you may be able to support assessing control risk below the maximum.
- The instance of noncompliance or lack of evidence was significant enough to result in a modification to the service auditor’s report.

In both situations, you should evaluate the service auditor’s observations, assess their impact on your ability to plan the audit and, possibly, assess control risk below the maximum. To make this assessment, consider the following questions:

- How would the plan’s financial statements be misstated if the control failed and there were no other controls in place to prevent or detect the misstatement?
- How significant would the misstatement be to the plan’s financial statements?
- Considering the significance of the noted instance of noncompliance plus the operation of other controls that address the same control objective, what is the likelihood that a misstatement to the plan’s financial statements could occur?
• Given the type of misstatement that could occur, its significance to the plan’s financial statements, and its likelihood of happening, are your planned audit procedures sufficient? Consider the following:

— *The nature of the planned procedures.* The noncompliance with controls at the service organization may result in you performing different types of substantive tests.

— *The extent of the planned procedures.* The noncompliance with controls at the service organization may result in you performing more of the same planned substantive procedure; for example, sending more confirmations.

— *The timing of the planned procedures.* The noncompliance with controls at the service organization may result in you performing your substantive tests closer to the plan’s year-end.

If you had planned on relying on the control to reduce your substantive tests, an instance of noncompliance with controls at the service organization may preclude you from assessing control risk below the maximum.

Finally, you should consider whether the instances of noncompliance indicate a control deficiency at the service organization that should be reported to the plan sponsor. See AU Sections 325, *Communication of Internal Control Related Matters Noted in an Audit* (AICPA, Professional Standards, vol. 1, AU sec. 325), and AU Section 9325, *Communication of Internal Control Related Matters Noted in an Audit: Auditing Interpretations of Section 325* (AICPA, Professional Standards, vol. 1, AU sec. 9325), for guidance on reporting control deficiencies.
To implement the suggestions contained in this publication, you should be familiar with the following terms, which are defined in AICPA Statement on Auditing Standards (SAS) No. 70, *Service Organizations* (AICPA, Professional Standards, vol. 1, AU sec. 324), as amended:

- **User organization.** The entity that has engaged a service organization and whose financial statements are being audited; in an employee benefit plan audit, this term applies to the client.

- **User auditor.** The auditor who reports on the financial statements of the user organization; in an employee benefit plan audit, this term applies to the auditor of the plan’s financial statements, which are referred to in this publication as “you.”

- **Service organization.** The entity (or segment of an entity) that provides services to a user organization that are part of the user organization’s information system; in an employee benefit plan audit, the most common service organizations are:
  - Recordkeepers, whose responsibilities include the maintenance of participant accounts
  - Trustees and custodians, whose responsibilities include the custody of assets, reporting of income, prices and investment shares, execution of trades, and the preparation of checks
  - Claims processors for health and welfare plans
  - Payroll processing providers

- **Service auditor.** The auditor who reports on controls of a service organization that may be relevant to a user organization’s internal control as it relates to an audit of financial statements.
These practice aids have been prepared to illustrate ways in which you might implement and document the requirements for considering the plan’s use of a service organization in an employee benefit plan audit. These practice aids incorporate the nonauthoritative suggestions contained in this publication.

These tools have not been peer reviewed or subjected to any other form of quality assurance. Before using them on your engagements, you should determine that they are suitable for your purpose.
AUDIT PROGRAM: CONSIDERING SERVICE ORGANIZATION CONTROLS

AP-SAS No. 70: Audit Program for
Consideration of SAS No. 70 Reports

Plan: ________________________________ Balance Sheet Date:

<table>
<thead>
<tr>
<th>Audit Objective</th>
<th>Audit Procedure for Consideration</th>
</tr>
</thead>
</table>

Audit Objective

A. Determine whether a SAS No. 70 report is required in order to:
   • Obtain an understanding of the design of internal controls and whether they have been placed in operation (all audits).
   • Assess control risk below the maximum for certain financial statement assertions (if applicable).

B. Read and understand the SAS No. 70 report to determine how service organization’s controls affect the following:
   • Types of potential misstatements to the plan’s financial statements
   • Factors that affect the risk of material misstatement
   • Design of substantive audit tests
   • Assessment of control risk for individual assertions

Planning (See the “SAS No. 70 Planning Checklist.”)

1. Identify plan transactions that are processed by a service organization.

2. Link the transactions identified in Step 1 to the plan’s financial statements and relevant assertions.

3. Determine whether a SAS No. 70 report is needed for each of the transactions identified in Step 1. If a SAS No. 70 report is not needed or is unavailable, then either:
   a. Perform alternative procedures to obtain the information necessary to plan the audit, or
Practice Aids

Audit Objective | Audit Procedure for Consideration | N/A Performed By | Working Paper Index
---|---|---|---

b. Modify the auditor’s report for a scope limitation.

4. Obtain the necessary SAS No. 70 report(s), either from the client or directly from the service organization.

Read and Assess the Implications of the SAS No. 70 Report

5. Read the service auditor’s report and assess its implications for the audit of the plan’s financial statements, including:
   a. Whether the service auditor prepared a Type 1 or Type 2 report
   b. The nature of the opinions rendered and whether these included any modifications to the standard reporting language
   c. The timing of the engagement, that is:
      i. The date “as of” when the description of controls applies
      ii. The period of time covered by the tests of operating effectiveness of controls, if control risk is to be assessed below the maximum

6. Read the description of the service organization’s controls and evaluate the effect of the following on the audit of the plan’s financial statements:
   a. Whether the description includes all significant transactions, processes, computer applications, or business units that affect the audit of the plan’s financial statements
   b. Whether the description includes all five components of internal control
   c. Whether the description is sufficiently detailed to understand how the service organization’s processing affects the plan’s financial statements
   d. Changes to service organization controls
   e. Instances of noncompliance with service organization controls

(continued)
<table>
<thead>
<tr>
<th>Audit Objective</th>
<th>Audit Procedure for Consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td>f.</td>
<td>Whether the description of controls is adequate to provide an understanding of those elements of the plan’s accounting information system maintained by the service organization.</td>
</tr>
</tbody>
</table>

7. List all complementary user organization controls identified in the SAS No. 70 report that the service auditor assumed were maintained by the client. Cross reference this list to the audit work performed to:

a. Understand the design of these complementary client controls and whether they have been placed in operation.

b. If applicable, test the operating effectiveness of these controls.

Tests of Operating Effectiveness, If Applicable

8. Review the service auditor’s description of the tests of controls and assess their adequacy for your purposes. Consider the following:

a. The link between the financial statement assertion and the control objective

b. The link between the control objective and the controls tested

c. The nature, timing, and extent of the tests performed

9. Evaluate the results of the tests of controls and determine whether they support assessing control risk below the maximum.
Instructions for Use

This “SAS No. 70 Planning Checklist,” is a tool that you can use to provide a high-level summary of the service organizations that provide services to the plan that affect the plan’s financial statements. (See Chapter 3 of this practice aid for guidance on using this planning checklist.) The following are the definitions of the column headings that appear in the checklist:

Transactions and Processes. The first column of the checklist gives a list of the employee benefit plan transactions and processes that are most commonly processed by a service organization. These were described earlier in this book. This example list is a good starting point but ultimately must be tailored to your individual client.

Financial Statement Line Items and Assertions. Use these two columns to summarize financial statement line items and the assertions affected by each transaction.

Risk Below Maximum? Use this column to document the assertions for which you plan to assess control risk below the maximum. If you plan a 100-percent substantive audit for all assertions related to the transaction, enter None.

Processed by Service Organization? Use this column to indicate whether the process is performed by the service organization. A no response indicates that the function is performed by the client.

SAS No. 70 Report Needed? As discussed previously in this publication, the fact that a service organization is part of the plan’s information system does not require you to obtain a SAS No. 70 report. Depending on the facts and circumstances of the relationship between the plan and the service organization, you may be able to achieve your audit objectives related to understanding internal control without obtaining a SAS No. 70 report. Using the suggestions provided earlier in this book, you should determine whether a SAS No. 70 report is needed for the controls related to each of the transactions and processes indicated on the checklist. You can use this column of the checklist to document your conclusions about the need for a SAS 70 report.

Service Organization. In this column, you identify the service organizations, if any, that provide services related to the transactions or processes.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant-level transactions</td>
<td></td>
<td></td>
<td>Y N</td>
<td>Y N</td>
<td>Y N</td>
<td></td>
</tr>
<tr>
<td>Purchase and sale of securities</td>
<td></td>
<td></td>
<td>Y N</td>
<td>Y N</td>
<td>Y N</td>
<td></td>
</tr>
<tr>
<td>Allocation of investment income</td>
<td></td>
<td></td>
<td>Y N</td>
<td>Y N</td>
<td>Y N</td>
<td></td>
</tr>
<tr>
<td>Services ancillary to holding equity securities</td>
<td></td>
<td></td>
<td>Y N</td>
<td>Y N</td>
<td>Y N</td>
<td></td>
</tr>
<tr>
<td>Pricing of derivatives and securities</td>
<td></td>
<td></td>
<td>Y N</td>
<td>Y N</td>
<td>Y N</td>
<td></td>
</tr>
<tr>
<td>Security lending transactions</td>
<td></td>
<td></td>
<td>Y N</td>
<td>Y N</td>
<td>Y N</td>
<td></td>
</tr>
<tr>
<td>Reconciliation of the participants' records</td>
<td></td>
<td></td>
<td>Y N</td>
<td>Y N</td>
<td>Y N</td>
<td></td>
</tr>
<tr>
<td>ERISA compliance</td>
<td></td>
<td></td>
<td>Y N</td>
<td>Y N</td>
<td>Y N</td>
<td></td>
</tr>
<tr>
<td>Preparation of Form 5500</td>
<td></td>
<td></td>
<td>Y N</td>
<td>Y N</td>
<td>Y N</td>
<td></td>
</tr>
</tbody>
</table>
SAS No. 70 Report Review Checklist

Part I: General Information

Name of the Service Organization: ________________________________________________

Type of SAS No. 70 report received: Type 1 _____ Type 2 _____

"As of" date for description of the service organization controls: ____________

Period covered by service auditor's tests of control operating effectiveness: ____________

Cross reference to SAS No. 70 planning checklist: _______________________________

If the SAS No. 70 planning checklist was not used:

List the kinds of transactions processed by the service organization that affect the plan's financial statements:

_____________________________________________________________________

_____________________________________________________________________

_____________________________________________________________________

List the significant financial statement accounts and disclosures affected by transactions processed by the service organization:

_____________________________________________________________________

_____________________________________________________________________

_____________________________________________________________________

List the financial statement assertions for which you plan to assess control risk below the maximum:

_____________________________________________________________________

_____________________________________________________________________

_____________________________________________________________________

_____________________________________________________________________

1 See Chapter 4 of this practice aid for guidance on using the SAS No. 70 Report Review Checklist.
Part II: Review of Service Auditor’s Report

Document the opinions provided in the service auditor’s report by checking the appropriate boxes in the following:

<table>
<thead>
<tr>
<th>Required Opinion</th>
<th>Service Auditor Opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whether the service organization’s description of its controls presents fairly, in all material respects, the relevant aspects of the service organization’s controls that had been placed in operation as of a specific date</td>
<td>☐  ☐</td>
</tr>
<tr>
<td>Whether the controls were suitably designed to achieve specified control objectives</td>
<td>☐  ☐</td>
</tr>
<tr>
<td>Whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute assurance that the control objectives were achieved during the period specified</td>
<td>☐  ☐</td>
</tr>
</tbody>
</table>

Describe any modifications to the service auditor’s standard opinion and the effect these modifications have on the audit of the plan’s financial statements.

Part III: Review of the Service Organization’s Description of Controls

<table>
<thead>
<tr>
<th>Internal Control Component</th>
<th>Control Environment</th>
<th>Risk Assessment</th>
<th>Information and Communication</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### Internal Control Component

<table>
<thead>
<tr>
<th></th>
<th>Control Environment</th>
<th>Risk Assessment</th>
<th>Information and Communication</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>3. The SAS No. 70 report identified no changes to controls since the later of the date of the last service auditor's report or within the last 12 months.</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>4. The SAS No. 70 report identified no instances of noncompliance with the service organization's controls identified in the service organization's description of controls.</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Additional Questions for the Information Component of Internal Control

The following questions apply only to those elements of the information system that are maintained by the service organization. To the extent that the client is responsible for performing certain accounting information functions (e.g., the preparation of significant estimates or disclosures), you should mark the question N/A.

5. The service auditor's report is adequate to allow us to obtain sufficient knowledge of the information relevant to the plan's financial reporting and to understand those elements of the information system maintained by the service organization related to the following:

   a. The classes of transactions in the plan's operations that are significant to the financial statements

   b. The procedures, both automated and manual, by which transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements

   c. The related accounting records, whether electronic or manual; supporting information; and specific accounts in the financial statements involved in initiating, recording, processing, and reporting transactions

   d. How the information system captures other events and conditions that are significant to the financial statements
Control Objectives, Related Controls, and Assertions

6. The scope of the SAS No. 70 report addresses the following:
   
a. All transactions, processes, or computer applications identified in Part I of this checklist that affect the plan’s financial statements
   
b. For all transactions, processes, or computer applications, a description in the service auditor’s report of the relevant assertions for the significant financial statement accounts identified in Part I of this checklist

Audit Response

Describe any no responses to the preceding questions by documenting:

• The conditions cited in the SAS No. 70 report that gave rise to the no response
• The planned audit response to these conditions

Part IV: Complementary User Organization Controls

List the controls identified in the SAS No. 70 report that the service organization assumed were placed in operation at the user organization (complementary user organization controls). Describe the procedures performed, information gathered, and conclusions reached regarding the design of these complementary user organization controls and whether they have been placed in operation.
Part V: Tests of Operating Effectiveness (if applicable)

Review the “SAS No. 70 Planning Checklist,” for the financial statement assertions affected by service organization services for which the planned control risk assessment is below maximum. Summarize these assertions across the horizontal axis. For each assertion, answer the questions listed in the first column, and document your answers by circling Y or N.

<table>
<thead>
<tr>
<th>Assertions for Which Control Risk Is to Be Assessed Below Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td>1. Is the assertion linked to a service organization control objective?</td>
</tr>
<tr>
<td>2. Is the control objective linked to related control activities?</td>
</tr>
<tr>
<td>3. Is the description of the nature, timing, and extent of the tests applied in sufficient detail to enable you to determine the effect of the tests on your assessment of control risk?</td>
</tr>
<tr>
<td>4. Do the results of the service auditor’s tests support assessing control risk below the maximum?</td>
</tr>
</tbody>
</table>

Describe any no responses to the preceding questions by documenting:

- The conditions cited in the SAS No. 70 report that gave rise to the no response
- The planned audit response to these conditions
APPENDIX A: EXCERPTS FROM AUDIT AND ACCOUNTING GUIDE
EMPLOYEE BENEFIT PLANS

The following guidance was excerpted from the AICPA Audit and Accounting Guide _Employee Benefit Plans_, with conforming changes as of March 1, 2005.

6.04 In some cases, a third-party administrator or service organization, such as a bank trustee, custodian, insurance company, or contract administrator (hereafter referred to collectively as service organization), processes certain transactions on behalf of the plan administrator. A service organization’s services are part of a plan’s information system if they affect any of the following:

a. The classes of transactions in the plan’s operations that are significant to the plan’s financial statements.

b. The related accounting records, whether electronic or manual, supporting information, and specific accounts in the plan’s financial statements involved in initiating, recording, processing and reporting the plan’s transactions.

c. How the plan’s information system captures other events and conditions that are significant to the financial statements.

d. The financial reporting process used to prepare the plan’s financial statements including significant accounting estimates and disclosures.

Many plans offer their participants direct access to the service organization by telephone or electronic means (such as the Internet or Intranet). Often, the plan sponsor does not maintain independent accounting records supporting these transactions. The auditor’s consideration of components of internal control maintained by the service organization will depend on the nature of the relationship between the plan and service organization.

6.05 If a service organization executes and processes transactions initiated by the plan, there may be a high degree of interaction between the activities at the plan and those at the service organization and, in these circumstances, it may be practicable for the plan to implement effective controls for those transactions. Accordingly, the plan may be able to maintain independent records of transactions authorized and executed by the service organization. In those circumstances, the auditor may be able to obtain a sufficient understanding of internal control relevant to transactions executed by the service organization to plan the audit and to determine the nature, timing, and extent of tests to be performed without considering those components of internal control maintained by the service organization. An example of such a service organization is a bank trust department that invests and services assets for a plan under a nondiscretionary or directed trust arrangement. However, even in such circumstances, the auditor may still find it more efficient to seek a reduction in the as-
sessed level of control risk for assertions related to transactions executed by the service organization by considering internal control maintained by the service organization.

6.06 If the service organization is authorized by the plan to initiate, execute, and account for the processing of transactions without specific authorization of individual transactions, there is a lower degree of interaction and it may not be practicable for the plan to implement effective controls for those transactions. The plan therefore may not have independent records of the transactions executed by the service organization. In those circumstances, the auditor may not be able to obtain an understanding of the components of internal control, relevant to such transactions, sufficient to plan the audit and to determine the nature, timing, and extent of tests to be performed without considering those components of internal control maintained by the service organization.

Service Organizations and Using SAS No. 70 Reports

6.07 Internal control of a benefit plan consists of the controls at the sponsor as well as the controls at applicable service organizations who perform significant plan functions including but not limited to processing of participant-level transactions such as contributions and distributions, investment custody and valuation, and execution of investment transaction. For a further discussion of internal control as it relates to investments, see the “Internal Control” section in chapter 7 of this guide. SAS No. 70, *Service Organizations*, as amended, provides guidance on the factors an independent auditor should consider when auditing the financial statements of an entity, such as a service organization to process certain transactions that are part of the plan’s information system. SAS No. 70, as amended, also provides guidance for independent auditors who issue reports on the processing of transactions by service organizations, such as bank trust departments, third-party administrators, or data processing service organizations, for use by other auditors. A report prepared in accordance with SAS No. 70, as amended, should be designed to provide user auditors with a sufficient understanding of controls at the service organization to plan the audit in accordance with SAS No. 55, as amended. (See the AICPA Audit Guide *Service Organizations: Applying SAS No. 70, as Amended*, for additional guidance for user auditors engaged to audit the financial statements of entities that use service organizations and for service auditors engaged to issue reports on the controls of service organizations.)

6.08 Under SAS No. 70, as amended, two types of reports may be issued by a service auditor:

a. A *Report on Controls Placed in Operation* (Type I report) is a report on a service organization’s description of its controls that may be relevant to a user organization’s internal control as it relates to an audit of financial statements. It addresses whether the description presents fairly, in all material respects, the relevant aspects of the service or-

---

+ It has come to the AICPA’s attention that in some cases, service auditors’ engagements are being performed and reported on by consulting organizations that are not licensed CPA firms. SAS No. 70, which is part of generally accepted auditing standards, is intended for use by licensed CPAs. For a user auditor to use a service auditor’s report, it must be issued by a licensed CPA. CPAs may not use a report provided by an unlicensed individual or entity. User auditors should be alert to the possibility that a service auditor’s report may not have been prepared by a licensed CPA and should consider contacting a representative of an unfamiliar organization to verify that the organization is properly licensed, peer reviewed, and able to provide its peer review report and letter of comments and response. If the organization is unlicensed, CPAs are advised to convey that finding to the state board of accountancy in the state in which the engagement was performed or to their own state board.
organization’s controls that had been placed in operation as of a specified date and whether such controls were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those controls were complied with satisfactorily. Such reports may be useful in providing user auditors with an understanding of the service organization’s controls sufficient to plan the audit and to design effective tests of controls and substantive tests at the user organization. However, they are not intended to provide user auditors with a basis for reducing their assessment of control risk below the maximum for financial statement assertions affected by the controls.

b. A Report on Controls Placed in Operation and Tests of Operating Effectiveness (Type II report) is a report on a service organization’s description of its controls that may be relevant to a user organization’s internal control as it relates to an audit of financial statements. It addresses whether the description presents fairly, in all material respects, the relevant aspects of the service organization’s controls that had been placed in operation as of a specified date; whether such controls were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those controls were complied with satisfactorily; and whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified. Such reports may be useful in providing user auditors with an understanding of the service organization’s controls that is sufficient to plan the audit and may also provide user auditors with a basis for reducing their assessment of control risk below the maximum for financial statement assertions affected by the controls.

6.09 The type of report (Type I or Type II) provided by the service organization may affect the nature, timing, and extent of the audit procedures performed by the auditor of an employee benefit plan. For example, a bank trust department may specify the control objective that security prices are received timely from an authorized source and properly used to price securities. If the bank provides a Type I report, the report should provide the auditor with sufficient information to plan the audit, in other words, to assess whether there are any deficiencies in the design of the controls that could affect financial statement assertions in the user organization’s financial statements. However, the auditor would have no basis to conclude that the controls were operating with sufficient effectiveness to achieve the control objective because they have not been tested. Therefore, the auditor may have to expand the testing of prices used at year-end. If, however, the bank issued a Type II report, the auditor could have a basis to rely on the effective operation of controls and therefore reduce the extent of the price testing.

6.10 A SAS No. 70 report may provide the most efficient means to obtain an understanding of relevant controls at the service organization. The auditor should read the entire SAS No. 70 document to determine if there are any instances of noncompliance with the service organization’s controls identified in (a) the service auditor’s report (b) the attached service organizations description of controls, and (c) the information provided by the service auditor, which may include a description of tests of operating effectiveness and other information. If the service organization’s SAS No. 70 report identifies instances of noncompliance with the service organization’s controls, the plan auditor should consider the effect of the findings on the assessed level of control risk for the audit of the plan’s financial statements, and as a result the plan auditor may decide to perform additional tests at the service organization or, if possible, perform additional audit procedures at the plan. In certain situations the SAS No. 70 report may identify instances of noncompliance with the service organization’s controls but the plan auditor concludes that no additional tests or audit procedures are
required because the noncompliance does not affect the assessment of control risk for the plan. Under no circumstances should the service auditor’s report be the only basis for reducing the assessed level of control risk below the maximum. The user auditor should read and consider both the report and the evidence provided by the tests of operating effectiveness and relate them to the assertions in the user organization’s financial statements. Although a type II report may be used to reduce substantive procedures, neither a type I nor a type II report is designed to provide a basis for assessing control risk sufficiently low to eliminate the need for performing any substantive tests for all of the assertions relevant to significant account balances or transaction classes.

6.11 The plan auditor should consider asking the plan’s management whether the service organization has reported any uncorrected errors to the user organization and should evaluate whether such errors will affect the nature, timing, and extent of his or her audit procedures. In certain instances, the plan auditor may need to obtain additional information to make this evaluation and should consider contacting the service organization and the service auditor to obtain the necessary information.

6.12 For a limited-scope audit, the auditor has no responsibility to obtain an understanding of the controls maintained by the certifying institution over assets held and investment transactions executed by the institution. Therefore in a limited-scope engagement, to the extent that the service organization is only providing investment transaction services, no SAS No. 70 report is required. However, if the provider is also providing services such as the processing of participant level transactions, a SAS No. 70 report generally should be obtained, if it is available and covers these activities.

6.13 When the administrator elects a full scope audit, even though a limited scope audit could be performed (see paragraphs 5.02 and 13.26 through 13.32 for a discussion of limited scope audits), or where the trustee or custodian does not qualify for the limited scope audit exemption, the auditor may need to obtain an understanding of controls at the trustee or custodian. A similar understanding may be required for information processed by the trustee or custodian related to financial statement components not subject to the limited scope audit exemption, for example, benefit claims or payments. As previously noted, this understanding can be efficiently achieved by obtaining and reading the entire SAS No. 70 document for the service organization. In determining whether a SAS No. 70 report would be useful, the auditor should consider (1) the nature and materiality of the transactions the service organization processes for the user organization, and (2) the degree of interaction between the service organization’s activities and those of the user organization. The plan auditor should read the description of controls to determine whether complementary user organization controls are required and whether they are relevant to the service provided to the plan. If they are relevant to the plan, the plan auditor should consider such information in planning the audit. See Exhibit B-2, Examples of User Controls When a Service Organization is Utilized, in appendix B of this guide for examples of user controls.

6.14 Service providers are not required to furnish SAS No. 70 reports. If a SAS No. 70 report is not available, information about the nature of the services provided by the service organization that are part of the user organization’s information system and the service organization’s controls over those services may be available from a wide variety of sources, such as user manuals, system overviews, technical manuals, the contract between the user organization and the service organization, and reports by internal auditors, or regulatory authorities on the service organization’s controls. If the services and the service organization’s
controls over those services are highly standardized, information obtained through the user auditor’s prior experience with the service organization may be helpful in planning the audit. The user auditor may consider utilizing the specific control objectives and selected controls provided in Exhibit B-1 of appendix B of this guide in obtaining this understanding. If the user auditor concludes that the available information is not adequate to obtain a sufficient understanding of the service organization’s controls to plan the audit, consideration should be given to contacting the service organization through the user organization, to obtain information or request that a service auditor be engaged to perform procedures at the service organization. If the user auditor is unable to obtain sufficient evidence to achieve the audit objectives, the user auditor should qualify the audit opinion or disclaim an opinion on the financial statements because of a scope limitation. (Historically, the DOL has rejected Form 5500 filings that contain either qualified opinions, adverse opinions or disclaimers of opinion on plan financial statements other than those issued in connection with a limited scope audit pursuant to 29 CFR 2520.103-8 or 12.)

6.15 A report prepared in accordance with SAS No. 70, as amended, for the service organization, for use by auditors of financial statements of employee benefit plans, will typically address in that report the control objectives that are relevant to the specific objectives of employee benefit plans as set forth in Exhibit B-1.

6.16 With the trend toward daily valuation of 401(k) plans, more benefit plans are using service providers to initiate, execute and perform the accounting processing of transactions on behalf of the plan administrator. Oftentimes the plan does not maintain independent accounting records of such transactions. For example, many plan sponsors no longer maintain participant enrollment forms detailing the contribution percentage and the investment fund allocation option. In these situations, the auditor may not be able to obtain a sufficient understanding of internal control relevant to such transactions to plan the audit and to determine the nature, timing, and extent of testing to be performed without considering those components of internal control maintained by the service organization. This understanding can be efficiently achieved by obtaining and reading the entire document prepared in accordance with SAS No. 70 for the service organization. SAS No. 70 reports generally cover the relevant operations of a service organization; however, certain operations of the service organization may not be addressed in the SAS No. 70 report, and those operations may be significant to the plan audit. In these instances, the engagement team will need to obtain an understanding of the controls in the relevant areas excluded from the scope of the SAS No. 70 report. In some cases, a provider may choose to engage an auditor to prepare a SAS No. 70 report on a rotating basis instead of annually. A report on controls placed in operation that is as of a date outside the plan’s reporting period may be useful in providing the plan auditor with a preliminary understanding of the controls placed in operation at the service organization if the report is supplemented by additional current information. If this occurs, the engagement team should contact the service organization and discuss with them any system changes, major changes in controls, or mergers/acquisitions that occurred during the year. If these changes have occurred, the engagement team should obtain an understanding of the changes and consider the effect of the changes on the audit. If the SAS No. 70 report is unavailable, the auditor should consider other appropriate procedures to obtain sufficient evidence to achieve the audit objectives. For example, if participant enrollment forms are unavailable from the plan sponsor, the auditor may wish to confirm the information directly with the participants. Alternatively, the auditor could consider requesting the enrollment forms from the service provider or visiting the service provider to perform the necessary
testing. The service provider may be able to provide detailed transaction reports at the plan or participant level, such as telephone or electronic means transaction reports, trade batch reports, distribution summaries, loan ledgers or details of purchases, sales and dividends posted to individual accounts.

6.17 If the independent auditor determines that the service organization had effective controls in place for processing plan transactions during the reporting period, the auditor generally would conclude that it is not necessary to visit or perform additional procedures at the service organization. However, in some situations, the auditor may conclude that additional audit work should be performed at the service organization. Following are some examples of those situations:

a. **The service organization issued a SAS No. 70 report describing the controls placed in operation ("Type 1" report) and the auditor wishes to determine whether to reduce the assessed level of control risk at the service organization**—The plan auditor should determine whether it is more efficient to attempt to reduce the assessed level of control risk for the assertions affected by the services performed at the service organization that are part of the plan’s information system, or to perform additional audit procedures on the plan’s financial statements. If the plan auditor decides it is more efficient to assess the operating effectiveness of the service organization’s controls placed in operation, tests of the service organization’s controls should be performed, most likely at the service organization.

b. **The service organization’s SAS No. 70 report covers a different reporting period than the plan’s fiscal year**—The plan auditor should make inquiries of the service organization or its auditor to determine whether there were changes in the service organization’s controls during the period not covered by the SAS No. 70 report. If the period not covered is significant, or there have been changes in the controls, the auditor should gain an understanding of the service organization’s controls relating to the plan’s transactions during the period not covered by the SAS No. 70 report.

c. **The service organization’s SAS No. 70 report covers only some of the services used by the plan (for example, the report might cover custodial services but not allocation services) or the report does not cover activities performed by subservice organizations**—The plan auditor should gain an understanding of the controls related to the services not covered in the SAS No. 70 report as they relate to the plan’s transactions processed by the service organization that are part of the plan’s information system. If the user auditor does not have sufficient information to assess control risk below the maximum, the plan auditor may decide to perform additional tests of the service organization’s controls or perform additional audit procedures on the plan’s financial statements. The plan auditor also should obtain a copy of the subservice organization’s SAS No. 70 report, if one was issued. Additionally, a service organization may use another service organization to perform functions or processing that is part of the plan’s information system as it relates to an audit of the financial statements. The subservice organization may be a separate entity from the service organization or may be related to the service organization. To plan the audit and assess control risk, the plan auditor may need to consider controls at the service organization and also may need to consider controls at the subservice organization, depending on the functions each performs. The following illustrates typical subservicing situations in a bank trust department that provides services to an employee benefit plan.

1. **Limited functions.** A bank trust department may use one or more pricing service organizations to determine the current market price of exchange-traded securities held by the plan.
Appendix A: Excerpts from Audit and Accounting Guide Employee Benefit Plans

(2) **Moderate functions.** A bank trust department may use a data processing service organization to record the transactions and maintain the related accounting records for the plan.

(3) **Extensive functions.** A bank trust department may use a service organization to perform essentially all of the transaction execution, recording, and processing for the plan.

The plan auditor should consider the effect of the subservice organization on the internal control of the plan as follows:

1. The degree of interaction, as well as the nature and materiality of the transactions processed by the service organization and the subservice organization.

2. The available information about the service organization's and subservice organization's controls, including (1) information in the plan management's possession, such as user manuals, system overviews, technical manuals, and the contract between the plan and the service organization; and (2) reports on the service organization's and subservice organization's controls, such as reports by service auditors, internal auditors, or regulatory authorities. Because a plan typically does not have any contractual relationship with the subservice organization, the plan should obtain available reports and information about the subservice organization from the service organization.

After considering the above factors and evaluating available information, the plan auditor may conclude that he or she has the means to obtain sufficient understanding of a user organization's internal control to plan the audit. If the user auditor concludes that information is not available to obtain a sufficient understanding to plan the audit, he or she may consider contacting the service organization through the user organization or contacting the subservice organization, through the user and service organizations, to obtain specific information or request that a service auditor be engaged to perform procedures that will supply the necessary information. Alternatively, the user auditor may visit the service organization or subservice organization and perform such procedures. (For further guidance on the use of subservice organizations, see chapter 5 in the AICPA Audit Guide *Service Organizations: Applying SAS No. 70, as Amended.*)

6.18 It is not uncommon for a Type II SAS No. 70 Report to have exceptions in tests of operating effectiveness. Those exceptions may result in a qualification of the report. Auditors should consider the following when a SAS No. 70 report contains exceptions to determine if an expansion of the scope of detailed testing is required:

- Whether the exception is related to user organization activities.

- The nature of the exception based on details provided in the SAS No. 70 report and inquiries of the user organization personnel and/or the service auditor.

- Whether any follow-up procedures and additional testing has been performed by the user organization or service organization to address the exception.

- Whether compensating controls exist that would mitigate the effect of the exception.

An auditor should consider whether they are able to rely on controls at the service organization if there are exceptions noted in the SAS No. 70 report.
6.19 A SAS No. 70 report may be qualified for the following reasons:

- The service organization’s controls are not correctly described.
- Controls were not suitably designed to achieve the specified control objectives.
- The controls that were tested were not operating effectively (exceptions in testing).

Auditors should consider the following when a SAS No. 70 report is qualified to determine if an expansion of the scope of detailed testing is required:

- Whether the qualification is related to user organization activities.
- The nature of the qualification based on details provided in the SAS No. 70 report and inquiries of the user organization personnel and/or the service auditor.
- Whether any follow-up procedures and additional testing has been performed by the user organization or the service organization to address the reason for the qualification.
- Whether compensating controls exist that would mitigate the effect of the qualification.

An auditor should determine whether or not they can rely on a qualified SAS No. 70 report.
This appendix provides illustrative control objectives for the service organizations most likely to be used by an employee benefit plan. This material originally appeared in Appendix E, “Illustrative Control Objectives for Various Types of Service Organizations,” of the AICPA Audit Guide Service Organizations: Applying SAS No. 70.

**SEcurities Custodian and ServiCer**

The control objectives in this section would be appropriate for a securities holder (custodian) and servicer that performs some or all of the following functions:

- Maintaining custody of securities and records of the securities held for the entities (Such securities may exist in physical or electronic form.)
- Collecting dividend and interest income and distributing such income to the entities
- Receiving notification of corporate actions and reflecting such actions in the records of entities
- Receiving notification of security purchase and sale transactions on behalf of entities for which the custodian is holding securities, and reflecting such transactions in the records of the entities
- Receiving payments from purchasers and disbursing proceeds to sellers for security purchase and sale transactions

**Illustrative Control Objectives for a Securities Custodian and Servicer**

Controls provide reasonable assurance that:

- Changes to nonmonetary participant data (for example, address changes and changes in allocation instructions) are authorized and correctly recorded on a timely basis.
- Trades are authorized, recorded, settled, and reported completely, accurately, and timely and in accordance with the client agreement.
- Investment income is collected and recorded accurately and timely.
- Corporate actions are identified, processed, settled, and recorded accurately and timely.
- The market values of securities are calculated based on market prices obtained from authorized pricing sources.
- Cash receipts and disbursements are authorized, processed, and recorded completely, accurately, and timely.
Physically-held securities are protected from loss, misappropriation, and unauthorized use.

The entity’s records accurately reflect securities held by third parties, for example, depositories or subcustodians.

Lender and borrower participation in lending programs is authorized.

Loan initiation, processing, maintenance, and termination are recorded accurately and timely.

Loans are adequately collateralized, and collateral is recorded timely and accurately.

Collateral is invested in accordance with the lender agreement and income is calculated and distributed accurately and timely.

**PARTICIPANT RECORDKEEPER FOR DEFINED CONTRIBUTION PLANS**

The illustrative control objectives included in this section would be appropriate for a participant recordkeeper for defined contribution plans that perform some or all of the following functions.

- Maintaining records of participant and employer contributions, disbursements, and account balances based on information received from the plan sponsor, participant, mutual fund investment adviser, transfer agent, custodian and others.

- Receiving instructions from participants and plan sponsors regarding investment elections, distributions, loans, hirings, terminations, and other matters, and communicating these instructions to other service organizations, such as transfer agents and custodians responsible for executing these instructions.

- Performing valuations of participant accounts and transactions.

- Periodic reporting to participants and plan sponsors.

**Illustrative Control Objectives for Participant Recordkeepers for Defined-Contribution Plans**

Controls provide reasonable assurance that:

- New accounts are properly established in the system in accordance with the plan agreement and individual elections.

- Changes to nonmonetary participant data (for example, address changes and changes in allocation instructions) are authorized and correctly recorded on a timely basis.

- Cash receipt transactions, loans, distributions of plan assets, and transactions reflecting a transfer of participants’ funds among investment options are recorded accurately, timely, and in accordance with instructions received from plan sponsors or participants.
• Investment income (loss) is accurately and timely allocated and recorded to individual participant accounts.

• Transactions and participant account balances are valued based on market prices obtained from authorized pricing sources.

• Participant transaction confirmations, and participant account statements, are accurate, distributed timely, and mailed directly to participants without intervention by individuals responsible for processing transactions.