1996

# Implementing SAS no. 70 : reports on the processing of transactions by service organizations; Auditing procedure study;

American Institute of Certified Public Accountants

Auditing
Procedure
Study

# Implementing SAS No. 70, *Reports on the Processing of Transactions by Service Organizations*

AICPA

American Institute of Certified Public Accountants

Implementing SAS No. 70

AICPA

## Statement of Policy

Auditing Procedure Studies are issued by the Auditing Standards Division. Each study is designed to inform auditors of developments and advances in auditing procedures. The studies express the views of the author or study group.

This Auditing Procedure Study has not been approved, disapproved, or otherwise acted on by the Auditing Standards Board, the membership, or the governing body of the American Institute of Certified Public Accountants. Therefore, the contents of this study, including recommendations, are not authoritative.

# Implementing SAS No. 70, *Reports on the Processing of Transactions by Service Organizations*

American Institute of Certified Public Accountants

**Library of Congress Cataloging-in-Publication Data**

Implementing SAS no. 70: reports on the processing of transactions by service organizations / AICPA, American Institute of Certified Public Accountants.
p. cm. — (Auditing procedure study)
ISBN 0–87051–174–2
1. Auditor's reports—United States. 2. Accounting—Standards—United States. 3. Financial statements—United States. 4. Service industries—United States—Accounting. I. American Institute of Certified Public Accountants. II. Series.
HF5667.6.I56 1996
657'.45—dc20 95–49705
CIP



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

# Contents

# Foreword

This Auditing Procedure Study (APS) provides guidance to service auditors engaged to issue reports on the control structure policies and procedures of service organizations. It also provides guidance to user auditors engaged to audit the financial statements of entities that use service organizations.

This APS does not incorporate the guidance in Statement on Auditing Standards (SAS) No. 78, *Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55.* SAS No. 78 revises the definition and description of internal control contained in SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit,* to recognize the definition and description contained in *Internal Control-Integrated Framework* published by the Committee of Sponsoring Organizations of the Treadway Commission. Conforming changes will be made in the next edition of this APS.

This APS is part of the Auditing Procedure Study series issued by the American Institute of Certified Public Accountants (AICPA) and was prepared by the following task force of the Auditing Standards Board:

George H. Tucker, Chair
Michael Henitz
Susan E. Kenney
William Levant
Andrew E. Nolan
Patrick H. Scott

Dan M. Guy
Vice President, Professional
Standards and Services
Judith M. Sherinsky
Technical Manager
Auditing Standards

# Introduction

## WHY ENTITIES USE SERVICE ORGANIZATIONS

Many entities use outside service organizations to perform tasks requiring specialized knowledge, skills, or equipment. Service organizations may provide services ranging from performing a specific task under the direction of an entity to replacing entire business units or functions of an entity. Entities generally use service organizations because the expertise or ability to perform certain services does not exist within the entity or because it may be cost effective to outsource the service.

## THE EFFECT OF A SERVICE ORGANIZATION ON THE AUDIT OF A USER ORGANIZATION'S FINANCIAL STATEMENTS

When an entity (a user organization) employs a service organization, the functions or processing performed by the service organization may affect the internal control structure of the user organization and, consequently, may affect the independent auditor's planning and performance of the audit of the user organization's financial statements. An auditor may be engaged to issue a report on the control structure policies and procedures of a service organization for use by user organizations and their auditors. Statement on Auditing Standards (SAS) No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, *Professional Standards,* vol. 1, AU sec. 324), provides guidance (1) to auditors performing an audit of a user organization's financial statements, and (2) to auditors performing procedures at a service organization that will enable them to report on the control structure policies and procedures at the service organization that may affect user organizations. Although a service auditor's report may be used by other interested parties, its primary purpose is to provide information to auditors of user organizations. The purpose of this Auditing Procedure Study (APS) is to provide guidance on the implementation of SAS No. 70 to auditors of entities that use service organizations (user auditors) and to auditors issuing reports on the control structure policies and procedures of service organizations (service auditors).

## DEFINITIONS

Readers of this APS should be familiar with the following terms, which are defined in SAS No. 70.

- *User organization.* The entity that has engaged a service organization and whose financial statements are being audited.
- *User auditor.* The auditor who reports on the financial statements of the user organization.
- *Service organization.* The entity (or segment of an entity) that provides services to the user organization.
- *Service auditor.* The auditor who reports on the processing of transactions by a service organization.

The concept of an entity's internal control structure is fundamental to SAS No. 70 and is defined in SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 319). An entity's internal control structure consists of the policies and procedures the entity establishes to provide reasonable assurance that specific entity objectives will be achieved. An entity's internal control structure consists of its control environment, accounting system, and control procedures. SAS No. 70 and this APS use the term *control structure policies and procedures* to refer to policies and procedures at a service organization that may affect a user organization's internal control structure and the assertions in its financial statements.

## EXAMPLES OF SERVICE ORGANIZATIONS

SAS No. 55 requires the auditor to obtain a sufficient understanding of an entity's internal control structure to plan the audit. In certain situations, an entity's internal control structure is not limited to the policies and procedures in place within the entity's physical facility or operational control and instead extends beyond the entity. This can happen if an entity uses another organization to perform specialized services that affect the entity's ability to record, process, summarize, and report financial information in its financial statements. SAS No. 70 refers to these specialized organizations as service organizations. Some examples of service organizations are the following.

- *Trust departments of banks, insurance companies, and similar entities.* Service organizations, such as the trust department of a bank or an insurance company, may provide a wide range of services to various user organizations, such as employee benefit plans. This type of service organization could be given authority to make decisions about how a plan's assets are invested. It also may serve as custodian of the plan's assets, maintain records of each participant's account, allocate investment income to the participants based on a formula in the trust agreement, make distributions to the partici-

pants, and prepare filings for the plan, such as Form 5500, "Internal Revenue Service Annual Return/Report of Employee Benefit Plan." If an employee benefit plan chooses to have a service organization perform some or all of these tasks, the service organization might be executing, recording, and maintaining the accountability for a portion of the plan's transactions that could have a material effect on the plan's financial statements.

- *Data processing service organizations.* Data processing service organizations also offer a wide range of services to user organizations. They may provide standardized services, such as entering a client's manually recorded data and processing it with software that produces computer-generated journals, a general ledger, and financial statements; or they may design and execute customized applications. They may specialize in a particular application, such as payroll or inventory, or in a particular industry, such as securities brokerage or banking. The data processing performed by these service organizations may have a significant effect on the financial statement assertions of user organizations.
- *Insurers that maintain the accounting for ceded reinsurance.* Reinsurance is the assumption by one insurer (the assuming company) of all or part of the risk originally undertaken by another insurer (the ceding company). Generally, the ceding company retains responsibility for claims processing and is reimbursed by the assuming company for claims paid. As noted in the AICPA Audit and Accounting Guide *Audits of Property and Liability Insurance Companies,* the assuming company should establish controls over the accuracy and reliability of data received from the ceding company. The auditor of the assuming company's financial statements should obtain an understanding of the assuming company's procedures for assessing the accuracy and reliability of the data received from the ceding company. As part of that process, the auditor of the assuming company's financial statements may wish to obtain a service auditor's report on the ceding company's controls over the processing of ceded reinsurance claims.
- *Mortgage servicers or depository institutions that service loans for others.* Investor organizations may purchase mortgage loans or participation interests in such loans from thrifts, banks, or mortgage companies. The loans become assets of the investor organizations, but the sellers continue to service the loans. Mortgage servicing activities generally consist of collecting mortgage payments from borrowers, conducting collection and foreclosure activities, maintaining escrow accounts for the payment of property taxes and insurance, paying taxing authorities and insurance companies as payments become due, remitting monies to investors (user organizations), and reporting data concerning the mortgage to user organizations. The user organization may have little or no contact with the mortgage servicer other than the monthly payments sent to the

mortgage servicer and reports received from the mortgage servicer. The user organization records transactions related to the underlying mortgage loans based on data provided by the mortgage servicer. Auditors of the financial statements of mortgage investors may obtain information from a service auditor's report on the control structure policies and procedures related to the servicing of mortgages.

- *Value-Added Networks (VANs).* Organizations may agree to electronically send transactions to and receive transactions from each other as trading partners (that is, user organizations). Trading partners participating in electronic data interchange (EDI) frequently use VANs which function like mailboxes — storing and accumulating transactions. At various times, trading partners electronically transmit transactions to the VAN or receive electronic transmissions from the VAN. VANs provide protocol conversion to enable trading partners that use different communication standards to communicate with each other. They also provide a level of security by validating trading partners' user identification numbers and passwords. A user organization may use a VAN for a significant volume and dollar amount of transactions that are reflected in the user organization's financial statements. A service auditor's report on the VAN may be useful to auditors of the trading partners' financial statements because it may provide information about the controls over the completeness and accuracy of the transaction processing between the trading partners.

The list of service organizations presented above is not intended to be a comprehensive list; other types of entities may also function as service organizations.

Chapter 1

# Audit Considerations If an Entity Uses a Service Organization

*This chapter identifies the information a user auditor may need to obtain about the processing performed by a service organization for a user organization and also describes how a user auditor obtains that information.*

## APPLYING SAS NO. 55 TO THE AUDIT OF A USER ORGANIZATION'S FINANCIAL STATEMENTS

SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 319), states that an entity's internal control structure consists of the three following elements:

- The control environment
- The accounting system
- The control procedures

In all audits of financial statements, the auditor should obtain a sufficient understanding of each of these elements to plan the audit. After obtaining this understanding, the auditor should assess control risk for the assertions embodied in the account balances, transaction classes, and disclosure components of the financial statements. The auditor may assess control risk at the maximum level because he or she believes policies and procedures are unlikely to pertain to an assertion, are unlikely to be effective, or because evaluating their effectiveness would be inefficient. Alternatively, the auditor may obtain evidential matter about the effectiveness of both the design and operation of a policy or procedure that supports a lower assessed level of control risk. SAS No. 55 defines tests of controls as tests performed to assess the design or operating effectiveness of internal control structure policies and procedures. Evidential matter about the operating effectiveness of policies and procedures may be obtained from tests of controls

specifically planned and performed for this purpose, or from procedures performed to obtain an understanding of the internal control structure, which, nevertheless, provide evidential matter about the operating effectiveness of the controls. Either while or after obtaining this understanding and assessing control risk, the auditor may seek a further reduction in the assessed level of control risk for certain assertions. In such cases, the auditor should consider whether evidential matter sufficient to support a further reduction in the assessed level of control risk is likely to be available and whether performing additional tests of controls to obtain such evidential matter will be efficient. If so, the auditor performs additional tests of controls to obtain evidence that the controls are operating effectively. The auditor uses his or her understanding of the internal control structure and assessed level of control risk to determine the nature, timing, and extent of the substantive tests required for financial statement assertions.

If an organization uses a service organization, transactions that affect the user organization's financial statements are subjected to policies and procedures that may be physically and operationally apart from the user organization. Consequently, the internal control structure of a user organization may include a component that is not directly under the control and monitoring of the user organization's management. For this reason, planning the audit may require a user auditor to gain an understanding of the control structure policies and procedures at the service organization that may affect the user organization's financial statements. This understanding may be gained in several ways, including obtaining a service auditor's report. The fact that an entity uses a service organization is not, in and of itself, a compelling reason for a user auditor to conclude that it is necessary to obtain a service auditor's report to plan the audit. Factors to consider in determining whether a user auditor should obtain a service auditor's report are presented in the following section.

## THE EFFECT OF A SERVICE ORGANIZATION ON A USER ORGANIZATION'S INTERNAL CONTROL STRUCTURE AND PLANNING THE AUDIT OF A USER ORGANIZATION'S FINANCIAL STATEMENTS[1]

When planning the audit of a user organization's financial statements, a user auditor should determine the significance of the control structure policies and procedures at the service organization to the internal control structure of the user organization. If the user auditor determines that the control structure policies and procedures at the service organization are

1. Refer to paragraphs 6 through 10 of SAS No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, *Professional Standards*, vol.1, AU sec. 324), for guidance on the effect of a service organiztion on a user organization's internal control structure and planning the audit of a user organization's financial statements.

significant to the user organization's internal control structure, the user auditor should gain a sufficient understanding of those policies and procedures to plan the audit, as required by SAS No. 55. Several factors may affect the significance of a service organization's control structure policies and procedures to a user organization's internal control structure. The most important factors are the following.

- *The nature and materiality of the transactions or accounts affected by the service organization.* If the transactions processed or accounts affected by the service organization are material to the user organization's financial statements, the user auditor may need to obtain an understanding of the control structure policies and procedures at the service organization. In certain situations, the transactions processed and the accounts affected by the service organization may not appear to be material to the user organization's financial statements, but the nature of the transactions processed may require the user auditor to obtain an understanding of those policies and procedures. For example, consider a situation in which a service organization provides third-party administration services to self-insured organizations providing health benefits to employees. Although transactions processed and accounts affected may not appear to be material to the user organization's financial statements, the user auditor may need to gain an understanding of the control structure policies and procedures at the third-party administrator because improper processing may result in a material understatement of the liability for unpaid claims.
- *The degree of interaction between the internal control structure policies and procedures of the user organization and the policies and procedures of the service organization.* The degree of interaction refers to the extent to which a user organization is able to and elects to implement effective internal control structure policies and procedures over the processing performed by the service organization.

The degree of interaction depends primarily on the nature of the services provided by the service organization. If the services provided by the service organization are limited to recording user organization transactions and processing the related data, and the user organization retains responsibility for authorizing the transactions and maintaining the related accountability, there will be a high degree of interaction. For example, consider a situation in which an employee benefit plan uses the trust department of a bank to invest and maintain custody of its assets in a *directed* trust. In a directed trust, the employee benefit plan instructs the bank trust department to execute specific transactions, such as the purchase and sale of securities. The trust department may not act without specific authorization from the employee benefit plan. Under such an arrangement, the employee benefit plan is able to independently generate records of its investment activities to be used for the preparation of financial statements, and is also

able to independently reconcile its records to information received from the bank trust department. If the employee benefit plan retains responsibility for authorizing the transactions and for maintaining the related accountability by independently generating and maintaining records and reconciling them to information provided by the bank trust department, there will be a high degree of interaction. However, if the employee benefit plan authorizes the transactions but does not generate and maintain independent records of its investment activities, and record its investment activities solely from information generated by the bank trust department, there will be a lower degree of interaction between the internal control structure policies and procedures of the user organization and the control structure policies and procedures of the service organization.

Alternatively, consider another situation in which an employee benefit plan establishes a *discretionary* trust rather than a directed trust. In a discretionary trust, the bank trust department is given discretionary authority to invest the plan's assets. The trust department is authorized to initiate and execute transactions without prior authorization of each transaction by the employee benefit plan. Under this arrangement, the employee benefit plan must record investment activities from information provided by the trust department because the employee benefit plan has no means of independently generating a record of its transactions. In such a situation, there will be a lower degree of interaction between the internal control structure policies and procedures of the user organization and the control structure policies and procedures of the service organization.

If an auditor is auditing financial statements that contain material assertions derived from a service organization's recordkeeping, and the user organization is unable to, or elects not to, implement effective internal control structure policies and procedures over the processing performed by the service organization (there is a low degree of interaction), the auditor generally will need to obtain an understanding of the control structure policies and procedures at the service organization that affect those transactions.

Paragraph 8 of SAS No. 70 states that the service auditor should consider the following factors in determining the significance of the service organization's policies, procedures, and records to planning the audit.

- The significance of the financial statement assertions that are affected by the policies and procedures of the service organization
- The inherent risk associated with the assertions affected by the policies and procedures of the service organization
- The nature of the services provided by the service organization and whether they are highly standardized and used extensively by many user organizations or unique and used only by a few
- The extent to which the user organization's internal control structure policies and procedures interact with the policies and procedures of the service organization

- The user organization's internal control structure policies and procedures that are applied to the transactions affected by the service organization's activities
- The terms of the contract between the user organization and the service organization (for example, their respective responsibilities and the extent of the service organization's discretion to initiate transactions)
- The service organization's capabilities, including its —
  - Record of performance
  - Insurance coverage
  - Financial stability
- The user auditor's prior experience with the service organization
- The extent of the auditable data in the user organization's possession
- The existence of specific regulatory requirements that may dictate the application of audit procedures beyond those required to comply with generally accepted auditing standards (GAAS)

If a user auditor determines that the control structure policies and procedures at the service organization are significant to the internal control structure of the user organization, the user auditor should gain an understanding of the control structure policies and procedures. That understanding should include —

- Features of the service organization's control environment that affect the service provided to the user organization.
- Specific activities that may represent the user organization's accounting system, for example, the flow of transactions through the service organization.

Such knowledge should be used to —

- Identify the types of potential misstatements that could occur in the user organization's financial statement assertions affected by the service provided.
- Consider the factors that affect the risk of material misstatement.
- Design substantive tests.

## SOURCES OF INFORMATION ABOUT A SERVICE ORGANIZATION

A user auditor should determine whether a service auditor's report is available from the service organization. Chapter 3 of this APS, "Using Type 1 and Type 2 Reports," provides guidance on using such a report. A user auditor should also consider information available at the user organization about the control structure policies and procedure at the service organiza-

tion, such as user manuals, system overviews, technical manuals, and reports from the service or user organization's internal auditors. If the user auditor concludes that information is not available to obtain a sufficient understanding of the internal control structure to plan the audit, he or she may consider contacting the service organization, through the user organization, to obtain information or request that a service auditor be engaged to perform procedures that will supply the necessary information. The user auditor may also visit the service organization and perform procedures there, if the service organization agrees to such an arrangement. If the user auditor is unable to obtain sufficient evidence to achieve his or her audit objectives, the user auditor should qualify his or her opinion or disclaim an opinion on the financial statements because of a scope limitation.

## THE USER AUDITOR'S ASSESSMENT OF CONTROL RISK[2]

After obtaining an understanding of the internal control structure, the user auditor should assess control risk for the assertions in the user organization's financial statements, including the assertions affected by the service organization. In doing so, the user auditor may identify certain internal control structure policies and procedures that, if operating effectively, would permit the user auditor to assess control risk below the maximum for assertions affected by the service organization. In certain situations, those policies and procedures may be implemented at the user organization. For example, an organization using a payroll service organization could compare the data submitted to the service organization with reports or information received from the service organization. The user organization could also recompute a sample of the payroll amounts for clerical accuracy and could review the total amount of the payroll for reasonableness. If a user auditor determines that such internal control structure procedures are operating effectively to prevent or detect material misstatements in the user organization's financial statements, the user auditor may be able to assess control risk below the maximum for the assertions affected by the service organization, without identifying and testing control structure policies and procedures at the service organization.

In other situations, control structure policies and procedures may be implemented at the service organization. If they are operating effectively, either by themselves or in concert with policies and procedures at the user organization, they may support an assessed level of control risk below the maximum. For example, a service organization may implement a control procedure requiring that all program changes be tested and approved by a quality assurance group at the service organization prior to being placed into the production environment. Similarly, a trust department may implement a control procedure requiring that internal records concerning secu-

2. Refer to paragraphs 11 through 16 of SAS No. 70 for guidance on assessing control risk at the user organization.

rities held by an outside custodian be periodically reconciled to information provided by the custodian.

Generally, a user auditor identifies relevant service organization control structure policies and procedures by reading a description of the service organization's policies and procedures. Information about the effectiveness of such policies and procedures may be obtained from such a report *if* the report includes tests of operating effectiveness. If the service auditor's report does not include tests of operating effectiveness, the user auditor may contact the service organization, through the user organization, to request that a service auditor be engaged to perform agreed-upon procedures that will test the operating effectiveness of those controls. The user auditor also may visit the service organization and perform procedures at the service organization if the service organization agrees to such an arrangement. In all cases, the user auditor's assessments regarding financial statement assertions are based on the combined evidence provided by the service auditor's report and the user auditor's own procedures.

## OTHER TYPES OF INTERNAL CONTROL ENGAGEMENTS

In addition to SAS No. 70, the following professional standards provide guidance to practitioners who (1) report on aspects of an entity's internal control structure or (2) are required to identify and report certain conditions related to an entity's internal control structure observed during an audit of the entity's financial statements. The objectives of these engagements differ from the objectives of a service auditor's engagement.

- *Statement on Standards for Attestation Engagements (SSAE) No. 2,* Reporting on an Entity's Internal Control Structure Over Financial Reporting (*AICPA,* Professional Standards, *vol. 1, AT sec. 400*). SSAE No. 2 provides guidance to practitioners engaged to examine and report on management's written assertion about the effectiveness of an entity's internal control structure over financial reporting. An entity's internal control structure over financial reporting includes those policies and procedures that pertain to an entity's ability to record, process, summarize, and report financial data consistent with the assertions embodied in its financial statements. In this type of engagement, the practitioner obtains an understanding of the internal control structure over financial reporting, tests and evaluates the design and operating effectiveness of the internal control structure, and expresses an opinion on whether management's assertion about the effectiveness of the entity's internal control structure over financial reporting is fairly stated in relation to identified criteria. Unlike a service auditor's report, which is designed to be used by a user auditor to plan an audit, it does not include a description of the control structure policies and procedures at a service organization or a description of tests of operating effectiveness and results of the tests. A report

issued under SSAE No. 2 is not intended to be used by a user auditor to plan the audit of a user organization.

- *SSAE No. 3,* Compliance Attestation (*AICPA,* Professional Standards, *vol. 1, AT sec. 500*). SSAE No. 3 provides guidance to a practitioner engaged to report on management's written assertion about either (1) an entity's compliance with requirements of specified laws, regulations, rules, contracts, or grants; or (2) the effectiveness of an entity's internal control structure over compliance with specified requirements. Unlike a service auditor's report, which is designed to be used by a user auditor to plan an audit, it does not include a description of the control structure policies and procedures at a service organization or a description of tests of operating effectiveness and results of the tests.
- *SAS No. 60,* Communication of Internal Control Structure Related Matters Noted in an Audit (*AICPA,* Professional Standards, *vol. 1, AU sec. 325*). As part of an audit of an entity's financial statements, an auditor may be required to issue an internal control communication in accordance with the requirements of SAS No. 60. SAS No. 60 does not apply to a service auditor's engagement because it provides guidance on identifying and communicating reportable conditions that come to an auditor's attention during the audit of an entity's financial statements, to an audit committee or to individuals with a level of authority and responsibility equivalent to an audit committee.

Chapter 2

# Form and Content of Reports on the Processing of Transactions By Service Organizations

*This chapter describes the two types of service auditor's engagements that a service auditor may perform and describes the reports that are issued for each engagement. It also identifies the sections in each report and describes the information that should be included in each section.*

## TYPES OF SERVICE AUDITORS' REPORTS

A service auditor may provide a service organization with two types of reports —

- A report on policies and procedures placed in operation, which will be referred to as a type 1 report in this Auditing Procedure Study (APS)
- A report on policies and procedures placed in operation and tests of operating effectiveness, which will be referred to as a type 2 report in this APS.

The type of engagement to be performed and the related report to be issued should be determined by the service organization. However, if circumstances permit, discussions between the management of the service organization and the management of the user organizations are advisable to determine the services or applications to be covered by the report and the type of engagement and related report that will be most useful to the user organizations and their auditors.

## FORMAT AND CONTENT OF TYPE 1 AND TYPE 2 PRESENTATIONS

Although the format of a type 1 or type 2 report is flexible, these reports will always contain the following information, ordinarily in the sections noted:

- Independent service auditor's report (section 1)
- Service organization's description of policies and procedures (section 2)

In addition, the following may also appear in both types of reports, ordinarily in the sections noted:

- Information provided by the independent service auditor (section 3): This section is always included in a type 2 report because the service auditor must describe the tests of operating effectiveness he or she has performed and the results of those tests. This section is optional in a type 1 report.
- Other information from the service organization (section 4): This section is optional in both type 1 and type 2 reports.

Throughout the remainder of this APS, the terms *type 1 report* and *type 2 report* will be used to refer to the entire document; that is, sections 1 and 2 and — if they are present — sections 3 and 4. The term *service auditor's report* will be used only to refer to section 1, which is the letter issued by the service auditor expressing an opinion on (1) the fairness of the presentation of the service organization's description of policies and procedures, (2) the suitability of the design of the policies and procedures to achieve specified control objectives, and, (3) in a type 2 engagement — whether the specified policies and procedures were operating with sufficient effectiveness to achieve the related control objectives.

Although the format of a type 1 or type 2 report is flexible, the organization and presentation of the reports should differentiate between (1) the service auditor's report (the letter issued by the service auditor), (2) the service organization's description of policies and procedures, (3) information provided by the service auditor, and (4) other information from the service organization. This is done to clearly indicate that —

- The service auditor is responsible for the representations in the service auditor's report (section 1) and for information provided by the service auditor (section 3).
- The service organization is responsible for the representations in the description of policies and procedures (section 2) and for other information from the service organization (section 4).

A service auditor's report (the letter issued by the service auditor) should *not* be distributed without the accompanying description of the ser-

vice organization's policies and procedures, and when applicable, the description of the service auditor's tests of operating effectiveness and the results of the tests.

## THE INDEPENDENT SERVICE AUDITOR'S REPORT

In a type 1 engagement, the service auditor issues a report on a description of policies and procedures that has been prepared by the service organization. The service auditor makes inquiries of appropriate management, supervisory, and staff personnel; inspects documents and records; and observes activities at the service organization to gather evidence needed to express an opinion on whether the —

- Description presents fairly, in all material respects, the relevant aspects of the service organization's policies and procedures that had been placed in operation as of a specified date.
- Policies and procedures were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those policies and procedures were complied with satisfactorily.

A type 1 report is intended to provide user auditors with information about the control structure policies and procedures at a service organization that may be relevant to a user organization's internal control structure. This information, in conjunction with other information about a user organization's internal control structure, should assist the user auditor in obtaining a sufficient understanding of the user organization's internal control structure to plan the audit, as described in paragraph 2 and paragraphs 16 through 26 of SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 319). The user auditor obtains this understanding to enable him or her to (1) identify the types of misstatements that may occur in a user organization's financial statements, (2) consider the factors that affect the risk of material misstatement, and (3) design substantive tests. *A type 1 report, however, is* not *intended to provide a user auditor with a basis for reducing his or her assessment of control risk below the maximum.* Paragraph 38 of SAS No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, *Professional Standards,* vol. 1, AU sec. 324) presents an example of a service auditor's report for a type 1 engagement.

In a type 2 engagement, the service auditor performs the procedures required for a type 1 engagement and also performs tests of specified control structure policies and procedures to evaluate their operating effectiveness in achieving specified control objectives. Tests of operating effectiveness address how policies and procedures are applied, how consistently they are applied, and who applies them. The service auditor issues a report that includes the type 1 report opinions and that refers readers to a description of tests of operating effectiveness performed by the service

auditor. The report states whether, in the opinion of the service auditor, the policies and procedures tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.

If policies and procedures of a service organization are operating with sufficient effectiveness to achieve related control objectives, the user auditor may be able to assess control risk below the maximum for certain financial statement assertions affected by the service organization's service or processing and, consequently, may be able to reduce the extent of substantive procedures performed for those assertions. To assess control risk below the maximum, a user auditor should consider the operating effectiveness of the relevant policies and procedures at the service organization in conjunction with the internal control structure policies and procedures at the user organization. In considering the operating effectiveness of the relevant control structure policies and procedures at the service organization, the user auditor should read and consider *both* the service auditor's —

- Report on the operating effectiveness of the control structure policies and procedures.
- Description of the tests of operating effectiveness of control structure policies and procedures that may be relevant to specified assertions in the user organization's financial statements, and the results of those tests.

*In no case, should the service auditor's report (the letter issued by the service auditor) 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 2 report may be used to reduce substantive procedures, neither a type 1 report nor a type 2 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. Paragraph 54 of SAS No. 70 presents an example of a service auditor's report for a type 2 engagement.

Table 2.1 summarizes the service auditor's opinions included in each type of service auditor's report.

## THE SERVICE ORGANIZATION'S DESCRIPTION OF POLICIES AND PROCEDURES

The service organization's description of policies and procedures is generally prepared by the service organization. The service organization is responsible for the completeness, accuracy, and method of presentation of the description. If the service auditor assists the service organization in

***Table 2.1***
**Service Auditor's Opinions Included in Type 1 and Type 2 Service Auditors' Reports**

| *Opinion* | *Type 1 Report* | *Type 2 Report* |
|---|---|---|
| (1) Whether the service organization's description of its policies and procedures presents fairly, in all material respects, the relevant aspects of the service organization's policies and procedures that have been placed in operation as of a specific date. | Included | Included |
| (2) Whether the policies and procedures were suitably designed to achieve specified control objectives. | Included | Included |
| (3) Whether the policies and procedures 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. | Not Included | Included |

preparing the description, the representations in the description remain the responsibility of the service organization. The description should provide user auditors with information about the service organization's control structure policies and procedures that may be relevant to the user organizations' internal control structures. Service organization control structure policies and procedures that would be considered relevant to user organizations' internal control structures are policies and procedures that directly affect the services provided to user organizations and that affect the user organizations' control environments, accounting systems, or control procedures, and consequently affect assertions in their financial statements.

The description of policies and procedures should be presented at a level of detail that provides user auditors with sufficient information for them to plan the audit as described in paragraphs 7 and 8 of SAS No. 70 and paragraphs 16 through 22 of SAS No. 55. The description need not address every aspect of the service organization's processing or the services provided to user organizations. Certain aspects of the processing or the services provided may not be relevant to user organizations and their auditors or may be beyond the scope of the engagement. For example, a data processing service organization that provides five different applications to user organizations may engage a service auditor to report on only three of those applications. Similarly, a trust department that has separate organizational units providing personal trust services and institutional trust services may engage a service auditor to report on only the institutional trust services. In these situations, the service organization's description should only address the control structure policies and procedures pertain-

ing to the applications or organizational units included in the scope of the engagement.

The service organization's description of policies and procedures generally should contain the following information:

- Features of the control environment that may affect the services provided to user organizations
- Policies and procedures that represent the user organization's accounting system, or a portion thereof
- Control objectives and related control structure policies and procedures

## Features of the Control Environment That May Affect the Services Provided to User Organizations

This section describes features of the service organization's control environment that may affect the services provided to user organizations. The control environment reflects the overall attitude, awareness, and actions of the service organization's board of directors, management, owners, and others concerning the importance of control and its emphasis in the entity. For example, management's hiring and training practices generally would be considered a control environment feature because they affect the quality of the personnel performing services for user organizations. Paragraph 9 of SAS No. 55 provides the following examples of control environment factors:

- Management's philosophy and operating style
- The entity's organizational structure
- The functioning of the board of directors and its committees, particularly the audit committee
- Methods of assigning authority and responsibility
- Management control methods for monitoring and following up on performance, including internal auditing
- Personnel policies and practices
- Various external influences that affect the entity's operations and practices, such as regulatory agencies

Only relevant control environment factors that affect the services provided to user organizations should be described in this section of the report. Ordinarily, control environment elements are not presented in the form of control objectives because of their nature; however, management is not precluded from presenting its control environment policies and procedures in the context of control objectives.

## Policies and Procedures That Represent the User Organization's Accounting System, or a Portion Thereof

Activities of the service organization that may represent the user organization's accounting system or a portion thereof include the methods and

records established by the service organization to identify, assemble, analyze, classify, record, and report a user organization's transactions.

Paragraph 21 of SAS No. 55 states that the auditor should obtain sufficient knowledge of the accounting system to understand —

- The classes of transactions in the entity's operations that are significant to the financial statements.
- How those transactions are initiated.
- The accounting records, supporting documents, machine-readable information, and specific accounts in the financial statements involved in the processing and reporting of transactions.
- The accounting processing involved from the initiation of a transaction to its inclusion in the financial statements, including how the computer is used to process data.
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.

The description of policies and procedures should provide sufficient information for user auditors to understand how the service organization's processing affects the elements listed above. The degree of detail presented should be equivalent to the degree of detail a user auditor would require if a service organization were not used. 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. This section also should indicate the extent of the manual and computer processing used.

## Control Objectives, Related Control Structure Policies and Procedures, and Assertions in User Organizations' Financial Statements

This section contains a discussion of the service organization's control objectives and how they relate to the service organization's control structure policies and procedures and assertions in the user organizations' financial statements.

The form and content of a service organization's control objectives are flexible and should be tailored to the service provided by the service organization. The control objectives help the user auditor determine how the service organization's control structure policies and procedures affect the user organization's financial statement assertions. SAS No. 31, *Evidential Matter* (AICPA, *Professional Standards*, vol. 1, AU sec. 326), states that assertions are representations by management that are embodied in financial statement components. They can be either explicit or implicit and can be classified according to the following broad categories:

- Existence or occurrence
- Completeness
- Rights and obligations
- Valuation or allocation
- Presentation and disclosure

Although the management of the service organization will not be able to determine how service organization control structure policies and procedures specifically relate to the assertions embodied in all the user organizations' financial statements, it should be able to identify the types of assertions to which its control structure policies and procedures are likely to relate. The service organization should establish control objectives (1) that it believes relate to those assertions, and (2) that provide a framework for user auditors to assess the effect of the service organization's control structure policies and procedures on those assertions. The following are examples of how a service organization's control objectives relate to assertions in a user organization's financial statements.

## Example 1

In the sample type 2 report for Example Computer Service Organization presented on page 71 of appendix A of this APS, the service organization provides computer services to user organizations in the financial services industry. Example Computer Service Organization has engaged a service auditor to report on its description of policies and procedures related to its savings, mortgage loan, and consumer loan applications. With respect to the savings application, the service organization maintains the detailed records of savings account balances and processes related transactions affecting those balances. It also calculates interest and penalty amounts and produces reports that are provided to user organizations for use in the preparation of their financial statements.

The service organization has established control objectives that it believes relate to assertions in the user organizations' financial statements. Table 2.2 indicates the control objectives established by the service organization and the kinds of assertions in the user organizations' financial statements to which they relate.

## Example 2

In the sample type 2 report for Example Trust Organization presented on page 103 of appendix A, the service organization provides fiduciary services to institutional, corporate, and personal trust customers. The Example Trust Organization has engaged a service auditor to report on its description of policies and procedures related to its processing of transactions for users of the institutional trust division. Example Trust Organization has discretionary authority over investment activities, maintains the detailed records of investment transactions, and records investment income and expense. Reports are provided to user organizations for use in the preparation of their financial statements.

***Table 2.2***

**Examples of Assertions in User Organizations' Financial Statements and Related Service Organization Control Objectives***

| *Assertions in User Organizations' Financial Statements* | *Control Objectives of the Service Organization* |
|---|---|
| | Control structure policies and procedures provide reasonable assurance that — |
| Existence or occurrence | Savings deposit and withdrawal transactions are received from authorized sources. |
| | Data maintained on files remain authorized, complete, and accurate. |
| Completeness | Savings deposit and withdrawal transactions received from the user organizations are initially recorded completely and accurately. |
| | Output data and documents are complete and accurate and distributed to authorized recipients on a timely basis. |
| Valuation or allocation | Programmed interest and penalties are calculated in conformity with the description. |
| | Output data and documents are complete and accurate and distributed to authorized recipients on a timely basis. |

**Source:* Sample type 2 report for Example Computer Service Organization presented on page 71 of appendix A.

The service organization has established control objectives that it believes relate to assertions in the user organizations' financial statements. Table 2.3 indicates the control objectives established by the service organization and the types of assertions in the user organizations' financial statements to which they relate.

The control objectives were specified by the management of Example Trust Organization who considered, among other things, the control objectives presented in appendix B of the AICPA Audit and Accounting Guide *Audits of Employee Benefits Plans*. Appendix B of that guide contains control objectives that are appropriate for an employee benefit plan. The set of control objectives established by Example Trust Organization is not identical to the set of control objectives presented in appendix B of the guide but is a subset of those control objectives, including only the objectives that relate to the processing performed by the service organization.

The examples of control objectives presented in the preceding tables are not intended to be comprehensive or to suggest specific control objectives. They illustrate how a user organization's financial statement assertions may relate to a service organization's control objectives. Frequently, a financial

*Table 2.3*
**Examples of Assertions in User Organizations' Financial Statements and Related Service Organization Control Objectives***

| *Assertions in User Organizations' Financial Statements* | *Control Objectives of the Service Organization* |
|---|---|
| | Control policies and procedures provide reasonable assurance that — |
| Completeness | Investment purchases and sales are recorded completely, accurately, and on a timely basis. |
| Valuation or allocation | Investment income is recorded at the appropriate amount and in the appropriate period. |
| Rights and obligations | Investment purchases and sales are recorded completely, accurately, and on a timely basis. |

**Source:* Sample type 2 report for Example Trust Organization presented on page 103 of appendix A.

statement assertion relates to more than one control objective, and a control objective relates to more than one financial statement assertion.

Although the control objectives are usually specified by the service organization, they may be designated by an outside party, such as a regulatory agency or a user group. If the control objectives are specified by the service organization, they should be reasonable in the circumstances and consistent with the service organization's contractual obligations. If the control objectives are specified by an outside party, the outside party is responsible for their completeness and reasonableness.

A service organization may design its service with the assumption that certain control structure policies and procedures will be implemented by the user organizations. If such user organization policies and procedures are necessary to achieve certain control objectives, the service organization should describe the user organizations' responsibilities for those policies and procedures in its description of policies and procedures. Refer to chapter 3 of this APS, "Using Type 1 and Type 2 Reports," for guidance to user auditors on complementary controls at user organizations and to chapter 4 of this APS, "Performing a Service Auditor's Engagement," for guidance to service auditors on complementary controls at user organizations.

Most service organizations are heavily dependent on computer processing to perform contracted services. Although the service organization may have manual control policies and procedures in place to ensure accurate and timely computer processing, the service organization's description of policies and procedures ordinarily should include a description of the computer environment and the related general computer controls, such as program change controls, controls that affect access to programs and data, and controls that affect the processing of data, because such information usually is significant to user auditors.

Although it is not necessary to evaluate a service organization's policies and procedures related to business continuity and contingency planning for the purpose of planning an audit or assessing control risk in an audit of financial statements, such information generally is of interest to the management of the user organizations. If the service organization wishes to describe its policies and procedures related to business continuity and contingency planning, such information may be included in either section 4, "Other Information Provided by the Service Organization," or section 2, "The Service Organization's Description of Policies and Procedures" of a type 1 or type 2 report.

## INFORMATION PROVIDED BY THE SERVICE AUDITOR

This section of a type 1 or type 2 report generally contains the following elements:

- A description of the tests of operating effectiveness of control structure policies and procedures and the results of those tests (This would only be included in a type 2 report.)
- Other information the service auditor may provide (This is an optional section in both type 1 and type 2 reports.)

### The Description of the Tests of Operating Effectiveness of Control Structure Policies and Procedures and the Results of Those Tests

Although the format of the description of the service auditor's procedures is flexible, it should provide an indication of the nature, timing, extent, and results of the tests performed. The description should include tests of the control environment elements as well as tests of other policies and procedures that relate to specific control objectives.

In preparing the description of the tests of operating effectiveness, the service auditor should consider the extent of detail user auditors will need to determine the effect of such tests on their assessments of control risk. The description need not be a duplication of the service auditor's detailed audit program, which in some cases would make the report too voluminous for user auditors and would provide more than the required level of detail. The description should, however, provide enough information for user auditors to determine whether control risk may be assessed below the maximum for certain financial statement assertions affected by the service organization's processing.

Although there is no single format for presenting a description of the tests of operating effectiveness, the following elements should be included in the description:

- The control structure policies and procedures that were tested
- The control objectives the policies and procedures were intended to achieve

- An indication of the nature, timing, extent, and results of the tests applied in sufficient detail to enable user auditors to determine the effect of such tests on their assessments of control risk (Detailed guidance about the content of this section is presented in chapter 4, and examples of descriptions of tests of operating effectiveness are presented on pages 40 through 47 of chapter 4 and in appendix A.

### Other Information the Service Auditor May Provide

In type 1 or type 2 reports, the service auditor may wish to provide other information that may be useful to user organizations and their auditors. This information would ordinarily be included in section 3 of a type 1 or type 2 report, "Information Provided by the Service Auditor." Such information might more fully describe the objectives of a service auditor's engagement or might provide information relating to regulatory requirements.

The service auditor also may wish to provide, in a separate communication to the service organization, recommendations for improving the service organization's control structure policies and procedures. However, if the service organization wishes, these recommendations may be included in this optional section of the report.

## OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

A service organization may wish to present other information in a separate section of a type 1 or type 2 report that is not a part of the description of policies and procedures and, consequently, is not covered by the service auditor's opinion. The service auditor should read such other information and consider the guidance in SAS No. 8, *Other Information in Documents Containing Audited Financial Statements* (AICPA, *Professional Standards,* vol. 1, AU sec. 550). Because this information is not a part of the description, the service auditor should include a paragraph in his or her report disclaiming an opinion on the other information provided by the service organization. Refer to page 54 of this APS for an example of such a disclaimer paragraph.

## ALTERNATIVE METHODS OF ORGANIZING TYPE 1 AND TYPE 2 REPORTS

The method of organizing a type 1 or type 2 report presented in this chapter (that is, using four sections) is not meant to be a rigid standard. Accordingly, service organizations and service auditors may choose to organize their reports in other ways. The sample report in example 1 of appendix A illustrates how this framework could be applied to a type 2 report using the four sections described in this chapter. Examples 2 and 3

of appendix A illustrate variations on the basic framework and are designed to eliminate redundancy in the reports, as described in the following paragraphs.

In applying the framework presented in this chapter to a type 2 report, it is not necessary to list the control structure policies and procedures and related control objectives in both the service organization's description of policies and procedures and in the service auditor's section of the report. To eliminate the redundancy that would result from repeating this information in both sections of the report, the Example Computer Service Organization type 2 report in example 2 of appendix A presents the control structure policies and procedures and related control objectives only in the service auditor's section of the report. The table of contents of the report directs the reader to the service auditor's section of the report for a description of the control objectives and control structure policies and procedures, and a paragraph in the service organization's description of policies and procedures indicates that the control objectives and related control structure policies and procedures presented in the service auditor's section are the responsibility of the service organization and should be considered a part of the service organization's description of policies and procedures.

In the Example Trust Organization type 2 report in example 3 of appendix A, the control objectives and control structure policies and procedures, along with the description of the tests of operating effectiveness, are presented in the service organization's section of the report. This is another method of presentation designed to avoid repetition of the control objectives and control structure policies and procedures in both the service organization's section and the service auditor's section. The service auditor's section of this report further describes the general nature of the types of tests performed.

## OTHER MATTERS

### Engagements Involving Subservice Organizations

Additional guidance on the form and content of a type 1 or type 2 report for situations in which a service organization uses another service organization (a subservice organization) to perform certain aspects of the processing performed for user organizations is presented in chapter 5 of this APS, "Service Organizations That Use Other Service Organizations."

### Certification of Computer Software

A type 2 report is not intended to be a certification that computer software functions as designed or as asserted by the management of the service organization, but rather to provide information about the effectiveness of the controls over the functioning of the software. For example, consider a situation in which a loan servicer uses a computer program to calculate interest. A type 1 or type 2 report would describe the control structure poli-

cies and procedures that have been designed to provide reasonable assurance that interest is calculated in conformity with the description, and a type 2 report would also provide information about the operating effectiveness of the tested controls. Such controls may be manual in nature (for example, recalculation of the interest accrual for a sample of loans) or automated (for example, controls embedded in the computer programs or controls over changes to and execution of the programs). The service auditor would identify and test the manual or automated controls to determine whether they provide reasonable assurance that interest is calculated in conformity with the description.

Chapter 3

# Using Type 1 and Type 2 Reports

*This chapter provides guidance to a user auditor on how and whether to use a given service auditor's report in an audit of a user organization's financial statements. It supplements paragraphs 18 through 21 of SAS No. 70,* Reports on the Processing of Transactions by Service Organizations *(AICPA,* Professional Standards, *vol. 1, AU sec. 324), by describing factors a user auditor should consider when using a type 1 or type 2 report to plan the audit of a user organization's financial statements.*

## DETERMINING WHETHER TO USE A GIVEN TYPE 1 OR TYPE 2 REPORT

In determining whether to use a given type 1 or type 2 report to plan the audit or to assess control risk, the user auditor should make inquiries about the professional reputation of the service auditor. Refer to paragraph 18 of SAS No. 70 for additional guidance in this area.

The user auditor should determine whether a type 1 or type 2 report will meet the user auditor's objectives. This topic is addressed in paragraph 19 of SAS No. 70. To make this determination, the user auditor should read the service auditor's report, the attached service organization's description of control structure policies and procedures, and the information provided by the service auditor, which may include a description of tests of operating effectiveness and other information. The service auditor's report on the service organization's description states whether the description is a fair presentation of that information; however, the report alone does not provide a user auditor with the understanding necessary to plan the audit.

In order for the user auditor to obtain a sufficient understanding of the user organization's internal control structure to plan the audit, he or she should consider the information provided in the type 1 or type 2 report, along with information about the user organization, to determine whether the user auditor has sufficient information to —

- Understand the aspects of the service organization's control environment that may be relevant to the processing of user transactions.

- Understand the flow of significant transactions through the service organization. (The user auditor should use this information, along with information obtained from the user organization, to determine the points in the transaction flow where material misstatements in the user organization's financial statements could occur.)
- Determine whether the control objectives are relevant to the user organization's financial statement assertions.
- Determine whether the service organization's control structure policies and procedures are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements.

The user auditor should also determine whether the service organization's description is as of a date that is appropriate for the user auditor's purposes.

For purposes of assessing control risk below the maximum, as described in paragraph 14 of SAS No. 70, the user auditor should determine whether—

- A type 2 report provides adequate evidence of the nature, timing, extent, and results of the tests of operating effectiveness for the user auditor to determine whether he or she may assess control risk below the maximum for financial statement assertions affected by the service organization's processing.
- The timing of the tests of operating effectiveness performed by the service auditor is appropriate for the user auditor's purposes.
- The service auditor's report identifies results of tests (exceptions or other information) that could affect the user auditor's considerations. (Exceptions noted by the service auditor or a report modification in the service auditor's report do not automatically mean that the service auditor's report will not be useful in planning the audit of a user organization's financial statements or in assessing control risk.)

If control structure policies and procedures at a service organization are operating effectively, the user auditor may be able to assess control risk below the maximum for certain financial statement assertions affected by the service organization's service or processing, and reduce the substantive procedures performed for those assertions. To assess control risk below the maximum, a user auditor should evaluate the operating effectiveness of the relevant control structure policies and procedures at the service organization in conjunction with internal control structure policies and procedures at the user organization. The user auditor should also consider whether the user organization has implemented complementary internal control structure policies and procedures contemplated in the design of the service organization's control structure policies and procedures that are recommended in the service organization's description of policies and procedures. To determine whether control risk may be reduced for assertions affected by the service organization and whether the level of substantive

tests may be reduced, the user auditor should not only read the service auditor's report on operating effectiveness (that is, the letter issued by the service auditor), but also should read and assess the testing performed and the results of the tests relevant to those assertions. The reader should consider the quality and quantity of the evidence provided by the report in determining whether it provides a sufficient basis for assessing control risk below the maximum for specified financial statement assertions. *In no case should the user auditor* only *consider the service auditor's report (that is, the letter issued by the service auditor) as the basis for reducing control risk below the maximum.*

If, after considering the policies and procedures at the user organization and other available information, the user auditor determines that the information in a type 1 or type 2 report does not meet his or her objectives, the user auditor may supplement his or her understanding of the service auditor's procedures and conclusions by discussing the scope and the results of the service auditor's work with the service auditor. The user auditor may also contact the service organization, through the user organization, to request that the service auditor perform agreed-upon procedures at the service organization, or the user auditor may perform such procedures. If the user auditor is still unsuccessful in gaining sufficient information to plan the audit, he or she should qualify his or her opinion on the financial statements because of a scope limitation.[1]

## TIMING CONSIDERATIONS RELATED TO USING A SERVICE ORGANIZATION'S DESCRIPTION OF POLICIES AND PROCEDURES

A service organization's description of policies and procedures is as of a point in time for both a type 1 and a type 2 report. Accordingly, the service auditor issues a report on whether the description presents fairly, in all material respects, the relevant aspects of the service organization's control structure policies and procedures at a point in time. Such information may be used to plan the audit of a user organization's financial statements in the same way that the auditor's understanding of the internal control structure at a point in time is used to plan the audit of the financial statements of an entity that does not use a service organization.

A report on policies and procedures placed in operation that is as of a date outside the reporting period of a user organization may be useful in providing a user auditor with a preliminary understanding of the control structure policies and procedures placed in operation at the service organ-

1. Paragraph 13.02 of the AICPA Audit and Accounting Guide *Audits of Employee Benefit Plans* indicates that historically the Department of Labor has rejected Form 5500, "Internal Revenue Service Annual Return/Report of Employee Benefit Plan," filings that contain either qualified opinions, adverse opinions, or disclaimers of opinion other than those issued in connection with a limited scope audit pursuant to 29 CFR 2520.103-8 or 12.

ization if the report is supplemented by additional current information from other sources. If the service organization's description is as of a date that precedes the beginning of the period under audit, the user auditor should consider updating the information in the description to determine whether there have been any changes in the service organization's control structure policies and procedures relevant to the processing of the user's transactions. Procedures to update the information in a service auditor's report may include —

- Discussions with user organization personnel who would be in a position to know about changes at the service organization.
- A review of current documentation and correspondence issued by the service organization.
- Discussions with service organization personnel or with the service auditor.

If the user auditor determines that there have been significant changes in the service organization's control structure policies and procedures, the user auditor should attempt to gain an understanding of the changes and consider the effect of the changes on the audit.

## THE USER AUDITOR'S CONSIDERATION OF TESTS OF OPERATING EFFECTIVENESS

As indicated in chapter 2, "Form and Content of Reports on the Processing of Transactions by Service Organizations," a type 2 report includes a description of tests performed by the service auditor of the operating effectiveness of specified control structure policies and procedures. If the user auditor intends to assess control risk below the maximum for certain financial statement assertions affected by the service organization's processing, the user auditor should determine whether the policies and procedures tested by the service auditor are relevant to the assertions in the user organization's financial statements. For tests of policies and procedures that are relevant, the user auditor should consider whether the nature, timing, extent, and results of the tests, in conjunction with the service auditor's report on the operating effectiveness of the policies and procedures, provide appropriate evidence to support the assessed level of control risk. In evaluating the tests of operating effectiveness, the user auditor should keep in mind that the shorter the period covered by a specific test and the longer the time elapsed since the performance of the test, the less support for risk reduction the test may provide. For example, a report with a six-month testing period that only covers one or two months of the user organization's financial reporting period offers less support for control risk reduction than a report in which the testing covers six months of the user organization's financial reporting period. If the service auditor's testing period is completely outside the user organization's financial reporting

period, the user auditor should not rely on such tests as support for control risk reduction because they do not provide current audit period evidence of the effectiveness of the control structure policies and procedures, unless other procedures such as those described in the following paragraphs of SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 319), are performed.

> 53. Evidential matter about the effective design or operation of internal control structure policies and procedures that was obtained in prior audits may be considered by the auditor in assessing control risk in the current audit. To evaluate the use of such evidential matter for the current audit, the auditor should consider the significance of the assertion involved, the specific internal control structure policies and procedures that were evaluated during the prior audits, the degree to which the effective design and operation of those policies and procedures were evaluated, the results of the tests of controls used to make those evaluations, and the evidential matter about design or operation that may result from substantive tests performed in the current audit. The auditor should also consider that the longer the time elapsed since the performance of tests of controls to obtain evidential matter about control risk, the less assurance it may provide.
> 54. When considering evidential matter obtained from prior audits, the auditor should obtain evidential matter in the current period about whether changes have occurred in the internal control structure, including its policies, procedures and personnel, subsequent to the prior audits, as well as the nature and extent of any such changes. Consideration of evidential matter about these changes, together with the consideration in the preceding paragraph, may support either increasing or decreasing the evidential matter about the effectiveness of design and operation to be obtained in the current period.

## COMPLEMENTARY CONTROLS THAT MAY BE REQUIRED AT USER ORGANIZATIONS

In certain circumstances, the service provided by the service organization may be designed with the assumption that certain internal control structure policies and procedures will be implemented by the user organizations. For example, the service may be designed with the assumption that the user organizations will have policies and procedures in place for authorizing transactions before they are sent to the service organization for processing. If such complementary user organization controls are required to achieve certain control objectives, the service organization should describe them in its description of policies and procedures. The user auditor should read the type 1 or type 2 report to determine whether complementary user organization controls are required and whether they are relevant to the service provided to that specific user organization. If they are relevant to the user organization, the user auditor should consider such information in planning the audit. Refer to chapter 4, "Performing a Service Auditor's

Engagement," for guidance to the service auditor when complementary user organization controls are required.

## REPORTABLE CONDITIONS

Reportable conditions are matters coming to the auditor's attention during a financial statement audit that, in the auditor's judgment, should be communicated to the audit committee or to individuals with a level of authority and responsibility equivalent to an audit committee because they represent significant deficiencies in the design or operation of the organization's internal control structure that could adversely affect the organization's ability to record, process, summarize, and report financial data consistent with management's assertions. Reportable conditions are defined in paragraph 2 of SAS No. 60, *Communication of Internal Control Structure Related Matters Noted in an Audit* (AICPA, *Professional Standards,* vol.1, AU sec. 325). When reading a type 1 or type 2 report, the user auditor may become aware of situations at the service organization that constitute reportable conditions for the user organization. Such situations may relate to the design or the operating effectiveness of the service organization's policies and procedures. In such circumstances, the user auditor should follow the guidance in SAS No. 60.

## UNCORRECTED ERRORS AT THE SERVICE ORGANIZATION

In the course of providing its services, the service organization may make errors that, if uncorrected, could affect one or more user organizations. The management of the service organization should report any uncorrected errors that are other than clearly inconsequential to the affected user organizations.

In performing the audit of a user organization, the user auditor should inquire of the user organization'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 user 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.

Chapter 4

# Performing a Service Auditor's Engagement

*This chapter describes the responsibilities of each of the parties involved in a service auditor's engagement — the service organization, the user organization, the service auditor, and the user auditor. It also describes the procedures that should be performed in a service's auditor's engagement and provides detailed reporting guidance for various situations that might arise in a type 1 or type 2 engagement.*

A service auditor's engagement consists of examining the service organization's description of policies and procedures to determine whether —

1. It presents fairly, in all material respects, the relevant aspects of the service organization's control structure policies and procedures that had been placed in operation as of a specified date.
2. The policies and procedures were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those policies and procedures were complied with satisfactorily.

In a type 2 engagement, the service auditor performs the procedures described above and also performs tests of specified policies and procedures to determine whether they were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.

Paragraphs 22 through 58 of SAS No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, *Professional Standards,* vol. 1, AU sec. 324), describe the responsibilities of service auditors in reporting on policies and procedures placed in operation (type 1 engagements) and in reporting on policies and procedures placed in operation and tests of operating effectiveness (type 2 engagements). This chapter provides additional guidance for a service auditor to consider when performing and reporting on a service auditor's engagement.

## RESPONSIBILITIES OF THE SERVICE ORGANIZATION

In a service auditor's engagement, the service organization and the service auditor each have specific responsibilities. The service organization is responsible for preparing the description of policies and procedures. The service auditor may assist the service organization in preparing the description; however, the representations in the description are the responsibility of the service organization's management.

The service organization is responsible for determining which services, business units, functional areas, or applications the service auditor will be engaged to report on, and for providing this information in its description. The service organization is responsible for the completeness, accuracy, and method of presentation of the description of control structure policies and procedures, and is also responsible for specifying the control objectives, unless they are established by a third party. In a type 2 engagement, the service organization specifies which control objectives will be tested for operating effectiveness and may engage a service auditor to test all of the control objectives identified in the description or a subset of the control objectives. Other responsibilities of the service organization include —

- Providing the service auditor with access to appropriate service organization resources such as service organization personnel, systems documentation, contracts, and minutes of oversight committee meetings.
- Disclosing to the service auditor any significant changes in policies and procedures that have occurred since the service organization's last examination, or within the last twelve months if the service organization has not previously issued a service auditor's report.
- Disclosing to the service auditor and the affected user organizations any illegal acts, irregularities, or uncorrected errors attributable to the service organization's management or employees that may affect one or more user organizations.
- Disclosing to the service auditor any relevant design deficiencies in policies and procedures of which it is aware, including those for which management believes the cost of corrective action may exceed the benefits.
- In a type 2 engagement, disclosing to the service auditor all instances of which it is aware when policies and procedures have not operated with sufficient effectiveness to achieve the specified control objectives.
- Providing the service auditor with a letter of representations.

The service organization should ensure that the description provides sufficient information, within the scope of the examination, for user auditors to obtain an understanding of the service organization's control structure policies and procedures that may be relevant to user organizations' internal control structures. Chapter 2, "Form and Content of Reports on the

Processing of Transactions by Service Organizations," provides guidance on the form and content of the service organization's description of policies and procedures.

## RESPONSIBILITIES OF THE SERVICE AUDITOR

### Procedures to Report on the Fairness of the Presentation of the Service Organization's Description of Policies and Procedures

The service auditor should read the description of policies and procedures to gain an understanding of the representations made by management in the description. After reading the description, the service auditor should perform procedures to determine whether the description presents fairly, in all material respects, the relevant aspects of the service organization's policies and procedures that had been placed in operation. Service organization policies and procedures are considered *relevant* to user organizations if they represent or affect a user organization's control environment, accounting system, or control procedures. The term *placed in operation* means that the policies and procedures have been implemented or put into practice, as opposed to existing only on paper. Placed in operation does not imply that the policies and procedures are suitably designed or operating with sufficient effectiveness to achieve control objectives.

To determine whether the description is fairly presented, the service auditor should gain an understanding of the service provided by the service organization. Procedures to gain this understanding may include the following:

- Discussion with management and other service organization personnel
- Review of standard contracts with user organizations to gain an understanding of the service organization's contractual obligations
- Observation of the procedures performed by service organization personnel
- Review of service organization policy and procedure manuals and other systems documentation, for example, flowcharts and narratives
- Walk-through of selected transactions and control procedures
- Determining who the user organizations are and how the services provided by the service organization are likely to affect the user organizations, for example, the predominant type(s) of user organizations, and whether user organizations are regulated by governmental agencies

The service auditor should then compare his or her understanding of the service provided to user organizations with representations in the description to determine whether the service organization's description is fairly

stated. The description is considered fairly stated if it describes control structure policies and procedures in a manner that does not omit or distort information that may affect user auditors' decisions in planning the audit of the user organizations' financial statements and in assessing control risk.

The service auditor should determine whether the description addresses all of the major aspects of the processing (within the scope of the engagement) that may be relevant to user auditors in planning the audit. There may be aspects of the services performed by the service organization that the user organizations may assume are within the scope of the engagement that may or may not be included in the scope of the engagement. For example, a service organization may have formal or informal policies and procedures related to the conversion of new user organizations to the service organization's systems. The service organization's description may not include a description of its policies and procedures related to the conversion of new user organizations to the service organization's systems because the service organization may consider such policies and procedures to be outside the normal processing services provided to user organizations, and outside the scope of the engagement. To avoid misunderstanding by readers of the description, it may be desirable to state whether the description covers policies and procedures related to the conversion of new user organizations to the service organization's systems.

The service auditor should also determine whether the description objectively describes what is taking place at the service organization and whether it contains significant omissions or inaccuracies. The description should not state or imply that policies and procedures are being performed if they are not. Consider a situation in which a service organization provides two different loan processing applications: Application A, for which the service organization maintains independent totals and performs reconciliations of transactions processed, and application B, for which such totals are not maintained and for which reconciliations are not performed. The service organization's description should clearly indicate which application(s) are being described. If both applications are being described, the description should indicate the different levels of service provided. For the description to be fairly stated, the service organization should state that independent totals and reconciliations are performed for application A and should not state or imply that they are performed for application B.

If the service organization's description omits or misstates information that is within the scope of the engagement and that the service auditor believes user auditors would need to plan the audit, the service auditor should discuss the matter with the management of the service organization and should ask management to amend the description. If management does not amend the description by including the omitted information or correcting the misstated information, the service auditor should consider issuing a qualified or adverse opinion on whether the service organization's description of policies and procedures presents fairly, in all material respects, the relevant aspects of the service organization's policies and procedures. In such circumstances, the service auditor should add an explanatory paragraph to the service auditor's report, preceding the opin-

ion paragraph, which is the first opinion paragraph in a type 2 report. An example of such a paragraph follows:

> The accompanying description states that Example Service Organization maintains independent totals and performs reconciliations of transactions processed. Inquiries of staff personnel and inspection of activities indicate that such procedures are applied in application A but are not applied in application B.

In addition, the first sentence of the opinion paragraph, (the first opinion paragraph in a type 2 report) would be modified as follows:

> In our opinion, except for the matter referred to in the preceding paragraph, the accompanying description of the aforementioned applications presents fairly, in all material respects, the relevant aspects of Example Service Organization's policies and procedures that had been placed in operation as of December 31, 19XX.

For the description to be considered fairly presented, it should contain a complete set of control objectives. Paragraphs 35 and 50 of SAS No. 70 state that control objectives established by the service organization should be reasonable in the circumstances and consistent with the service organization's contractual obligations. A complete and reasonable set of control objectives should provide user auditors with a basis for determining the effect of the service organization's policies and procedures on user organizations' financial statement assertions. For example, a service organization that provides loan servicing to financial institutions and asserts that loan payments received are completely and accurately recorded should include a control objective in its description of policies and procedures, such as the following:

> Control policies and procedures provide reasonable assurance that loan payments received from user organizations are completely and accurately recorded.

Although it is the service organization's responsibility to specify the control objectives, it is the service auditor's responsibility to determine whether the control objectives are complete and reasonable in the circumstances, unless the control objectives are specified by a third party.

To enable the service auditor to identify the kinds of user organization financial statement assertions that are likely to be affected by the control structure policies and procedures at the service organization, the service auditor should obtain a general understanding of the nature of the user organizations and how they use the services provided. The service auditor should determine whether the control objectives specified by the service organization relate to such assertions. The service auditor cannot, however, be aware of all of the assertions in user organizations' financial statements that might be affected by the service organization's control structure policies and procedures or how those policies and procedures might affect the financial statement assertions of each user organization. Refer to chapter

2 for examples of how a service organization's control objectives relate to a user organization's financial statement assertions.

If the service auditor determines that the control objectives are not complete and reasonable in the circumstances, he or she should discuss the matter with the service organization's management and request that management amend the description by adding the appropriate control objective(s). If the service organization's management does not amend the description so that it includes the recommended control objective(s), the service auditor should add an explanatory paragraph to the service auditor's report identifying the omitted control objective(s). The following is an example of an explanatory paragraph that should be added before the opinion paragraph of the service auditor's report (the first opinion paragraph in a type 2 report) if the control objectives are incomplete:

> The accompanying description of policies and procedures does not include a control objective for the complete and accurate recording of loan payments received by Example Service Organization. We believe that this control objective and the related policies and procedures that might achieve this control objective should be specified in the Service Organization's description of policies and procedures because they are relevant to user organizations.

In addition, the first sentence of the opinion paragraph (the first opinion paragraph in a type 2 report) should be modified to read as follows:

> In our opinion, except for the matter referred to in the preceding paragraph, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of Example Service Organization's policies and procedures that had been placed in operation as of December 31, 19XX.

Depending on the severity of the omission, the service auditor may consider issuing an adverse opinion on whether the service organization's description of policies and procedures presents fairly, in all material respects, the relevant aspects of the service organization's policies and procedures. In such circumstances, the first sentence of the opinion paragraph of the service auditor's report (the first opinion paragraph in a type 2 report) would be modified as follows:

> In our opinion, because of the omission discussed in the preceding paragraph, the accompanying description of the aforementioned application does not present fairly, in all material respects, the relevant aspects of Example Service Organization's policies and procedures that had been placed in operation as of December 31, 19XX.

Although the service auditor may qualify his or her opinion on the fairness of the presentation of the description of policies and procedures, the omission would not necessarily affect the service auditor's opinion on the suitability of the design or operating effectiveness of the policies and procedures because those opinions only relate to control objectives that are

included in the service organization's description. The service auditor cannot report or comment on the suitability of the design or operating effectiveness of policies and procedures intended to achieve control objectives that are not included in the service organization's description of policies and procedures. The service auditor is not responsible for identifying or testing the policies and procedures that might achieve the omitted control objective(s).

The service auditor should ensure that the control objectives are objectively stated so that individuals having competence in and using the same or similar measurement criteria would arrive at reasonably similar conclusions about the possible achievement of the control objectives. For example, the following control objective would ordinarily be too subjective for evaluation:

> Control policies and procedures affecting physical access to computer equipment, storage media, and program documentation are adequate.

This control objective could be reworded as follows to meet the objectivity criteria described above:

> Control policies and procedures provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals.

If the service auditor determines that the control objectives do not meet the objectivity criteria described above, the service auditor should ask the service organization's management to reword the control objectives. If management of the service organization does not reword the control objectives, the service auditor should consider modifying his or her opinion on whether the service organization's description of policies and procedures presents fairly, in all material respects, the relevant aspects of the service organization's policies and procedures.

In some situations, the service organization may include objectives that would not be considered relevant to user auditors for the purpose of planning the audit and assessing control risk, such as objectives addressing the efficiency of the service organization's operations or its plans for the future. If such objectives are not relevant and cannot be objectively measured, they should be included in the section of a type 1 or type 2 report entitled, "Other Information Provided by the Service Organization" and excluded from the service auditor's opinion. Reporting guidance for such situations is presented later in this chapter under the heading, "Elements of the Service Organization's Description That Are Not Covered by the Service Auditor's Report."

In certain circumstances, the control objectives may be specified by an outside party, such as a regulatory agency or a user group. In these situations, the service auditor need not determine whether the control objectives are reasonable in the circumstances, consistent with the service organization's contractual obligations, and relevant to the user organiza-

tions' financial statement assertions. If the control objectives are established by an outside party, the service auditor's responsibility is to determine whether the control objectives in the description conform to those specified by the outside party.

## Procedures to Report on the Suitability of Design of Policies and Procedures to Achieve Specified Control Objectives

From the viewpoint of a user auditor, a control structure policy or procedure is suitably designed if individually, or in combination with other policies and procedures, it is likely to prevent or detect material misstatements in specific financial statement assertions. From the viewpoint of a service auditor in the context of a service auditor's engagement, a control structure policy or procedure is suitably designed if individually, or in combination with other policies and procedures, it is likely to prevent or detect errors that could result in the nonachievement of specified control objectives when the described policies and procedures are complied with satisfactorily. To determine if control structure policies and procedures are suitably designed to achieve specified control objectives, the service auditor should —

- Consider the linkage between the policies and procedures and the specified control objectives.
- Consider the ability of the policies and procedures to prevent or detect errors related to the control objectives.
- Perform procedures, such as inquiry of appropriate entity personnel, inspection of documents and reports, and observation of the application of specific control structure policies and procedures, to determine whether they are suitably designed to achieve the specified control objectives. (For service organizations with complex control structure policies and procedures, the service auditor should consider using flowcharts, questionnaires, or decision tables to facilitate the understanding of the design of the control structure policies and procedures.)

After performing procedures such as those mentioned above, a service auditor may conclude that the control structure policies and procedures are not suitably designed to achieve specified control objectives. For example, a service organization may identify a reconciliation of input to output as a control structure procedure designed to achieve the control objective that all output is complete and accurate, but may not have a policy or procedure for following-up on reconciling items and for obtaining independent review of the reconciliations. The service auditor should consider this design deficiency in his or her overall assessment of the control structure policies and procedures designed to achieve the control objective that all output is complete and accurate. The following is an example of an explanatory paragraph that should be added to the service auditor's report, preceding the opinion paragraph (the first opinion paragraph in a

type 2 report) if the service auditor determines that policies and procedures are not suitably designed to achieve a specified control objective.

> As discussed in the accompanying description, Example Service Organization reconciles the listing of loan payments received with the output generated. The reconciliation procedures, however, do not include a policy or procedure for follow-up on reconciling items and for independent review and approval of the reconciliations. These deficiencies result in the policies and procedures not being suitably designed to achieve the control objective, "Policies and procedures provide reasonable assurance that all output is complete and accurate."

The opinion paragraph of the service auditor's report (the first opinion paragraph in a type 2 report) should be modified as follows:

> In our opinion, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of Example Service Organization's policies and procedures that had been placed in operation as of December 31, 19XX. Also, in our opinion, except for the matter described in the preceding paragraph, the control structure policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described control structure policies and procedures were complied with satisfactorily.

## Procedures to Report on the Operating Effectiveness of Policies and Procedures to Achieve Specified Control Objectives

In a type 2 engagement, the service auditor performs tests of control structure policies and procedures to determine whether they were operating with sufficient effectiveness to achieve the related control objectives during a specified period. Operating effectiveness is concerned with how a policy or procedure is applied, the consistency with which it is applied, and by whom it is applied. As previously stated, the service organization specifies which control objectives will be tested and the service auditor determines which control structure policies and procedures are necessary to achieve the control objectives specified by management. The service auditor may conclude that all or only a portion of the policies and procedures identified by management are necessary to achieve a control objective. The service auditor also determines the nature, timing, and extent of the tests to be performed to express his or her opinion on the operating effectiveness of control structure policies and procedures.

Procedures to test the operating effectiveness of control structure policies and procedures may include the following procedures, or a combination thereof:

- Inquiry of appropriate service organization personnel
- Inspection of documents, reports, or other data
- Observation of the application of the policy or procedure
- Reperformance of the policy or procedure

Some tests of control structure policies and procedures provide more convincing evidence of the effectiveness of the policies and procedures than others do. Evidential matter obtained directly by the service auditor, such as through observation, provides greater assurance than evidential matter obtained indirectly or by inference, such as through inquiry. The service auditor should consider, however, that the observed application of a policy or procedure might not be performed in the same manner when the auditor is not present. Also, inquiry alone generally will not provide sufficient evidential matter to support a conclusion about the operating effectiveness of a specified control structure policy or procedure.

The service auditor should perform tests of aspects of the control environment related to the service provided and should assess their effectiveness in establishing, enhancing, or mitigating the effectiveness of specific control structure policies and procedures. As control environment aspects are judged to be less effective, more evidence of the operating effectiveness of the policies and procedures should be gathered to determine whether a control objective has been achieved. In some cases, deficiencies in the control environment may be so pervasive that the service auditor will need to modify his or her opinion on the achievement of one or more control objectives. In a type 2 report, the service auditor also includes a description of the nature, timing, and extent of the tests of the relevant aspects of the control environment in the section of the report that describes the service auditor's tests and results. Chapter 2, "Form and Content of Reports on the Processing of Transactions by Service Organizations," provides guidance on the features of the service organization's control environment that may affect the services provided to user organizations.

The nature, timing, and extent of the tests of operating effectiveness are also affected by the period covered by the report. Tests of operating effectiveness should provide evidence that will enable the service auditor to report on the entire period covered by the report. To be useful to user auditors, the report should ordinarily cover a minimum reporting period of six months. If the service auditor is engaged to report on a period of less than six months, he or she should disclose the reasons for the shorter period in the service auditor's section of the report. Circumstances that might necessitate a report covering a period of less than six months include —

- Engagement of the service auditor close to the report issuance date in a situation where certain controls can only be tested through observation.
- A service organization, system, or application that has been in operation for less than six months.
- Significant system changes have occurred and it is not practicable either (1) to wait six months before issuing a report or (2) to issue a report covering both the system before and after the changes.

Certain control structure policies and procedures may not leave documentary evidence that can be tested at a later date. The service auditor may

need to test the operating effectiveness of such policies and procedures at various times throughout the reporting period.

Situations may arise in which the service auditor's tests of operating effectiveness do not cover the same period for all control objectives. In such cases, the service auditor's report should disclose the applicable test periods.

Evidence from prior service auditor's engagements may also affect the nature, timing, and extent of the tests of operating effectiveness. To provide a basis for a reduction in testing, such evidential matter should be supplemented with evidential matter obtained during the current period to support the service auditor's conclusion that the relevant control structure policies and procedures are operating effectively. Decisions about the degree of assurance that may be obtained from prior engagement evidence and about the additional evidential matter needed in the current period are affected by considerations such as the following.

- Conditions that may affect whether the policies and procedures operate effectively, including
  - A change in the nature of the transactions being processed
  - An increase in the volume of transactions being processed
  - An increase in the number of changes made to the procedures, the system, or the computer programs
  - An increase in the number of user organizations
  - A change in management's attitude or a reduction in supervision
  - High turnover of employees
  - An increase in the responsibilities or workloads of employees
- The effects of related control structure policies and procedures and control environment factors that reinforce the continued effective operation of the control structure policies and procedures, including
  - The existence of documented procedures manuals
  - Close management supervision, including frequent communication and responsibility reporting
  - Periodic reviews by internal auditors
  - Effective general computer controls, such as program change controls

The service auditor should determine whether there were changes in the control structure policies and procedures subsequent to the previous engagement and should gather information about the nature and extent of such changes. If such changes are relatively minor, evidential matter obtained in prior audits may provide evidence for the current engagement and may consequently reduce, but not eliminate, the need for additional evidence in the current period. Conversely, changes may be so significant that evidential matter obtained in prior engagements may provide limited or no evidence of operating effectiveness for the current engagement.

Readers of this APS should refer to paragraphs 52 through 55 of SAS No. 55, *Consideration of the Internal Control Structure in a Financial State-*

*ment Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 319), for guidance on the timeliness and the degree of assurance provided by evidential matter and should refer to SAS No. 39, *Audit Sampling* (AICPA, *Professional Standards,* vol. 1, AU sec. 350) for guidance when sampling is used in performing tests of operating effectiveness.

## DESCRIBING TESTS OF OPERATING EFFECTIVENESS AND THE RESULTS OF THOSE TESTS

Paragraph 44*f* of SAS No. 70 specifies the elements that should be included in a description of tests of operating effectiveness. Paragraph 44*f* states in part:

> The description should include the policies and procedures that were tested, the control objectives the policies and procedures were intended to achieve, the tests applied, and the results of the tests. The description should include an indication of the nature, timing, and extent of the tests, as well as sufficient detail to enable user auditors to determine the effect of such tests on user auditors' assessments of control risk. To the extent that the service auditor identified causative factors for exceptions, determined the current status of corrective actions, or obtained other relevant qualitative information about exceptions noted, such information should be provided.

This paragraph has been interpreted to mean that in all cases, for each control objective tested, the description of tests of operating effectiveness should include all of the elements listed in paragraph 44*f* of SAS No. 70, whether or not the service auditor concludes that the control objective has been achieved. The description should provide sufficient information to enable user auditors to assess control risk for financial statement assertions affected by the service organization. The description need not be a duplication of the service auditor's detailed audit program, which in some cases would make the report too voluminous for user auditors and would provide more than the required level of detail.

Further, this paragraph has been interpreted to mean that in describing the nature, timing, and extent of the tests applied, the service auditor also should indicate whether the items tested represent a sample or all of the items in the population, but need not indicate the size of the population, except as noted below. In describing the results of the tests, the service auditor should include exceptions and other information that in the service auditor's judgment could be relevant to user auditors. Such exceptions and other information should be included for each control objective, whether or not the service auditor concludes that the control objective has been achieved. When exceptions that could be relevant to user auditors are noted, the description also should include the following information:

- The size of the sample, if sampling has been used
- The number of exceptions noted
- The nature of the exceptions

If the service auditor has identified causative factors for exceptions, determined the current status of corrective actions, or obtained other relevant qualitative information about exceptions noted, that information also should be provided.

If no exceptions or other information that could be relevant to user auditors are identified by the tests, the service auditor should indicate that finding with remarks such as "no relevant exceptions noted," "no exceptions noted," or "procedures operating as described."

The following examples illustrate situations in which a service auditor performs tests of the operating effectiveness of control structure policies and procedures, evaluates the results of the tests, and determines what information to include in the description of the results of tests. In each situation, the rationale used by the service auditor in determining what information to include in the description of the results of tests is presented. It is assumed that in each situation other relevant control structure policies and procedures and tests of operating effectiveness also would be described. As in all aspects of the engagement, the service auditor should use his or her judgment in determining what information to include in the results of tests.

In examples 1 and 2 that follow, the service auditor is performing tests of the operating effectiveness of control structure policies and procedures at a trust organization. Some of the services performed by the trust organization include purchasing and selling securities for user organizations upon their specific authorization, recording such transactions, and maintaining book-entry records of the securities owned by the user organizations.

## Example 1

*Control objective specified by the service organization.* Control structure policies and procedures provide reasonable assurance that purchases of securities are authorized.

*Control structure policy or procedure described by the service organization for this objective.* Securities are purchased for user organizations only after the service organization receives a security purchase authorization form signed by an employee of the user organization who has been specifically designated by the user organization to authorize purchases.

*The service auditor performed the following tests of operating effectiveness.* The service auditor selected a sample of $n$[1] security purchase authorization forms and examined the forms for an appropriate user employee signature.

*Results of tests.* One of the $n$ security purchase authorization forms did not have an appropriate user employee signature.

---

1. The sample size in each of the examples in this section is denoted by the letter $n$. Actual sample sizes would be determined by the service auditor.

*Reporting test results.* The service auditor concluded that user organizations and user auditors may be relying on the operating effectiveness of the control that requires appropriate user employee signatures on security purchase authorization forms to ensure that purchases of securities are properly authorized by the user organizations. The service auditor also concluded that information about the potential for unauthorized security purchases could be relevant to user auditors' assessments of control risk; accordingly, the service auditor concluded that this information would be included in the results of tests.

## Example 2

*Control objective specified by the service organization.* Control structure policies and procedures provide reasonable assurance that purchases of securities are authorized.

*Control structure policy or procedure described by the service organization for this objective.* Securities are purchased for user organizations only after the service organization receives authorization from the user organization. The service organization obtains such authorization through one of the following procedures: (1) receiving a security purchase authorization form, signed by an employee of the user organization who has been specifically designated by the user organization to authorize purchases; or (2) performing a callback procedure in which a telephone call is placed to a specifically designated user employee to obtain verbal authorization, and maintaining a record, such as a tape recording, of such authorization. If a security purchase authorization form is received without an appropriate authorizing signature, a telephone call is placed to the user organization to obtain verbal authorization.

*Tests of operating effectiveness performed by the service auditor.* The service auditor selected a sample of $n$ security purchase authorization forms and examined the forms for evidence of an appropriate user employee signature.

*Results of tests.* One of the $n$ security purchase authorization forms did not have an appropriate user signature. For the form without the signature, the service auditor examined the callback documentation and determined that the callback procedure had been performed.

*Reporting test results.* The service auditor concluded that the results of tests did not constitute an exception. Although the user signature was missing from one of the security purchase authorization forms, the callback procedure identified in the service organization's description had been performed. The results of the tests performed provided evidence that the identified control structure policies and procedures were operating effectively to ensure that an appropriately authorized employee of the user organization had authorized the purchase. Unlike the situation described

in example 1, the missing signature does not constitute an exception in this case because (1) the control described is to obtain a signature or, in the absence of a signature, to perform the callback procedure, and (2) the callback procedure was performed and documented.

The service auditor also considered whether it would be relevant to user auditors that one of the *n* items tested was authorized by a callback procedure rather than a signature. The service auditor concluded that this information would not be relevant to user auditors; accordingly, the service auditor concluded that the information about the missing signature would not be included in the results of tests. *If the service auditor had concluded that the number of items tested for which signatures were missing and callback procedures had been performed could have been relevant to user auditors, the service auditor would have reported such information in the results of tests.*

In examples 3 and 4, the service auditor is performing tests of the operating effectiveness of control structure policies and procedures at a data processing service organization that processes transactions for user organizations.

## Example 3

*Control objective specified by the service organization.* Control structure policies and procedures provide reasonable assurance that changes to application software are authorized, tested, and approved.

*Control structure policy or procedure described by the service organization for this objective.* The programming manager is required to sign (1) a program change form to authorize the change, and (2) the results of testing to indicate that the change has been made as authorized.

*Tests of operating effectiveness performed by the service auditor.* The service auditor selected a sample of *n* changes and examined the program change forms and the related results of testing for the programming manager's signatures.

*Results of tests.* For one of the *n* changes, the programming manager's signature was missing from the program change form, but was present on the results of testing.

*Reporting test results.* The service auditor concluded that the programming manager's signature on the results of testing provided evidence that the programming manager had also authorized the change. The service auditor concluded that the absence of the programming manager's signature on the program change form would not be relevant to user auditors; accordingly, the service auditor concluded that information about the missing signature would not be included in the results of tests.

## Example 4

*Control objective specified by the service organization.* Control structure policies and procedures provide reasonable assurance that changes to application software are authorized, tested, and approved.

*Control structure policy or procedure described by the service organization for this objective:* The programming manager is required to sign (1) the program change form to authorize the change, and (2) the results of testing to indicate that the change has been made as authorized.

*Tests of operating effectiveness performed by the service auditor.* The service auditor selected a sample of *n* changes and examined the program change forms and the related results of testing for the programming manager's signatures.

*Results of tests:* For one of the *n* changes, the programming manager's signature was missing from the results of testing. The programming manager's signature was present on all program change forms.

*Reporting test results:* The service auditor concluded that the absence of the programming manager's signature on the results of testing could result in an increased risk that an authorized change would be incorrectly made. Because this could affect user auditors' assessments of control risk for assertions affected by the computer processing, the service auditor concluded that information about the missing signature would be included in the results of tests.

In examples 5 and 6, the service auditor is performing tests of the operating effectiveness of control structure policies and procedures that prevent unauthorized access to programs and data at a data processing service organization.

## Example 5

*Control objective specified by the service organization.* Control structure policies and procedures provide reasonable assurance that access to programs and data is restricted to appropriately authorized individuals.

*Control structure policy or procedure described by the service organization for this objective.* The service organization uses software to control access to programs and data. User organizations must provide the service organization with an appropriately signed form to change user employees' access. The service organization makes the change within one business day of notification from the user organization.

*User control considerations.* User organizations are responsible for notifying the service organization when there is a need to change user employees' access privileges.

*Tests of operating effectiveness performed by the service auditor.* The service auditor selected a sample of *n* forms requesting termination of user access for specified employees to determine whether and when access for the employees had been terminated. The service auditor also examined customer service logs of user organization complaints.

*Results of tests.* Of the *n* forms tested, one user employee retained access to the system for four business days after the request for termination of access had been received.

*Reporting test results.* The significance of this exception could only be evaluated by user auditors in the context of other factors at the user organizations, for example, the number of employees with access to the system who had been terminated, the reasons for termination of access, the nature of the employees' access, and the existence of other relevant controls at the user organizations. Accordingly, the service auditor concluded that this information would be included in the results of tests.

## Example 6

*Control objective specified by the service organization.* Control structure policies and procedures provide reasonable assurance that access to programs and data is restricted to appropriately authorized individuals.

*Control structure policy or procedure described by the service organization for this objective.* The service organization uses software to control access to programs and data. User organizations must provide the service organization with an appropriately signed form to change user employees' access. The service organization makes the change within one business day of notification from the user organization.

*User control considerations.* User organizations are responsible for notifying the service organization when there is a need to change user employees' access privileges.

*Tests of operating effectiveness performed by the service auditor.* The service auditor selected a sample of *n* forms requesting termination of user access for specified employees to determine whether and when access to the system for the employees had been terminated. The service auditor also examined customer service logs of user organization complaints.

*Results of tests.* The service auditor noted three instances when user organizations complained that their employees' access had not been terminated within one business day of the employees' termination. The service auditor inspected the requests to change user employee access forms for these instances and determined that the user organizations had submitted the requests from one to three weeks after the employees had been ter-

minated. Correspondence indicated that the service organization had discussed these instances with the affected user organizations.

*Reporting test results.* The service auditor concluded that the instances noted resulted from the user organizations' failures to properly execute control structure policies and procedures that were their responsibility (as described in the user control considerations section of the report), and were not exceptions in the service organization's application of control structure policies and procedures. Because the report clearly describes the user organizations' responsibilities in the user control considerations section of the report, and because the items noted had been communicated to the affected user organizations, the service auditor concluded that information about the complaints of delayed termination of employees' access to the system would not be included in the results of tests. *If, after considering the specific facts and circumstances in the situation, the service auditor concluded that information about the user organizations' complaints of delayed termination of employee access to the system could be relevant to user auditors, that information would be included in the results of tests.*

In examples 7 and 8, the service auditor is performing tests of the operating effectiveness of control structure policies and procedures at a trust organization. One of the services performed by the trust organization is recording transactions for user organizations.

## Example 7

*Control objective specified by the service organization.* Control structure policies and procedures provide reasonable assurance that security purchase and sale transactions are recorded at the appropriate amounts and in the appropriate periods.

*Control structure policy or procedure described by the service organization for this objective.* Reconciliations are performed daily and reconciling items are identified and resolved within ten days and prior to the issuance of customer statements.

*Tests of operating effectiveness performed by the service auditor.* The service auditor inspected a sample of *n* reconciliations covering the test period.

*Results of tests.* Reconciliations are performed consistently and reconciling items are identified and resolved within ten days and prior to the issuance of customer statements. Reconciling items for the reconciliations examined appeared to result from normal processing and ranged from a few cents to several thousand dollars.

*Reporting test results.* The service auditor concluded that the results of tests provided evidence that the identified controls were operating effectively.

The service auditor also concluded that the reconciling items in the reconciliations examined resulted from normal processing and were being appropriately identified and resolved. Accordingly, the service auditor indicated that no exceptions had been noted in the tests of operating effectiveness. *If the service auditor had concluded that information about the reconciling items or the results of tests could be relevant to user auditors, that information would be included in the description of tests of operating effectiveness. For example, the service auditor might wish to communicate that the number and age of the reconciling items appeared reasonable and within the service organization's guidelines. (The sample service auditor's report for Example Trust Organization, presented in example 3 of appendix A illustrates this point.)*

## Example 8

*Control objective specified by the service organization.* Control structure policies and procedures provide reasonable assurance that security purchase and sale transactions are recorded at the appropriate amounts and in the appropriate periods.

*Control structure policy or procedure described by the service organization for this objective.* Reconciliations are performed daily and reconciling items are identified and resolved within ten days and prior to the issuance of customer statements.

*Tests of operating effectiveness performed by the service auditor.* The service auditor inspected a sample of *n* reconciliations covering the test period.

*Results of tests.* Reconciling items ranged from a few cents to several thousand dollars. Reconciling items were identified consistently but were not always resolved within the ten day period and prior to the issuance of customer statements.

*Reporting test results.* The service auditor concluded that the service organization's failure to consistently resolve all reconciling items within the required period could affect user auditors' assessments of whether transactions are completely and accurately reflected in customers' statements. Accordingly, the service auditor concluded that this information would be included in the results of tests.

## REPORTING WHEN CONTROL STRUCTURE POLICIES AND PROCEDURES ARE NOT OPERATING EFFECTIVELY

The service auditor should evaluate the results of the tests of operating effectiveness and the significance of any exceptions noted. The service auditor may conclude that specified control objectives have been achieved even if exceptions have been noted and reported. If the service auditor

determines that policies and procedures are not operating with sufficient effectiveness to achieve specified control objectives, the service auditor should report those conditions in an explanatory paragraph of the service auditor's report preceding the paragraph expressing an opinion on operating effectiveness. An example of such a paragraph follows:

> The Service Organization states in its description of policies and procedures and in Schedule X that it has policies and procedures in place to reconcile loan payments received with the output generated, to follow-up on reconciling items, and to independently review the reconciliation procedures. Our tests of operating effectiveness noted that significant reconciling items were not being resolved on a timely basis in accordance with the Service Organization's policy. This resulted in the nonachievement of the control objective "Control structure policies and procedures provide reasonable assurance that loan payments received are properly recorded."

In addition, the first sentence of the paragraph expressing an opinion on operating effectiveness should be modified as follows:

> In our opinion, except for the matter described in the preceding paragraph, the control structure policies and procedures that were tested, as described in Schedule X, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Schedule X were achieved during the period from January 1, 19XX, to December 31, 19XX.

## ADDITIONAL COMMENTS RELATED TO TYPE 2 ENGAGEMENTS

As previously stated in this chapter, in a type 2 engagement the service auditor performs procedures to determine whether (1) the description presents fairly the policies and procedures that have been placed in operation as of a specified date, (2) the control policies and procedures were suitably designed to achieve specified control objectives, and (3) the control policies and procedures were operating with sufficient effectiveness to provide reasonable assurance that the control objectives were achieved for the specified period. The nature and objectives of the tests performed to evaluate the fairness of the presentation of the description are different from those performed to evaluate the operating effectiveness of the control structure policies and procedures.

For instance, the description of policies and procedures for Example Computer Service Organization presented in example 1 of appendix A would ordinarily describe the method of calculating the interest on savings account balances and the control structure policies and procedures that provide reasonable assurance that the interest is calculated in conformity with the description (see control objective 10 in example 1 of appendix A). To determine whether the description of the calculation of interest is fairly presented, the service auditor would perform procedures, such as walkthroughs

or reperformance of the calculations, to determine whether the calculation, as described, had been placed in operation. Because the interest calculations are dependent on the general computer controls, the service auditor would also perform procedures to determine whether the service organization's description of the general computer controls is fairly stated.

The objective of tests of the operating effectiveness of control structure policies and procedures is to determine how the described policies and procedures are applied, the consistency with which they are applied, and by whom they are applied. In Example Computer Service Organization's description of tests of operating effectiveness, the tests of the operating effectiveness of the control structure policies, and procedures that provide reasonable assurance that interest is calculated in conformity with the description, are limited to testing the control structure policies and procedures over the general computer controls because the service organization relies on the computer to calculate interest in conformity with the description. The service auditor generally would not indicate that the only test of operating effectiveness performed was to recalculate interest because recalculation is performed to determine whether interest is calculated as stated in the description. Recalculation does not test the operating effectiveness of the controls.

## OTHER MATTERS RELATED TO PERFORMING A SERVICE AUDITOR'S ENGAGEMENT

### Complementary Controls at User Organizations

In performing his or her procedures and in considering the service organization's description of policies and procedures, it may become evident to the service auditor that the service was designed with the assumption that certain internal control structure policies and procedures would be implemented by user organizations. Such controls are called *complementary user organization controls.* Examples of complementary user organization controls include —

- Controls at the user organization over passwords needed to access the service organization's applications through computer terminals
- Controls at the user organization to ensure that all input sent to the service organization is complete, accurate, and authorized
- Controls at the user organization to ensure that all required output is received from the service organization and reconciled to the input sent to the service organization

Such required complementary user organization controls should be delineated in the service organization's description of policies and procedures. If the service organization's description does not identify the complementary user organization controls, the service auditor should request that the management of the service organization amend its description of

policies and procedures to include that information. If management does not amend the description, the service auditor should consider adding an explanatory paragraph to the report that describes the required complementary user organization controls and should consider qualifying his or her opinion on the fairness of the presentation of the description.

In certain situations, the application of user organization controls may be necessary to achieve a stated control objective. Consider the following control objective for a service organization that provides payroll services to user organizations and receives input payroll transactions from the user organizations via remote terminals:

> Control policies and procedures provide reasonable assurance that all input to the application is authorized.

This control objective could not be achieved without the implementation of input controls at the user organizations because transaction authorization rests with the user organizations. The service organization can only be responsible for ensuring that input transactions are received from authorized sources. Accordingly, if the control objective were "Control policies and procedures provide reasonable assurance that all input is received from authorized sources," the control objective could be achieved without controls at the user organizations.

If the application of such user organization controls is necessary to achieve a stated control objective, the service auditor should add the phrase "and user organizations applied the internal control structure policies and procedures contemplated in the design of service organization policies and procedures" following the words "complied with satisfactorily" in the scope and opinion paragraphs of the service auditor's report.

## Other Design Deficiencies Irrespective of Specified Control Objectives

Within the scope of the examination, the service auditor should consider whether any other information, irrespective of specified control objectives, has come to his or her attention that causes him or her to conclude (1) that design deficiencies exist that could adversely affect the ability of the service organization to record, process, summarize, or report financial data to user organizations without error, and (2) that user organizations would not generally be expected to have policies and procedures in place to mitigate such design deficiencies. However, a service auditor is not required to search for such deficiencies.

## Changes in the Service Organization's Policies and Procedures

Although a service organization's description of policies and procedures is as of a specified date, the service auditor should inquire about changes in the service organization's policies and procedures that may have occurred

before the beginning of fieldwork. If the service auditor believes that the changes would be considered significant by user auditors, those changes should be described in the service organization's description of policies and procedures. Generally, changes that occurred more than twelve months before the date being reported on would not be considered significant because they generally would not affect the user auditors' considerations.

Paragraphs 28 and 43 of SAS No. 70 present examples of changes in the service organization's policies and procedures that might be considered significant to user auditors. Such changes might include the following:

- Procedural changes made to accommodate provisions of a new Financial Accounting Standards Board (FASB) Statement of Financial Accounting Standards or provisions of new regulatory requirements
- Major changes in an application to permit on-line processing
- Major changes in an application to automate certain manual procedures
- Procedural changes to eliminate previously identified deficiencies
- Implementation of an access control software package

If the service organization does not include the changes in its description of policies and procedures, the service auditor should request that management amend the description. If management does not amend the description, the service auditor should describe the changes in a separate explanatory paragraph of his or her report, preceding the paragraph expressing an opinion on fair presentation of the description. The omission of the information about changes in the service organization's policies and procedures does not, however, warrant a qualification of the opinion on the fairness of presentation of the description because the description is fairly stated as of the date of the description. The explanatory paragraph should include the following:

- A description of the previous policy or procedure
- A description of the current policy or procedure
- An indication of when the change occurred

The following is an example of an explanatory paragraph that would be added to the service auditor's report before the opinion paragraph (the first opinion paragraph in a type 2 report) if disclosure about a significant change had not been included in the service organization's description of policies and procedures:

> The accompanying description states that the quality assurance group reviews a random sample of work performed by input clerks to determine the degree of compliance with the organization's input standards. Inquiries of staff personnel indicate that this procedure was first implemented on July 1, 19XX.

## Service Auditors' Recommendations for Improving Control Structure Policies and Procedures

Although it is not the objective of a service auditor's engagement, the service auditor may develop recommendations to improve the service organization's control structure policies and procedures. The service auditor and the service organization should agree as to how these recommendations will be communicated. In some situations, the service organization's management may request that the service auditor present this information in the service auditor's section of the report. In other situations, management may request that the service auditor include this information in a separate communication. Management's responses to such recommendations may also be included.

## Illegal Acts, Irregularities, or Uncorrected Errors at the Service Organization

In the course of performing procedures at a service organization, a service auditor may become aware of illegal acts, irregularities, or uncorrected errors attributable to the service organization's systems, management, or employees, that may affect one or more user organizations. For example, a bank trust department may inadvertently understate the amount of investment income that should be allocated to an employee benefit plan. Paragraph 23 of SAS No. 70 states that in such circumstances, unless clearly inconsequential, the service auditor should determine from the appropriate level of the service organization's management whether this information has been communicated to the affected user organizations. If management of the service organization has not communicated this information and is unwilling to do so, the service auditor should inform the service organization's audit committee or others with equivalent authority. If the audit committee does not respond appropriately, the service auditor should consider whether to resign from the engagement. The service auditor generally is not required to confirm with the user organizations that the service organization has communicated such information. If the user organizations have been notified in writing, the service auditor should consider requesting a copy of the written communication. In all cases, judgment should be used in determining what evidence should be obtained concerning the communication of such information and in determining whether the errors are significant enough to require disclosure in the service auditor's report. Unless expected to be significant, errors of a routine nature that recently have been identified in a reconciliation, and that are being corrected, generally would not be considered items that should be communicated to affected user organizations.

## Representation Letter from the Service Organization's Management

In all engagements, the service auditor should obtain written representations from the service organization's management. The representation let-

ter should be signed by members of the service organization's management whom the service auditor believes are responsible for and knowledgeable, directly or through others in the service organization, about the matters covered in the representations. Paragraph 57 of SAS No. 70 provides guidance as to the types of representations the service auditor should obtain. Additional matters to be included in the letter will be determined by the circumstances. The refusal by the service organization's management to provide the written representations considered necessary by the service auditor constitutes a limitation on the scope of the engagement that should be considered in forming the service auditor's opinion. The representation letter and the service auditor's report should each be dated as of the completion of fieldwork. An illustrative representation letter for a service auditor's engagement is presented in appendix B.

## Elements of the Service Organization's Description That Are Not Covered by the Service Auditor's Report

The service organization's description may contain information that is not covered by the service auditor's report. Examples of such information include the following:

- Information that is not included in the scope of the engagement
- Qualitative information, such as marketing claims, that may not be objectively measurable
- Information that would not be considered relevant to user organizations' internal control structures

If the service organization wishes to present such information, it should be placed in a separate section of the report entitled "Other Information Provided by the Service Organization," as described in chapter 3.

The fourth standard of reporting of the ten generally accepted auditing standards in SAS No. 1, *Generally Accepted Auditing Standards* (AICPA, *Professional Standards,* vol. 1, AU sec. 150) states:

> . . . In all cases where an auditor's name is associated with financial statements, the report should contain a clear-cut indication of the character of the auditor's work, if any, and the degree of responsibility the auditor is taking.

To adhere to the fourth standard of reporting, the service auditor should disclaim an opinion on information that is not covered by the service auditor's report. For example, consider a situation in which a data processing service organization provides payroll and inventory applications to its customers and the service auditor has been engaged to report on only the payroll application. If the service organization includes information about the inventory application in a separate section of the description, the service auditor should indicate in his or her report that the information about the inventory application is not covered by the service auditor's report. The service auditor's report should clearly identify the services or processing covered by the service auditor's report. The following is a sample

explanatory paragraph that would be added to the service auditor's report if information that is not covered by the report is included in the service organization's description:

> The information in section 4 describing Example Computer Service Organization's inventory application is presented by Example Computer Service Organization to provide additional information and is not a part of Example Computer Service Organization's description of control structure policies and procedures that may be relevant to user organizations' internal control structures. Such information has not been subjected to the procedures applied in the examination of the description of the payroll application, and accordingly, we express no opinion on it.

## Going-Concern Matters

In a financial statement audit, the auditor is required to consider whether there is substantial doubt about an entity's ability to continue as a going concern based on procedures performed and information obtained during the audit. Because of its nature and purpose, a service auditor's engagement does not provide the service auditor with a basis for determining whether there is substantial doubt about an entity's ability to continue as a going concern. Accordingly, a service auditor is not responsible for identifying or reporting going-concern matters related to the service organization when performing a service auditor's engagement.

## Reportable Conditions

Reportable conditions are matters coming to the auditor's attention during a financial statement audit that, in the auditor's judgment, should be communicated to the audit committee, or to individuals with a level of authority and responsibility equivalent to that of an audit committee. These matters are communicated because they represent significant deficiencies in the design or operation of the organization's internal control structure that could adversely affect the organization's ability to record, process, summarize, and report financial data consistent with management's assertions. The term *reportable conditions* specifically relates to audits of financial statements and not to service auditors' engagements. A service auditor is not in a position to identify reportable conditions at a service organization and is not responsible for identifying such conditions because a service auditor (1) is not performing an audit of the service organization's financial statements and, (2) is not aware of conditions existing at user organizations. Although a service auditor is not responsible for identifying reportable conditions, paragraphs 32 and 47 of SAS No. 70 require a service auditor to consider conditions that come to his or her attention that preclude the service auditor from obtaining reasonable assurance that specified control objectives would be achieved. The service auditor is required to disclose exceptions in the design or operation of control structure policies and procedures that cause the nonachievement of specified control objectives. The service auditor also is required to disclose any

other information, irrespective of specified control objectives, that comes to his or her attention that causes him or her to conclude (1) that design deficiencies exist that could adversely affect the ability to record, process, summarize, or report financial data to user organizations without error, and (2) that user organizations would not generally be expected to have policies and procedures in place to mitigate such design deficiencies. As discussed in chapter 3, "Using Type 1 and Type 2 Reports," it is the user auditor's responsibility to consider this and other information provided by the service organization when determining whether situations noted in the service auditor's report represent reportable conditions for user organizations.

## Related Parties

SAS No. 45, *Related Parties* (AICPA, *Professional Standards,* vol. 1, AU sec. 334), states:

> An audit performed in accordance with generally accepted auditing standards cannot be expected to provide assurance that all related party transactions will be discovered. Nevertheless, during the course of his audit, the auditor should be aware of the possible existence of material related party transactions that could affect the financial statements and of common ownership or management control relationships for which FASB Statement No. 57 [AC section R36] requires disclosure even though there are no transactions.

Because this concept is related to financial statement audits and not assertions about internal control, there is no requirement for the service organization to disclose such information in its description of policies and procedures. However, if a service organization is a subsidiary of another entity, and the service organization believes that such information would be relevant to user organizations, it may be disclosed in the service organization's description.

## Engagements to Provide a Service Auditor's Report on Only the General Data Processing Policies and Procedures of a Service Organization

Service organizations may engage an auditor to report on only the policies and procedures related to the general data processing of the service organization; this is sometimes called a *data center audit.* In such instances, the service auditor should determine whether such a report would provide information that would be relevant to user organizations. Refer to the discussion of "Responsibilities of the Service Auditor" at the beginning of this chapter for a discussion of the fair presentation of the service organization's description of policies and procedures. Such engagements generally are appropriate if the service organization provides only the computer hardware and system software, and user organizations provide their own application software (for example, certain types of data processing outsourcing), or if the user auditors are able to obtain sufficient information about application processing and application controls from other sources,

but are unable to obtain information about general computer controls from other sources. If a service organization is responsible for developing or changing application software or providing other transaction processing services, such as trust services or the reconciliation of transactions provided by user organizations, in addition to providing hardware or system software, a report on general data processing controls may not provide user auditors with a sufficient understanding of the service organization's control structure policies and procedures relevant to user organizations' internal control structures. For the description to be fairly presented in these circumstances, it should also describe the application processing and the flow of transactions.

Prior to accepting an engagement to report on the general data processing policies and procedures of a service organization that provides more than the hardware and system software for running user organizations' application software, the service auditor should consider, through discussion with management and review of standard contracts, how the report will most likely be used by the user organizations (for example, to plan the audit or to satisfy regulatory requirements). The service auditor is not responsible for contacting the user auditors to determine whether this type of report will meet their needs. If the report is likely to be used by user auditors to plan a financial statement audit, and information is not available from other sources, the service auditor should consider the propriety of accepting such an engagement because it will not sufficiently cover the relevant control structure policies and procedures at the service organization.

Chapter 5

# Service Organizations That Use Other Service Organizations

*This chapter describes how to apply the guidance in this APS to situations in which a service organization uses another service organization to perform some or all of the processing of the user organizations' transactions.*

As mentioned in previous chapters, a user organization may use a service organization that in turn uses another service organization (a *subservice organization).* The subservice organization may perform functions or processing that is significant to the service organization and to user organizations. To plan the audit and assess control risk, a user auditor may need to consider the control structure policies and procedures at the service organization (as discussed in chapter 1, "Audit Considerations If an Entity Uses a Service Organization"), and also may need to consider the control structure policies and procedures at the subservice organization. Similarly, a service auditor engaged to examine the control structure policies and procedures at a service organization and issue a service auditor's report may need to consider functions performed by a subservice organization and the effect of the subservice organization's policies and procedures on the service organization.

This chapter provides guidance for situations in which a subservice organization performs functions that are significant to the processing of user organization transactions. The concepts and guidance in previous chapters provide the basis for the additional guidance in this chapter; accordingly, readers should consider this chapter in the context of this entire APS.

## EXAMPLES OF SUBSERVICE ORGANIZATIONS AND SUBSERVICING SITUATIONS

Examples of subservicing can be found in virtually all types of applications and industries. The following paragraphs illustrate typical subservicing sit-

uations for a bank's trust department that provides services to employee benefit plans.

As discussed in the introduction of this APS, a bank trust department that provides services to employee benefit plans may be considered a service organization to those plans. The trust department may perform all of the functions involved in transaction processing (in which case this chapter does not apply), or it may use a subservice organization to perform a portion of the transaction processing. Subservice organizations may perform specific aspects of the transaction processing or may perform all of the transaction processing. Examples of the range of services subservice organizations may perform include the following:

- *Subservice organizations that perform limited functions.* A bank trust department may use one or more subservice organizations to determine the current market price of exchange-traded securities owned by employee benefit plans. Some pricing service organizations specialize in a specific type of security. The trust department may engage several pricing service organizations to determine the price of different types of securities. The trust department may also engage more than one pricing service organization to obtain comparative prices for the same securities and thereby have a basis for determining the reasonableness of the pricing. In the situation described above, the functions performed by each subservice organization are limited. Nevertheless, the functions performed by each subservice organization may be significant to the user organizations' internal control structures and to assertions in the user organizations' financial statements.
- *Subservice organizations that perform 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 employee benefit plans. In such a situation, the trust department may establish controls over the processing performed by the subservice organization, although, more commonly, the trust department relies on the subservice organization's control structure policies and procedures to achieve certain applicable control objectives.
- *Subservice organizations that perform extensive functions.* A bank trust department may use a service organization to perform essentially all of the transaction execution, recording, and processing for the employee benefit plans. In such a situation (which is commonly referred to as *private labeling*), the trust department's functions might be limited to establishing and maintaining the account relationship. The trust department relies on the subservice organization to perform essentially all of the functions and controls that affect user organizations and their internal control structures. In this case, the trust department's control structure policies and procedures would have a minimal effect on the internal control structures of user organizations, and the subservice organization's con-

trol structure policies and procedures would be significant to the user organizations' internal control structures and to assertions in the user organizations' financial statements.

## THE EFFECT OF A SUBSERVICE ORGANIZATION ON A USER ORGANIZATION'S INTERNAL CONTROL STRUCTURE

The involvement of a service organization and a subservice organization in the processing of transactions does not diminish the user auditor's responsibility to obtain a sufficient understanding of the entity's internal control structure to plan the audit. The use of a service organization that uses a subservice organization may require the user auditor to consider the control structure policies and procedures at the service organization and at the subservice organization, depending on the functions each performs.

Paragraphs 6 through 17 of SAS No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, *Professional Standards*, vol. 1, AU sec. 324), provide guidance to user auditors on considering the effect of a service organization on the internal control structure of a user organization. Although paragraphs 6 through 17 do not specifically refer to subservice organizations, if a subservice organization is used, the guidance in these paragraphs should be interpreted to include the subservice organization. Examples of how the user auditor considers the effect of a subservice organization on the internal control structure of a user organization are the following.

- In situations in which subservice organizations are used, the interaction described in paragraph 6 of SAS No. 70 would involve the user organization, the service organization, and the subservice organization. The degree of this interaction, as well as the nature and materiality of the transactions processed by the service organization and subservice organization, are the most important factors to consider in determining the significance of the subservice organization's control structure policies and procedures to the user organization's internal control structure.
- The factors listed in paragraph 8 of SAS No. 70, which a user auditor considers in determining the significance of control structure policies and procedures of a service organization to planning the audit of a user organization's financial statements, should also be considered with respect to a subservice organization.
- When applying the guidance in paragraph 9 of SAS No. 70 to situations involving a subservice organization, the user auditor should consider the available information about both the service organization's and the subservice organization's control structure policies and procedures, including (1) information in the user organization's possession, such as user manuals, system overviews, and technical manuals; and (2) reports on the service organization's and subservice organization's control structure poli-

> cies and procedures, such as reports by service auditors (on the service organization, subservice organization, or the service organization and subservice organization together), internal auditors (the user organization's, the service organization's, or the subservice organization's), or regulatory authorities. Because a user organization typically does not have any contractual relationship with the subservice organization, a user organization should obtain available reports and information about the subservice organization from the service organization.

After considering the above factors and evaluating the available information, the user auditor may conclude that he or she has the means to obtain a sufficient understanding of the internal control structure of the user organization 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.

Paragraphs 11 through 16 of SAS No. 70 address the approach a user auditor should follow in assessing control risk at a user organization. If a subservice organization is used, the user auditor may need to consider activities at both the service organization and the subservice organization in applying the guidance in these paragraphs.

## RESPONSIBILITIES OF SERVICE ORGANIZATIONS, USER AUDITORS, AND SERVICE AUDITORS IF CONTROL OBJECTIVES ARE ESTABLISHED BY THE SERVICE ORGANIZATION

The guidance in chapter 2, "Form and Content of Reports on the Processing of Transactions by Service Organizations," is applicable whether or not a subservice organization is used. In addition to this guidance, appendixes C and D and the remainder of this chapter summarize how the responsibilities of service organizations, user auditors, and service auditors are affected when a subservice organizations performs significant functions for a service organization.

A service auditor engaged to issue a report on the control structure policies and procedures of a service organization that uses a subservice organization should consider whether the functions and processing performed by the subservice organization are significant. If the subservice organization's functions are not significant to the user organization, appendixes C and D do not apply and there is no need to further consider the subservice organization's functions in the service auditor's engagement. *Significance* in this case should be determined in the same manner that

the significance of a service organization to a user organization is determined as described in paragraph 6 of SAS No. 70 and chapter 1 of this APS; that is, based on the nature of the services provided by the subservice organization to the service organization and considered in reference to the user organization.

## Responsibilities of Service Organizations

If the service organization establishes the control objectives, the service organization's description of policies and procedures should include the following items:

- A description of the control structure policies and procedures at the service organization that may be relevant to user organizations' internal control structures, as described in paragraph 26 of SAS No. 70 and chapter 2 of this APS.
- The control objectives established by the service organization, as described in paragraph 34*a* of SAS No. 70 and chapter 2 of this APS.

These items are required regardless of whether a subservice organization is involved.

In addition, the service organization should describe the functions and nature of the processing performed by the subservice organization in sufficient detail for user auditors to understand the significance of the subservice organization's functions to the processing of the user organizations' transactions. Ordinarily, disclosure of the identity of the subservice organization is not required. However, if the service organization determines that the identity of the subservice organization would be relevant to user organizations, the name of the subservice organization may be included in the description. The purpose of the description of the functions and nature of the processing performed by the subservice organization is to alert user organizations and their auditors to the fact that another entity (the subservice organization) is involved in the processing of the user organizations' transactions and to summarize the functions the subservice organization performs.

The service organization determines whether its description of control structure policies and procedures will include the relevant control structure policies and procedures of the subservice organization. The two alternative methods of presenting the description are the following:

- *The carve-out method.* The subservice organization's relevant control objectives and control structure policies and procedures are excluded from the description and from the scope of the service auditor's engagement. The service organization states in the description that the subservice organization's control structure policies and procedures and related control objectives are omitted from the description and that the control objectives in the report include only the objectives the service organization's control structure policies and procedures are intended to achieve.

- *The inclusive method.* The subservice organization's relevant control structure policies and procedures are included in the description and in the scope of the engagement. The description should clearly differentiate between control structure policies and procedures of the service organization and control structure policies and procedures of the subservice organization. The set of control objectives includes all of the control objectives a user auditor would expect both the service organization and the subservice organization to achieve. To accomplish this, the service organization should coordinate the preparation and presentation of the description of policies and procedures with the subservice organization.

In either method, the service organization includes in its description of policies and procedures a description of the functions and nature of the processing performed by the subservice organization.

Although the inclusive method provides more information to user auditors, it may not be appropriate or feasible in all circumstances. In determining which approach to follow, the service organization should consider (1) the nature and extent of information about the subservice organization that user auditors will require, and (2) the practical difficulties entailed in implementing the inclusive method as described in the following section.[1]

## Responsibilities of User Auditors

If the functions performed by the subservice organization are limited, the carve-out method generally will provide user auditors with sufficient information about the subservice organization because the description will indicate the functions performed by the subservice organization and may include information about controls exercised by the service organization over the activities of the subservice organization. If the functions performed by the service organization are more extensive, the user auditor may require more information about the subservice organization's control structure policies and procedures. Such information may be available from other sources such as those listed in paragraph 9 of SAS No. 70, which include systems overviews, technical manuals, and reports on the subservice organization's control structure policies and procedures, such as reports by a subservice auditor, internal auditors, or a regulatory authority.

An inclusive report is generally most useful in the following circumstances.

- The subservice organization's functions are extensive.
- User auditors require more information than that provided by the carve-out method.
- Information from other sources is not readily available.

1. This APS does not provide for the option of having a service auditor make reference to or rely on a subservice auditor's report as the basis, in part, for a service auditor's opinion.

However, this approach is difficult to implement and may be impossible to execute in certain circumstances. The approach requires extensive planning and communication between the service auditor, the service organization, and the subservice organization. Both the service organization and the subservice organization must agree on this approach before it is adopted. Matters such as the following must be coordinated by all of the parties involved:

- The scope and timing of the examination
- The responsibilities for the preparation and content of the service organization's and subservice organization's description of policies and procedures
- The timing of the tests of controls
- Responsibilities for the content of the representation letters and signatures to be obtained
- Other administrative matters

Such issues become more complex if multiple subservice organizations are involved. The approach is facilitated if the service organization and the subservice organization are related parties or have a contractual relationship that provides for inclusive reports and visits by service auditors. If the inclusive method is not a practical or feasible alternative and additional information is required, the user auditor should consider the guidance in paragraph 10 of SAS No. 70.

If the service organization establishes the control objectives, the user auditor should determine whether the report meets the user auditor's needs. If the user auditor needs additional information about the functions performed by the subservice organization or about the control structure policies and procedures at the subservice organization, the user auditor should consider obtaining such information about the subservice organization in the manner described in paragraphs 7 through 21 of SAS No. 70.

## Responsibilities of Service Auditors

If the service organization establishes the control objectives, the service auditor should —

- Disclose in the service auditor's report that the control objectives were established by the service organization, as required by paragraphs 29*c* and 44*c* of SAS No. 70. (The service auditor should be satisfied that the control objectives are reasonable in the circumstances and consistent with the service organization's contractual obligations, as required by paragraph 35 of SAS No. 70.)
- Report on (1) the fairness of the presentation of the description of policies and procedures placed in operation, (2) whether the policies and procedures were suitably designed to achieve specified control objectives, and (3) for type 2 reports, whether the policies

and procedures that were tested were operating with sufficient effectiveness to achieve the related control objectives.

These requirements are also applicable if a subservice organization is not involved.

If the functions and processing performed by the subservice organization are significant to the processing of the user organizations' transactions, and the service organization does not disclose the existence of a subservice organization and the functions it performs, the service auditor should request that management of the service organization amend the description to disclose the required information. If management does not amend the description, the service auditor should issue a qualified or adverse opinion as to the fairness of the presentation of the description of policies and procedures.

If the service organization has adopted the carve-out method, the service auditor should modify the scope paragraph of the service auditor's report to briefly summarize the functions and nature of the processing performed by the subservice organization. This summary ordinarily would be briefer than the information provided by the service organization in its description of the functions and nature of the processing performed by the subservice organization. The service auditor should include a statement in the scope paragraph of the service auditor's report indicating that the description of policies and procedures includes only the control structure policies and procedures and related control objectives of the service organization; accordingly, the service auditor's examination does not extend to control structure policies and procedures of the subservice organization. An example of the scope paragraph of a service auditor's report using the carve-out method is presented in the following section. Additional or modified report language is shown in boldface italics.

## Sample Scope Paragraph of a Service Auditor's Report Using the Carve-Out Method

Independent Service Auditor's Report

To the Board of Directors of Example Trust Organization:

We have examined the accompanying description of the policies and procedures of Example Trust Organization applicable to the processing of transactions for users of the institutional trust division. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Example Trust Organization's policies and procedures that may be relevant to a user organization's internal control structure; (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if those policies and procedures were complied with satisfactorily, and user organizations applied the internal control structure policies and procedures contemplated in the design of Example Trust Organization's policies and procedures; and (3) such policies and procedures had been placed in operation as of June 30,

19XX. ***Example Trust Organization uses a computer processing service organization for all of its computerized application processing. The accompanying description includes only those policies and procedures and related control objectives of Example Trust Organization, and does not include policies and procedures and related control objectives of the computer processing service organization. Our examination did not extend to policies and procedures of the computer processing service organization.*** The control objectives were specified by the management of Example Trust Organization. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

[*The remainder of the report is the same as the standard service auditor's report presented in paragraphs 38 and 54 of SAS No. 70.*]

If the service organization has used the inclusive method, the service auditor should perform procedures comparable to those described in paragraph 12 of SAS No. 70. Such procedures may include performing tests of the service organization's controls over the activities of the subservice organization or performing procedures at the subservice organization. If the service auditor will be performing procedures at the subservice organization, the service organization should arrange for such procedures. The service auditor should recognize that the subservice organization generally is not the client for the engagement. Accordingly, in these circumstances, the service auditor should determine whether it will be possible to obtain the required evidence to support the portion of the opinion covering the subservice organization and whether it will be possible to obtain an appropriate letter of representations regarding the subservice organization's control structure policies and procedures.

An example of a service auditor's report using the inclusive method is presented below. Additional or modified report language is shown in boldface italics.

## Sample Service Auditor's Report Using the Inclusive Method

Independent Service Auditor's Report

To the Board of Directors of Example Trust Organization:

We have examined the accompanying description of the policies and procedures of Example Trust Organization ***and Computer Processing Service Organization, an independent service organization that provides computer processing services to Example Trust Organization,*** applicable to the processing of transactions for users of the institutional trust division. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Example Trust Organization's and ***Computer Processing Service Organization's*** policies and procedures that may be relevant to a user organization's internal control structure; (2) the control structure policies and procedures included in the description were suitably

designed to achieve the control objectives specified in the description, if those policies and procedures were complied with satisfactorily, and user organizations applied the internal control structure policies and procedures contemplated in the design of Example Trust Organization's policies and procedures; and (3) such policies and procedures had been placed in operation as of June 30, 19XX. The control objectives were specified by the management of Example Trust Organization. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned policies and procedures presents fairly, in all material respects, the relevant aspects of Example Trust Organization's ***and Computer Processing Service Organization's*** policies and procedures that had been placed in operation as of June 30, 19XX. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily and user organizations applied the internal control structure policies and procedures contemplated in the design of Example Trust Organization's policies and procedures.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific policies and procedures, listed in Schedule X, to obtain evidence about their effectiveness in meeting the control objectives, described in Schedule X, during the period from January 1, 19XX, to June 30, 19XX. The specific policies and procedures and the nature, timing, extent, and results of the tests are listed in Schedule X. This information has been provided to user organizations of Example Trust Organization and to their auditors to be taken into consideration, along with information about the internal control structure of user organizations, when making assessments of control risk for user organizations. In our opinion, the policies and procedures that were tested, as described in Schedule X, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Schedule X were achieved during the period from January 1, 19XX, to June 30, 19XX.

The relative effectiveness and significance of specific policies and procedures at Example Trust Organization ***and Computer Processing Service Organization*** and their effect on assessments of control risk at user organizations are dependent on their interaction with the policies, procedures, and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of policies and procedures at individual user organizations.

The description of policies and procedures at Example Trust Organization and ***Computer Processing Service Organization*** is as of June 30, 19XX, and the information about tests of the operating effectiveness of specified policies and procedures covers the period from January 1, 19XX, to June 30, 19XX. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specified policies and procedures at Example Trust Organization ***and Computer Processing Service Organization*** is subject to inherent limitations and, accordingly, errors or

irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report is intended solely for use by the management of Example Trust Organization, users of its institutional trust division, and the independent auditors of its users.

July 10, 19XX

Performing procedures at the subservice organization will require coordination and communication between the service organization, the subservice organization, and the service auditor. This alternative may be less difficult to implement if the service organization and the subservice organization are related or if the contract between the service organization and the subservice organization provides for visits by the service organization's auditors.

A service auditor should question accepting an engagement in which a service organization functions primarily as an intermediary between the user organizations and the subservice organization, and performs few or no functions that affect transaction processing for user organizations. If the service organization's control structure policies and procedures are so limited that there are no relevant control objectives, a report on its policies and procedures would not be useful to user auditors in planning the audit.

Although when using the carve-out method, the control objectives typically address only policies and procedures at the service organization, situations may arise in which the service organization specifies control objectives whose achievement depends on control structure policies and procedures at a subservice organization. In these situations, the service auditor should consider modifying the scope and opinion paragraphs of the report in a manner similar to the modifications made for user control considerations, as specified in footnote 3 to paragraph 54 of SAS No. 70.

## RESPONSIBILITIES OF SERVICE ORGANIZATIONS, USER AUDITORS, AND SERVICE AUDITORS IF CONTROL OBJECTIVES ARE ESTABLISHED BY AN OUTSIDE PARTY

If an outside party establishes the control objectives, the responsibilities of the service organization, user auditors, and service auditors do not change except for the following items, as indicated in the table in appendix D.

- The service organization should describe the control objectives established by the outside party and the source of the control objectives.
- The service auditor does not need to determine whether the control objectives are reasonable in the circumstances and con-

sistent with the service organization's contractual obligations because the control objectives have been established by an outside party.

## SUBSERVICE ORGANIZATIONS THAT MAINTAIN CUSTODY OVER SECURITIES

Many service organizations, such as bank trust departments, use subservice organizations to maintain custody and safekeeping of securities (custodial organizations). Such custodial organizations may perform some or all of the following services:

- Maintaining physical custody of marketable securities and records of the securities held for the entities (In some cases, physical custody may be replaced by electronic recordkeeping)
- 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 the entities
- Receiving notification of security purchase and sale transactions on behalf of entities for which it 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

In such situations, confirmation procedures may provide substantive audit evidence of the existence of securities and ownership by the user organizations. A service auditor's report on the custody and safekeeping subservice organization may also provide useful information to user organizations, user auditors, service organizations, and service auditors regarding the controls over custody, safekeeping, and any other functions such custodians may perform.

Other types of reports related to the internal control structure of a service organization, such as those listed in chapter 1, or reports issued pursuant to regulatory requirements may also be useful to user organizations and their auditors.

Appendix A

# Examples of Service Auditors' Reports, Descriptions of Policies and Procedures Placed in Operation, and Descriptions of Tests of Operating Effectiveness

Although SAS No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, *Professional Standards,* vol. 1, AU sec. 324), is fairly specific about the information that should be included in a type 1 or type 2 report, it is not specific about the format for these reports. Service organizations and service auditors may organize and present the required information in a variety of formats. Following are three examples of type 2 reports presented for illustrative purposes. The concepts illustrated in these type 2 reports also apply to type 1 reports, which are not illustrated. The reports are for Example Computer Service Organization and Example Trust Organization and illustrate the reporting guidance presented in chapter 2, "Form and Content of Reports on the Processing of Transactions by Service Organizations," chapter 3, "Using Type 1 and Type 2 Reports," and chapter 4, "Performing a Service Auditor's Engagement." The examples illustrate three different methods of organizing a type 2 report. For brevity, the sample reports do not include everything that might be described in a type 2 report. Ellipses (. . .) or notes to readers indicate places where detail has been omitted from the sample reports.

The control objectives and control structure policies and procedures specified by the sample service organizations in the sample reports, as well as the testing performed by the sample service auditors, are presented for illustrative purposes only. They are not intended to represent a complete or standard set of control objectives, control structure policies and procedures, or tests of operating effectiveness that would be applicable to all service organizations. The determination of the appropriate control objectives, control structure policies and procedures, and tests of operating effectiveness for a specific service organization can only be made in the context of

specific facts and circumstances. Accordingly, it is expected that actual service auditors' reports will present differing control objectives, control structure policies and procedures, and tests of operating effectiveness.

The sample report in example 1 for Example Computer Service Organization contains the four sections described in chapter 2 of this APS. The service organization's control objectives and related control structure policies and procedures are included in section II of the report, "Example Computer Service Organization's Description of Policies and Procedures." The control objectives and related policies and procedures *that were tested* are repeated in section III, "Information Provided by the Service Auditor." In this sample report, a number of the control objectives included in the service organization's description of policies and procedures were not tested by the service auditor for operating effectiveness. Additionally, for the control objectives that were tested for operating effectiveness, the service auditor may not have tested all of the control structure policies and procedures listed in the service organization's description for that control objective. The service auditor determines which control structure policies and procedures will be tested and the nature, timing, and extent of the tests that will be performed to determine whether a control objective has been achieved.

Example 2 is also based on Example Computer Service Organization. In Example 2, however, the control objectives and related control structure policies and procedures are omitted from section II, "Example Computer Service Organization's Description of Policies and Procedures," and are only presented in section III, "Information Provided by the Service Auditor." The purpose of this presentation is to eliminate the redundancy that would result if the control objectives and related control structure policies and procedures were listed in both sections of the report. A paragraph is included in section II alerting readers to the fact that the control objectives and related control structure policies and procedures presented in section III are the responsibility of the service organization and should be considered part of the service organization's description. In this example, the reader is to assume that all of the control objectives were tested for operating effectiveness.

Example 3 is based on Example Trust Organization. In this sample report, the service organization's control objectives and related control structure policies and procedures as well as the tests performed by the service auditor, and the results of the tests are presented in section II, "Example Trust Organization's Description of Policies and Procedures." As in example 2, the objective of this method of presentation is to avoid the redundancy that would result from presenting the same material in two sections. A paragraph is included in section III indicating that the tests of operating effectiveness and results of the tests presented in section II are the responsibility of the service auditor and should be considered part of the service auditor's section. In this example, the reader is to assume that all of the control objectives were tested for operating effectiveness.

**Example 1**

# EXAMPLE COMPUTER SERVICE ORGANIZATION

## Report on Policies and Procedures Placed in Operation and Tests of Operating Effectiveness

### Table of Contents



* Items marked with an asterisk are presented in the table of contents for illustrative purposes only and are not included in this sample report.

* Items marked with an asterisk are presented in the table of contents for illustrative purposes only and are not included in this sample report.

# I

# INDEPENDENT SERVICE AUDITOR'S REPORT

To the Board of Directors of Example Computer Service Organization:

We have examined the accompanying description of the Savings, Mortgage Loan, and Consumer Loan applications of Example Computer Service Organization. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Example Computer Service Organization's policies and procedures that may be relevant to a user organization's internal control structure; (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if those policies and procedures were complied with satisfactorily, and user organizations applied the internal control structure policies and procedures contemplated in the design of Example Computer Service Organization's policies and procedures; and (3) such policies and procedures had been placed in operation as of June 30, 19XX. The control objectives were specified by the management of Example Computer Service Organization. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned applications presents fairly, in all material respects, the relevant aspects of Example Computer Service Organization's policies and procedures that had been placed in operation as of June 30, 19XX. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily and user organizations applied the internal control structure policies and procedures contemplated in the design of Example Computer Service Organization's policies and procedures.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specified policies and procedures, included in section III of this report, to obtain evidence about their effectiveness in meeting the control objectives described in section III during the period from January 1, 19XX to June 30, 19XX. The specified policies and procedures and the nature, timing, extent, and results of the tests are listed in section III. This information has been provided to user organizations of Example Computer Service Organization and their auditors to be taken into consideration, along with information about the internal control structures at user organizations, when making

assessments of control risk for user organizations. In our opinion, the policies and procedures that were tested, as described in section III of this report, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in section III were achieved during the period from January 1, 19XX to June 30, 19XX. However, the scope of our engagement did not include tests to determine whether control objectives not listed in section III were achieved; accordingly, we express no opinion on the achievement of control objectives listed in section II of this report and not included in section III.

The relative effectiveness and significance of specific policies and procedures at Example Computer Service Organization and their effect on assessments of control risk at user organizations are dependent on their interaction with the policies, procedures, and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of policies and procedures at individual user organizations.

The description of policies and procedures at Example Computer Service Organization is as of June 30, 19XX, and information about tests of the operating effectiveness of specified policies and procedures covers the period from January 1, 19XX, to June 30, 19XX. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specified policies and procedures at Example Computer Service Organization is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

The information included in section IV of this report is presented by Example Computer Service Organization to provide additional information to user organizations and is not a part of Example Computer Service Organization's description of policies and procedures placed in operation. The information in section IV has not been subjected to the procedures applied in the examination of the description of the Savings, Mortgage Loan, and Consumer Loan applications, and accordingly, we express no opinion on it.

This report is intended solely for use by the management of Example Computer Service Organization, its users, and the independent auditors of its users.

July 10, 19XX

# II

# EXAMPLE COMPUTER SERVICE ORGANIZATION'S DESCRIPTION OF POLICIES AND PROCEDURES

## OVERVIEW OF OPERATIONS

Example Computer Service Organization (the Organization) is located in Los Angeles, California, and provides computer services primarily to user organizations in the financial services industry. Applications enable user organizations to process savings, mortgage loan, consumer loan, commercial loan, and general ledger transactions. This description only addresses the control structure policies and procedures related to the Savings, Mortgage Loan, and Consumer Loan applications. Section IV of this report contains certain information about the Commercial Loan and General Ledger applications.

Numerous terminals located at user organizations are connected to the Organization through leased lines that provide on-line, real-time activity for the applications. The Organization processes transactions using one ABC central processor under the control of Operating System Release 2.1. . . .

## CONTROL ENVIRONMENT ELEMENTS

Operations are under the direction of the president and the board of directors of the Organization. The board of directors has established an audit committee that oversees the internal audit function. The Organization employs a staff of approximately 35 people and is supported by the functional areas listed below.

- *Administration/systems development.* Coordinates all aspects of the service organization's operations including service billing. Identifies areas requiring internal controls and implements those controls. Performs systems planning, development, and implementation. Reviews network operations and telecommunications, and performs disaster-recovery planning and database administration.
- *Customer support.* Supports end-users in all aspects of their use of the application system, including research and resolution of identified problems. Administers application security (including passwords), changes to application parameters, and distribution of user documentation.
- *Application programming.* Performs regular maintenance programming, programming for user-requested enhancements, and updates the systems documentation.

- *Terminal support.* Performs end-user terminal training. Researches and resolves terminal and network problems and performs timely installations of enhancements to terminal and network software.
- *Operations.* Manages daily computer operations, nightly production processing, report production and distribution, and system utilization and capacities.
- *Marketing.* Provides analysis for new business prospects and new product planning.

The managers of each of the functional areas report to the director of information systems.

The Organization's employees are not authorized to initiate or authorize transactions, to change or modify user files except through normal production procedures, or to correct user errors. All shifts at the Organization are managed by shift supervisors and the director of information systems. Incident reports, processing logs, job schedules, and equipment activity reports are monitored by the director of information systems. These reports track daily processing activities and identify hardware and software problems and system usage.

Weekly management meetings are held to discuss special processing requests, operational performance, and the development and maintenance of projects in process.

Written position descriptions for employees are maintained by the director of information systems and the personnel department. The descriptions are reviewed annually and revised as necessary.

References are sought and background, credit, and security checks are conducted for all Organization personnel hired. The confidentiality of user-organization information is stressed during the new-employee orientation program and is emphasized in the personnel manual issued to each employee. The Organization provides a mandatory orientation program to all full-time employees and encourages employees to attend other formal outside training. An internal supervisory training program was recently initiated.

Employees are required to take vacation in accordance with the Organization's policy, which requires that all employees who are eligible for two or more weeks of vacation take off five consecutive business days during each calendar year. No employee may take vacation during the last week or the first ten days of each quarter. Vacation must be taken in the calendar year in which it is earned.

The Organization's policy requires that after three months of employment, new employees receive a written performance evaluation from their supervisors, and that all employees receive an annual written performance evaluation and salary review. These reviews are based on employee-stated goals and objectives that are prepared and reviewed with each employee's supervisor. Completed appraisals are reviewed by senior management and become a permanent part of the employee's personnel file.

The internal auditors provide the audit committee with an appraisal of internal controls. The internal auditors execute an information-technology

internal audit program, and follow-up on any operational exceptions or concerns that may arise. The internal auditors use audit software to perform various recalculations and analyses using actual production data in an off-line mode.

## APPLICATION PROCESSING

### Overview of the Flow of Transactions

The Organization's Savings, Mortgage Loan, and Consumer Loan applications are part of an integrated software system. This system provides on-line, real-time processing of monetary and nonmonetary transactions and provides batch and memo postprocessing capabilities. Processing activities are divided into on-line and off-line processing segments. During normal business hours, user organizations may make inquiries and enter monetary and nonmonetary transactions through various terminals, including teller terminals. Additional input is provided from automatic teller machine (ATM) transactions, transactions from the Federal Reserve Bank, and other transactions received from user banks. Such transactions are received via electronic data transmission or via tape delivered by courier.

Each application uses the standard operating system and related systems software to interact with terminals, to accept data, to apply prescribed processes to data, to maintain an audit trail, and to respond to inquiries.

On-line daily processing occurs during preestablished hours when customer banks are open. Monetary, nonmonetary, and inquiry transactions are entered at teller terminals located at branch offices of user organizations serviced by the Organization. Nonmonetary and inquiry transactions are entered at other terminals designated as administrative terminals in branch offices and other offices of user organizations. Terminals are linked to the on-line data communications network through leased telephone lines. Telecommunications software polls the terminals in the network for available input transactions . . . .

Off-line daily processing is performed in accordance with daily schedules and generally occurs when the on-line system is not running. These programs determine whether control totals agree with the totals of related detail accounts, modify database fields, and produce daily and special-request reports.

Following is a description of the Savings, Mortgage Loan, and Consumer Loan applications.

### Savings Application

The Savings application maintains account balances based on deposits, withdrawals, earnings postings, journal debits and credits, and other transactions. The application provides for on-line data entry and inquiry functions and on-line, real-time posting of monetary and nonmonetary transactions entered through teller terminals . . . .

***Note to Readers:*** *The remainder of the description of the Savings application and the descriptions of the Mortgage Loan and Consumer Loan applications are not presented in this sample report.*

## CONTROL OBJECTIVES AND RELATED POLICIES AND PROCEDURES

### General Computer Controls

#### *Systems Development and Maintenance*

*Control objective 1.* Control structure policies and procedures provide reasonable assurance that changes to existing applications are authorized, tested, approved, properly implemented, and documented.

*Description of policies and procedures.* Each user organization designates the individuals who are authorized to request program changes. All program-change requests are submitted in writing to the manager of customer support. The manager of customer support maintains a log of all program-change requests received. Once a program-change request has been received and logged, it is reviewed by personnel in the customer support department to determine whether the requested change is an enhancement of a program or the correction of a programming error, and to develop an estimate of the number of hours that will be required to make and implement the program change.

Biweekly management meetings are held with the director of information systems, the manager of application programming, and representatives of the user organizations to consider program-change requests and the status of active projects. Based on these discussions, the director of information systems approves or disapproves the change request. Upon approval, the director of information systems signs off on the program-change request and forwards it to the manager of application programming.

The manager of application programming receives approved program-change requests and prepares a customer-work request (CWR) form. The form contains the following information: the name of the originator, the bank name, the bank's user code, the program affected, and a description of the requested program change. A log of all CWRs is maintained and monitored by the manager of application programming.

The director of information systems must authorize change-control personnel to release production-program source code to the programmer. The programming staff does not have direct access to production-program source code. The programmer makes changes to program code using a program-development library. The programmer does not have the ability to compile a changed program into executable form in the production environment. Programming changes are made using an on-line programming utility and changes to source code are generated and annotated with the date of the change. Depending on the change, program-unit tests and sys-

tem tests are completed by the programmer and reviewed by the manager of application programming.

Acceptance tests are performed using test files, and the resulting output is verified by the requesting party. Recently processed production data is used as test data, without updating any live files. If the program change involves a new function, test data is jointly developed by the programmer and the requesting party. All test results are verified by the programmer, the manager of application programming, and the requesting party. At the completion of all testing, the programmer, the manager of application programming, and the requesting party sign off on the CWR.

After acceptance tests are completed, the director of information systems reviews all test results and documentation. If the director is satisfied with the program change, he or she authorizes change-control personnel to compile the new source code in the production environment and sign off on the CWR. Updates to the production libraries are performed by change-control personnel after authorization by the director of information systems. Each time a program is compiled in the production environment, an entry is electronically recorded in a log that is printed and reviewed daily for any unauthorized activity.

Documentation is updated by the programmer, reviewed by the manager of application programming, and distributed to the appropriate parties.

***Note to Readers:*** *The control structure policies and procedures related to control objectives 2 through 9 are not presented in this sample report.*

*Control objective 2.* Control structure policies and procedures provide reasonable assurance that new applications being developed are authorized, tested, approved, properly implemented, and documented.

*Control objective 3.* Control structure policies and procedures provide reasonable assurance that changes to the existing system software and implementation of new system software are authorized, tested, approved, properly implemented, and documented.

### *Access*

*Control objective 4.* Control structure policies and procedures provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

*Control objective 5.* Control structure policies and procedures provide reasonable assurance that logical access to data files is restricted to properly authorized individuals.

### *Computer Operations*

*Control objective 6.* Control structure policies and procedures provide reasonable assurance that processing is appropriately scheduled and that deviations from scheduled processing are identified and resolved.

*Control objective 7.* Control structure policies and procedures provide reasonable assurance that data transmissions between the Organization and its user organizations are complete, accurate, and secure.

## Savings Application Controls

*Control objective 8.* Control structure policies and procedures provide reasonable assurance that savings deposit and withdrawal transactions are received from authorized sources.

*Control objective 9.* Control structure policies and procedures provide reasonable assurance that savings deposit and withdrawal transactions received from the user organizations are initially recorded completely and accurately.

*Control objective 10.* Control structure policies and procedures provide reasonable assurance that programmed interest and penalties are calculated in conformity with the description.

***Note to Readers:*** *Control objective 10 illustrates a situation in which the application of a specific user organization internal control structure policy or procedure is required to achieve the control objective. See "User Control Considerations" below and paragraph 46 of SAS No. 70.*

*Description of policies and procedures.* Application security restricts update access to user-defined indices for calculating interest and penalties to the appropriate user organization. Within each user organization, passwords are required to update or change the indices.

Programs used to calculate interest and penalties are subject to the control structure policies and procedures described for control objective 1, "Control structure policies and procedures provide reasonable assurance that changes to existing applications are authorized, tested, approved, properly implemented, and documented."

*User control considerations.* User organizations are responsible for establishing controls at the user organizations to restrict access to and change of user-defined indices to authorized user-organization personnel. Any index can be selected and changed on-line at any time by a user organization with an appropriate password. The balances applicable to each rate are established by the user organizations in account-type parameters. A report can be produced that shows the current content of the indices and the date they were last changed.

***Note to Readers:*** *The control structure policies and procedures related to control objectives 11 through 14 are not presented in this sample report.*

*Control objective 11.* Control structure policies and procedures provide reasonable assurance that processing is performed in accordance with user specifications.

*Control objective 12.* Control structure policies and procedures provide reasonable assurance that data maintained on files remain authorized, complete, and accurate.

*Control objective 13.* Control structure policies and procedures provide reasonable assurance that output data and documents are complete and accurate and distributed to authorized recipients on a timely basis.

### Other

*Control objective 14.* Control structure policies and procedures provide reasonable assurance that the service organization can provide continuity of operations.

## USER CONTROL CONSIDERATIONS

The Organization's applications were designed with the assumption that certain internal control structure policies and procedures would be implemented by user organizations. In certain situations, the application of specified internal control structure policies and procedures at user organizations is necessary to achieve certain control objectives included in this report. In such instances, those user-organization internal control structure policies and procedures are indicated under the related control objective in section II of this report.

This section describes other internal control structure policies and procedures that should be in operation at user organizations to complement the control structure policies and procedures at the Organization. User auditors should consider whether the following policies and procedures have been placed in operation at user organizations:

- Policies and procedures to ensure that changes to processing options (parameters) are appropriately authorized, implemented, and approved
- Policies and procedures to ensure that transactions are appropriately authorized, complete, and accurate
- Policies and procedures to ensure that erroneous input data are corrected and resubmitted
- Policies and procedures to ensure that output reports are reviewed by appropriate users for completeness and accuracy
- Policies and procedures to ensure that output received from the Organization is routinely reconciled to relevant control totals

The list of user-organization control considerations presented above is not a comprehensive list of all internal control structure policies and procedures that should be applied by user organizations. Other internal control structure policies and procedures may be needed at user organizations.

# III

# INFORMATION PROVIDED BY THE SERVICE AUDITOR

## TESTS OF CONTROL ENVIRONMENT ELEMENTS

In addition to the tests of operating effectiveness of specified control structure policies and procedures described in this section, our procedures also included consideration and tests of the following relevant elements of the Organization's control environment:

- Organizational structure
- Personnel policies and practices
- Management's control methods for monitoring and following up on performance, including internal audit
- Protection of physical assets

Such tests included inquiry of appropriate management, supervisory, and staff personnel; inspection of the Organization's documents and records; and observation of the Organization's activities and operations. The results of these tests were considered in planning the nature, timing, and extent of our tests of the specified control structure policies and procedures related to the control objectives described below.

## CONTROL OBJECTIVES, RELATED POLICIES AND PROCEDURES, AND TESTS OF OPERATING EFFECTIVENESS

### General Computer Controls

#### *Systems Development and Maintenance*

*Control objective 1.* Control structure policies and procedures provide reasonable assurance that changes to existing applications are authorized, tested, approved, properly implemented, and documented.

*Description of policies and procedures.* All program-change requests are submitted in writing to the manager of customer support. The manager of customer support maintains a log of all program-change requests received.

After approval, the director of information systems signs off on the program-change request and forwards it to the manager of application programming.

The manager of application programming receives approved program-change requests and prepares a CWR form. A log of all CWRs is maintained and monitored by the manager of application programming.

The director of information systems must authorize change-control personnel to release production-program source code to the programmer. The programming staff does not have direct access to production-program source code.

The programmer makes changes to the program code using a program-development library. The programmer does not have the ability to compile a changed program into executable form in the production environment. Programming changes are made using an on-line programming utility and changes to source code are generated and annotated with the date of the change. Depending on the change, program unit tests and system tests are completed by the programmer and reviewed by the manager of application programming. Acceptance tests are performed using test files and the resulting output is verified by the requesting party.

All test results are verified by the programmer, the manager of application programming, and the requesting party. At the completion of all testing, the programmer, the manager of application programming, and the requesting party sign off on the CWR.

After all tests are completed, the director of information systems reviews the test results and documentation. If the director is satisfied with the program change, he or she authorizes change-control personnel to compile the new source code in the production environment and sign off on the CWR.

Updates to the production libraries are performed by change-control personnel after authorization by the director of information systems. Each time a program is compiled in the production environment, an entry is electronically recorded in a log that is printed and reviewed daily for any unauthorized activity.

Documentation is updated by the programmer, reviewed by the manager of application programming, and distributed to the appropriate parties.

*Tests of operating effectiveness.*

- Examined documents evidencing the processing of program-change requests to ensure that requests were logged, reviewed by appropriate management personnel, and submitted in writing.
- Examined the log of CWRs and traced a sample of entries in the log to the CWR form and the corresponding program-change request. Inspected each CWR form and program-change request in the sample for completeness and proper approval. For the program changes in the sample that were completed and implemented during the period, inspected the test results for proper documentation and approval. Reviewed the CWR forms for proper authorization of the program change to be compiled in the production environment.
- Selected a sample of program changes implemented during the period from a report generated by the program-change software and inspected the CWR forms and the program-change requests for completeness and proper approval.

- Determined through review of various system reports, security tables, and observation that the programming staff does not have direct access to program source code.
- Examined a sample of the daily logs of compiled programs for reasonableness and evidence of review.

*Results of tests.* No relevant exceptions were noted.

***Note to Readers:*** *The control structure policies and procedures and tests of operating effectiveness for control objectives 2 through 9 are not presented in this sample report.*

*Control objective 2.* Control structure policies and procedures provide reasonable assurance that new applications being developed are authorized, tested, approved, properly implemented, and documented.

*Control objective 3.* Control structure policies and procedures provide reasonable assurance that changes to the existing system software and implementation of new system software are authorized, tested, approved, properly implemented, and documented.

### *Access*

*Control objective 4.* Control structure policies and procedures provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

*Control objective 5.* Control structure policies and procedures provide reasonable assurance that logical access to data files is restricted to properly authorized individuals.

### *Computer Operations*

*Control objective 6.* Control structure policies and procedures provide reasonable assurance that processing is scheduled appropriately and deviations from scheduled processing are identified and resolved.

*Control objective 7.* Control structure policies and procedures provide reasonable assurance that data transmissions between the Organization and its user organizations are complete, accurate, and secure.

### *Savings Application Controls*

*Control objective 8.* Control structure policies and procedures provide reasonable assurance that savings deposit and withdrawal transactions are received from authorized sources.

*Control objective 9.* Control structure policies and procedures provide reasonable assurance that savings deposit and withdrawal transactions

received from the user organizations are initially recorded completely and accurately.

*Control objective 10.* Control structure policies and procedures provide reasonable assurance that programmed interest and penalties are calculated in conformity with the description.

***Note to Readers:*** *The service auditor performs procedures to test the fairness of the presentation of the description of how interest and penalties are calculated and also performs procedures to test the operating effectiveness of the controls that provide reasonable assurance that programmed interest and penalties are calculated in conformity with the description. The nature and objective of the procedures performed to evaluate the fairness of the description of how interest and penalties are calculated are different from those performed to evaluate the operating effectiveness of the controls over the calculation of interest and penalties. The service auditor might recalculate interest and penalties to test the fairness of the description; however, recalculation generally would not provide evidence of the operating effectiveness of the controls over the calculation of interest and penalties. In this example, the service auditor tested the general computer controls to obtain evidence about the operating effectiveness of the controls because the service organization relies on the computer to calculate interest and penalties. The service auditor generally would not indicate that the only test of operating effectiveness performed for this control objective was recalculating interest and penalties.*

*Description of policies and procedures.* Application security restricts update access to user-defined indices for calculating interest and penalties to the appropriate user organization. Within each user organization, passwords are required to update or change the indices. Programs used to calculate interest and penalties are subject to the control structure policies and procedures described for control objective 1, "Control structure policies and procedures provide reasonable assurance that changes to existing applications are authorized, tested, approved, properly implemented, and documented."

*Tests of operating effectiveness.*

- Selected a sample of tables containing user-defined indices for interest and penalty calculations. Examined the application security tables to determine whether access to change entries for the indices was restricted to the appropriate user organizations.
- Observed the process of changing indices (using a test facility), noting that passwords are required.

Changes to the interest and penalty calculation programs were included in the population of program changes tested for control objective 1.

*Results of tests.* No relevant exceptions were noted.

***Note to Readers:*** *The control structure policies and procedures and tests of operating effectiveness for control objectives 11 through 13 are not presented in this sample report.*

*Control objective 11.* Control structure policies and procedures provide reasonable assurance that processing is performed in accordance with user organization specifications.

*Control objective 12.* Control structure policies and procedures provide reasonable assurance that data maintained on files remain authorized, complete, and accurate.

*Control objective 13.* Control structure policies and procedures provide reasonable assurance that output data and documents are complete, accurate, and distributed to authorized recipients on a timely basis.

***Note to Readers:*** *In this sample report, the service auditor did not perform tests of operating effectiveness for every control objective included in the service organization's description of policies and procedures. That is why control objective 14 and the tests of operating effectiveness for control objective 14 are not included in this section of the report.*

# IV

# OTHER INFORMATION PROVIDED BY EXAMPLE COMPUTER SERVICE ORGANIZATION

***Note to Readers:*** *Details of other information provided by Example Computer Service Organization are not presented in this sample report.*

**Example 2**

# EXAMPLE COMPUTER SERVICE ORGANIZATION

## Report on Policies and Procedures Placed in Operation and Tests of Operating Effectiveness

### Table of Contents



* Items marked with an asterisk are presented in the table of contents for illustrative purposes only and are not included in this sample report.

General Computer Controls
Systems Development and Maintenance
Access
Computer Operations
Savings Application Controls
Mortgage Loan Application Controls*
Consumer Loan Application Controls *
Other

**IV. Other Information Provided by Example Computer Service Organization**

Description of Other Applications*
Commercial Loan*
General Ledger*

Description of Planned Changes to Applications*

# I

# INDEPENDENT SERVICE AUDITOR'S REPORT

To the Board of Directors of Example Computer Service Organization:

We have examined the accompanying description of the Savings, Mortgage Loan, and Consumer Loan applications of Example Computer Service Organization. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Example Computer Service Organization's policies and procedures that may be relevant to a user organization's internal control structure; (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if those policies and procedures were complied with satisfactorily, and user organizations applied the internal control structure policies and procedures contemplated in the design of Example Computer Service Organization's policies and procedures; and (3) such policies and procedures had been placed in operation as of June 30, 19XX. The control objectives were specified by the management of Example Computer Service Organization. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned applications presents fairly, in all material respects, the relevant aspects of Example Computer Service Organization's policies and procedures that had been placed in operation as of June 30, 19XX. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily and user organizations applied the internal control structure policies and procedures contemplated in the design of Example Computer Service Organization's policies and procedures.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specified policies and procedures, included in section III of this report, to obtain evidence about their effectiveness in meeting the control objectives, described in section III, during the period from January 1, 19XX to June 30, 19XX. The specified policies and procedures and the nature, timing, extent, and results of the tests are listed in section III. This information has been provided to user organizations of Example Computer Service Organization and to their auditors to be taken into consideration, along with information about the internal control structures at user organizations, when making assessments of control risk for user organizations. In our opinion, the

policies and procedures that were tested, as described in section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in section III were achieved during the period from January 1, 19XX to June 30, 19XX.

The relative effectiveness and significance of specific policies and procedures at Example Computer Service Organization and their effect on assessments of control risk at user organizations are dependent on their interaction with the policies, procedures, and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of policies and procedures at individual user organizations.

The description of policies and procedures at Example Computer Service Organization is as of June 30, 19XX, and information about tests of the operating effectiveness of specified policies and procedures covers the period from January 1, 19XX to June 30, 19XX. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specified policies and procedures at the Service Organization is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

The information included in section IV of this report is presented by Example Computer Service Organization to provide additional information to user organizations and is not a part of Example Computer Service Organization's description of policies and procedures placed in operation. The information in section IV has not been subjected to the procedures applied in the examination of the description of the Savings, Mortgage Loan, and Consumer Loan applications, and, accordingly, we express no opinion on it.

This report is intended solely for use by the management of Example Computer Service Organization, its users, and the independent auditors of its users.

July 10, 19XX

# II

# EXAMPLE COMPUTER SERVICE ORGANIZATION'S DESCRIPTION OF POLICIES AND PROCEDURES

## OVERVIEW OF OPERATIONS

Example Computer Service Organization (the Organization) is located in Los Angeles, California and provides computer services primarily to user organizations in the financial services industry. Applications enable user organizations to process savings, mortgage loan, consumer loan, commercial loan, and general ledger transactions. This description only addresses the control structure policies and procedures related to the Savings, Mortgage Loan, and Consumer Loan applications. Section IV of this report contains certain information about the Commercial Loan and General Ledger applications.

Numerous terminals located at user organizations are connected to the Organization through leased lines that provide on-line, real-time activity for the applications. The Organization processes transactions using one ABC central processor under the control of Operating System Release 2.1 . . . .

## CONTROL ENVIRONMENT ELEMENTS

Operations are under the direction of the president and the board of directors of the Organization. The board of directors has established an audit committee that oversees the internal audit function. The Organization employs a staff of approximately 35 people and is supported by the functional areas listed below.

- *Administration/systems development.* Coordinates all aspects of the service organization's operations including service billing. Identifies areas requiring internal controls and implements those controls. Performs systems planning, development, and implementation. Reviews network operations and telecommunications and performs disaster-recovery planning and database administration.
- *Customer support.* Supports end users in all aspects of their use of the application system including research and resolution of identified problems. Administers application security (including passwords), changes to application parameters, and distribution of user documentation.
- *Application programming.* Performs regular maintenance programming, programming for user-requested enhancements, and updates the systems documentation.
- *Terminal support.* Performs end-user terminal training. Researches and resolves terminal and network problems and performs timely installations of enhancements to terminal and network software.

- *Operations.* Manages daily computer operations, nightly production processing, report production and distribution, and system utilization and capacities.
- *Marketing.* Provides analysis for new business prospects and new product planning.

The managers of each of the functional areas report to the director of information systems.

The Organization's employees are not authorized to initiate or authorize transactions, to change or modify user files except through normal production procedures, or to correct user errors. All shifts at the Organization are managed by shift supervisors and the director of information systems. Incident reports, processing logs, job schedules, and equipment activity reports are monitored by the director of information systems. These reports track daily processing activities and identify hardware and software problems and system usage.

Weekly management meetings are held to discuss special processing requests, operational performance, and the development and maintenance of projects in process.

Written position descriptions for employees are maintained by the director of information systems and the personnel department. The descriptions are reviewed annually and revised as necessary.

References are sought and background, credit, and security checks are conducted for all Organization personnel hired. The confidentiality of user-organization information is stressed during the new-employee orientation program and is emphasized in the personnel manual issued to each employee. The Organization provides a mandatory orientation program to all full-time employees and encourages employees to attend other formal outside training. An internal supervisory training program was recently initiated.

Employees are required to take vacation in accordance with the Organization's policy, which requires that all employees who are eligible for two or more weeks of vacation take off five consecutive business days during each calendar year. No employee may take vacation during the last week or the first ten days of each quarter. Vacation must be taken in the calendar year in which it is earned.

The Organization's policy requires that after three months of employment, new employees receive a written performance evaluation from their supervisors, and that all employees receive an annual written performance evaluation and salary review. These reviews are based on employee-stated goals and objectives that are prepared and reviewed with each employee's supervisor. Completed appraisals are reviewed by senior management and become a permanent part of the employee's personnel file.

The internal auditors provide the audit committee with an appraisal of internal controls. The internal auditors execute an information-technology internal audit program, and follow up on any operational exceptions or concerns that may arise. The internal auditors use audit software to perform various recalculations and analyses using actual production data in an off-line mode.

## APPLICATION PROCESSING

### Overview of the Flow of Transactions

The Organization's Savings, Mortgage Loan, and Consumer Loan applications are part of an integrated software system. This system provides on-line, real-time processing of monetary and nonmonetary transactions and provides batch and memo postprocessing capabilities. Processing activities are divided into on-line and off-line processing segments. During normal business hours, user organizations may make inquiries and enter monetary and nonmonetary transactions through various terminals, including teller terminals. Additional input is provided from automatic teller machine (ATM) transactions, transactions from the Federal Reserve Bank, and other transactions received from user banks. Such transactions are received via electronic data transmission or via tape delivered by courier.

Each application uses the standard operating system and related systems software to interact with terminals, to accept data, to apply prescribed processes to data, to maintain an audit trail, and to respond to inquiries.

On-line daily processing occurs during preestablished hours when customer banks are open. Monetary, nonmonetary, and inquiry transactions are entered at teller terminals located at branch offices of user organizations serviced by the Organization. Nonmonetary and inquiry transactions are entered at other terminals designated as administrative terminals in branch offices and other offices of user organizations. Terminals are linked to the on-line data communication network through leased telephone lines. Telecommunication software polls the terminals in the network for available input transactions . . . .

Off-line daily processing is performed in accordance with daily schedules and generally occurs when the on-line system is not running. These programs determine whether control totals agree with the totals of related detail accounts, modify database fields, and produce daily and special-request reports.

Following is a description of the Savings, Mortgage Loan, and Consumer Loan applications.

### Savings Application

The Savings application maintains account balances based on deposits, withdrawals, earnings postings, journal debits and credits, and other transactions. The application provides for on-line data entry and inquiry functions and on-line, real-time posting of monetary and nonmonetary transactions entered through teller terminals . . . .

***Note to Readers:*** *The remainder of the description of the Savings application and the descriptions of the Mortgage Loan and Consumer Loan applications are not presented in this sample report.*

## CONTROL OBJECTIVES AND RELATED POLICIES AND PROCEDURES

The Organization's control objectives and related policies and procedures are included in section III of this report, "Information Provided by the Service Auditor," to eliminate the redundancy that would result from listing them here in section II and repeating them in section III. Although the control objectives and related policies and procedures are included in section III, they are, nevertheless, an integral part of the Organization's description of policies and procedures.

***Note to Readers:*** *The paragraph above has been included to clearly indicate to readers that the control objectives and related policies and procedures are an integral part of the Organization's description even though they have been included in the service auditor's section to reduce redundancy in the report.*

## USER CONTROL CONSIDERATIONS

The Organization's applications were designed with the assumption that certain internal control structure policies and procedures would be implemented by user organizations. In certain situations, the application of specified internal control structure policies and procedures at user organizations is necessary to achieve certain control objectives included in this report. In such instances, the required user-organization internal control structure policies and procedures are indicated under the related control objective in section III of this report.

This section describes other internal control structure policies and procedures that should be in operation at user organizations to complement the control structure policies and procedures at the Organization. User auditors should consider whether the following policies and procedures have been placed in operation at user organizations:

- Policies and procedures to ensure that changes to processing options (parameters) are appropriately authorized, implemented, and approved
- Policies and procedures to ensure that transactions are appropriately authorized, complete, and accurate
- Policies and procedures to ensure that erroneous input data are corrected and resubmitted
- Policies and procedures to ensure that output reports are reviewed by appropriate users for completeness and accuracy
- Policies and procedures to ensure that output received from the Organization is routinely reconciled to relevant control totals

The list of user-organization control considerations presented above is not a comprehensive list of all internal control structure policies and procedures that should be employed by user organizations. Other internal control structure policies and procedures may be required at user organizations.

# III

# INFORMATION PROVIDED BY THE SERVICE AUDITOR

## TESTS OF CONTROL ENVIRONMENT ELEMENTS

In addition to the tests of operating effectiveness of specified control structure policies and procedures described in this section, our procedures included consideration and tests of the following relevant elements of the Organization's control environment:

- Organizational structure
- Personnel policies and practices
- Management's control methods for monitoring and following up on performance, including internal audit
- Protection of physical assets

Such tests included inquiry of appropriate management, supervisory, and staff personnel; inspection of the Organization's documents and records; and observation of the Organization's activities and operations. The results of these tests were considered in planning the nature, timing, and extent of our tests of the specified control structure policies and procedures related to the control objectives described below.

## CONTROL OBJECTIVES, RELATED POLICIES AND PROCEDURES, AND TESTS OF OPERATING EFFECTIVENESS

### General Computer Controls

#### *Systems Development and Maintenance*

*Control objective 1.* Control structure policies and procedures provide reasonable assurance that changes to existing applications are authorized, tested, approved, properly implemented, and documented.

*Description of policies and procedures.* Each user organization designates the individuals who are authorized to request program changes. All program-change requests are submitted in writing to the manager of customer support. The manager of customer support maintains a log of all program-change requests received.

After a program-change request has been received and logged, it is reviewed by personnel in the customer support department to determine whether the requested change is an enhancement of a program or the correction of a programming error and to develop an estimate of the number of hours that will be required to make and implement the program change.

Biweekly management meetings are held with the director of information systems, the manager of application programming, and representatives of the user organizations to consider program-change requests and the status of active projects. Based on these discussions, the director of information systems approves or disapproves the change request. Upon approval, the director of information systems signs off on the program-change request and forwards it to the manager of application programming.

The manager of application programming receives approved program-change requests and prepares a customer work request (CWR) form. Information listed on the form includes the name of the originator, the bank name, the bank's user code, the program affected, and a description of the requested program change. A log of all CWRs is maintained and monitored by the manager of application programming.

The director of information systems must authorize change control personnel to release production-program source code to the programmer. The programming staff does not have direct access to production-program source code. The programmer makes changes to program code using a program-development library. The programmer does not have the ability to compile a changed program into executable form in the production environment. Programming changes are made using an on-line programming utility and changes to source code are generated and annotated with the date of change. Depending on the change, program unit tests and system tests are completed by the programmer and reviewed by the manager of application programming.

Acceptance tests are performed using test files and the resulting output is verified by the requesting party. Recently processed production data is used as the test data, without updating any live files. If the program change involves a new function, test data is developed jointly by the programmer and the requesting party. All test results are verified by the programmer, the manager of application programming, and the requesting party. At the completion of all testing, the programmer, the manager of application programming, and the requesting party sign off on the CWR.

After acceptance tests are completed, the director of information systems reviews all test results and documentation. If the director is satisfied with the program change, he or she authorizes change-control personnel to compile the new source code in the production environment and sign off on the CWR.

Updates to the production libraries are performed by change-control personnel after authorization by the director of information systems. Each time a program is compiled in the production environment, an entry is electronically recorded in a log that is printed and reviewed daily for any unauthorized activity.

Documentation is updated by the programmer, reviewed by the manager of application programming, and distributed to the appropriate parties.

*Tests of operating effectiveness.*

- Examined documents evidencing the processing of program-change requests to ensure that requests were logged, reviewed by appropriate management personnel, and submitted in writing.

- Examined the log of CWRs and traced a sample of entries in the log to the CWR form and the corresponding program-change request. Inspected each CWR form and program-change request in the sample for completeness and proper approval. For the program changes in the sample that were completed and implemented during the period, inspected the test results for proper documentation and approval. Reviewed the CWR forms for proper authorization of the program change to be compiled in the production environment.
- Selected a sample of program changes implemented during the period from a report generated by the program-change software and inspected the CWR form and program-change request for completeness and proper approval.
- Determined through review of various system reports, security tables, and observation that the programming staff does not have direct access to program-source code.
- Examined a sample of the daily logs of compiled programs for reasonableness and evidence of review.

*Results of tests.* No relevant exceptions were noted.

***Note to Readers:*** *The control structure policies and procedures and tests of operating effectiveness for control objectives 2 through 9 are not presented in this sample report.*

*Control objective 2.* Control structure policies and procedures provide reasonable assurance that new applications being developed are authorized, tested, approved, properly implemented, and documented.

*Control objective 3.* Control structure policies and procedures provide reasonable assurance that changes to the existing system software and implementation of new system software are authorized, tested, approved, properly implemented, and documented.

### *Access*

*Control objective 4.* Control structure policies and procedures provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

*Control objective 5.* Control structure policies and procedures provide reasonable assurance that logical access to data files is restricted to properly authorized individuals.

### *Computer Operations*

*Control objective 6.* Control structure policies and procedures provide reasonable assurance that processing is appropriately scheduled and deviations from scheduled processing are identified and resolved.

*Control objective 7.* Control structure policies and procedures provide reasonable assurance that data transmissions between Example Computer Service Organization and its user organizations are complete, accurate, and secure.

## Savings Application Controls

*Control objective 8.* Control structure policies and procedures provide reasonable assurance that savings deposit and withdrawal transactions are received from authorized sources.

*Control objective 9.* Control structure policies and procedures provide reasonable assurance that savings deposit and withdrawal transactions received from the user organizations are initially recorded completely and accurately.

*Control objective 10.* Control structure policies and procedures provide reasonable assurance that programmed interest and penalties are calculated in conformity with the description.

***Note to Readers:*** *Control objective 10 illustrates a situation in which the application of a specific user-organization internal control structure policy or procedure is required to achieve the control objective. See "User Control Considerations" below and paragraph 46 of SAS No. 70.*

*Description of policies and procedures.* Application security restricts update access to user-defined indices used to calculate interest and penalties to the appropriate user organization. Within each user organization, passwords are required to update or change the indices.

Programs used to calculate interest and penalties are subject to the control structure policies and procedures described for control objective 1, "Control structure policies and procedures provide reasonable assurance that changes to existing applications are authorized, tested, approved, properly implemented, and documented."

*User control considerations.* User organizations are responsible for establishing controls at the user organizations to restrict access to and change of user-defined indices to authorized user-organization personnel. Any index can be selected and changed on-line at any time by user organizations with an appropriate password. The balances applicable to each rate are established by the user organizations in account-type parameters. A report can be produced that shows the current content of the indices and the date they were last changed.

*Tests of Operating Effectiveness.*

- Selected a sample of tables containing user-defined indices for interest and penalty calculations. Examined the application security tables to determine whether access to change entries for the indices was restricted to the appropriate user organizations.

- Observed the process of changing indices (using a test facility), noting that passwords are required.

Changes to the interest and penalty calculation programs were included in the population of program changes tested for control objective 1.

*Results of tests.* No exceptions were noted.

***Note to Readers:*** *The service auditor performs procedures to test the fairness of the presentation of the description of how interest and penalties are calculated and also performs procedures to test the operating effectiveness of the controls that provide reasonable assurance that programmed interest and penalties are calculated in conformity with the description. The nature and objective of the procedures performed to evaluate the fairness of the description of how interest and penalties are calculated are different from those performed to evaluate the operating effectiveness of the controls over the calculation of interest and penalties. The service auditor might recalculate interest and penalties to test the fairness of the description; however, recalculation generally would not provide evidence of the operating effectiveness of the controls over the calculation of interest and penalties. In this example, the service auditor tested the general computer controls to obtain evidence about the operating effectiveness of the controls because the service organization relies on the computer to calculate interest and penalties. The service auditor generally would not indicate that the only test of operating effectiveness performed for this control objective was recalculating interest and penalties.*

***Note to Readers:*** *The control structure policies and procedures related to control objectives 11 through 14 are not presented in this sample report.*

*Control objective 11.* Control structure policies and procedures provide reasonable assurance that processing is performed in accordance with user specifications.

*Control objective 12.* Control structure policies and procedures provide reasonable assurance that data maintained on files remain authorized, complete, and accurate.

*Control objective 13.* Control structure policies and procedures provide reasonable assurance that output data and documents are complete and accurate and distributed to authorized recipients on a timely basis.

## Other

*Control objective 14.* Control structure policies and procedures provide reasonable assurance that the service organization can provide continuity of operations.

# IV

# OTHER INFORMATION PROVIDED BY EXAMPLE COMPUTER SERVICE ORGANIZATION

***Note to Readers:*** *Details of other information provided by Example Computer Service Organization are not included in this sample report.*

**Example 3**

# EXAMPLE TRUST ORGANIZATION

## Report on Policies and Procedures Placed in Operation and Tests of Operating Effectiveness of the Institutional Trust Division

### Table of Contents



* Items marked with an asterisk are presented in the table of contents for illustrative purposes only and are not included in this sample report.

* Items marked with an asterisk are presented in the table of contents for illustrative purposes only and are not included in this sample report.

# I

# INDEPENDENT SERVICE AUDITOR'S REPORT

To the Board of Directors of Example Trust Organization:

We have examined the accompanying description of the policies and procedures of Example Trust Organization applicable to the processing of transactions for users of the institutional trust division. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Example Trust Organization's policies and procedures that may be relevant to the internal control structures of users of the institutional trust division; (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if those policies and procedures were complied with satisfactorily, and users of the institutional trust division applied the internal control structure policies and procedures contemplated in the design of Example Trust Organization's policies and procedures, as described in section II; and (3) such policies and procedures had been placed in operation as of December 31, 19XX. Example Trust Organization uses various service organizations to obtain information related to the pricing of securities and to perform various functions related to the custody of securities. The accompanying description includes only those policies and procedures and related control objectives at Example Trust Organization, and does not include policies and procedures and related control objectives at these other service organizations. Our examination did not extend to policies and procedures at pricing and custodial service organizations. The control objectives were specified by the management of Example Trust Organization. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the policies and procedures of Example Trust Organization presents fairly, in all material respects, those aspects of Example Trust Organization's policies and procedures that may be relevant to users of the institutional trust division and that had been placed in operation as of December 31, 19XX. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily and users of the institutional trust division applied the internal control structure policies contemplated in the design of Example Trust Organization's policies and procedures, as described in section II.

In addition to the procedures we considered necessary to render our opinion, as expressed in the previous paragraph, we applied tests to specified policies and procedures to obtain evidence about their effectiveness in meeting the related control objectives during the period from January 1, 19XX to December 31, 19XX. The specific policies and procedures and the nature, timing, extent, and results of the tests are summarized in sections II and III. This information has been provided to users of the institutional trust division of Example Trust Organization and to their auditors to be taken into consideration, along with information about the internal control structures at user organizations, when making assessments of control risk for user organizations. In our opinion, the policies and procedures that were tested, as described in sections II and III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from January 1, 19XX to December 31, 19XX. The relative effectiveness and significance of specific policies and procedures at Example Trust Organization, and their effect on assessments of control risk at users of the institutional trust division, are dependent on their interaction with the policies, procedures, and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of policies and procedures at individual users of the institutional trust division.

The description of policies and procedures at Example Trust Organization is as of December 31, 19XX, and information about tests of the operating effectiveness of specified policies and procedures covers the period from January 1, 19XX to December 31, 19XX. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specified policies and procedures at Example Trust Organization is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

The information included in section IV of this report is presented by Example Trust Organization to provide additional information to user organizations and is not a part of Example Trust Organization's description of policies and procedures placed in operation. The information in section IV has not been subjected to the procedures applied in the examination of Example Trust Organization's description of policies and procedures applicable to the processing of transactions for users of the institutional trust division, and accordingly, we express no opinion on it.

This report is intended solely for use by the management of Example Trust Organization, users of its institutional trust division, and the independent auditors of its users.

January 15, 19XX

# II

# EXAMPLE TRUST ORGANIZATION'S DESCRIPTION OF POLICIES AND PROCEDURES

## OVERVIEW OF SERVICES PROVIDED

Example Trust Organization (the Organization) is a full-service trust organization providing fiduciary services to corporate, personal, and institutional trust users. The Organization provides services through the following five divisions:

- *Corporate trust division.* Serves as a trustee for securities issued by corporations . . . .
- *Personal trust division.* Services trusts established by individuals, foundations . . . .
- *Institutional trust division.* Services institutional users, including employee benefit plans, public funds, insurance companies, and other financial institutions. The institutional trust division has ultimate responsibility for the administration of institutional trust accounts (Accounts), including liaising with plan sponsors and investment managers. Account administration includes customer accounting and reporting, securities lending administration, participant loan administration, performance measurement, and compliance with the Employee Retirement Income Security Act (ERISA) of 1974. Each Account has a designated administrator in the institutional trust division. The administrator is supported by the investment management division for accounts for which the Organization has investment discretion. The institutional trust division is organized along regional lines, with a senior executive responsible for oversight of each region's activities. The senior executives report to the executive vice president of the institutional trust division, who reports to the president of the Organization.
- *Investment management division.* Provides investment advisory services to accounts of the corporate trust, personal trust, and investment trust divisions for which the Organization is granted investment discretion.
- *Trust support division.* Serves as a central utility for the processing of transactions for users of the corporate trust, personal trust, and institutional trust divisions. The trust support division is organized along functional lines and includes the following groups:
  - *Computerized information systems group (CISG).* Provides data-processing services to the five divisions of the Organization. The CISG operates from a centralized processing site that provides numerous application-processing services to its users. The CISG's size and organization provide for separation of incompatible duties relating to computer operations, systems and program-

ming, system software support, and data control. CISG personnel are subject to the Organization's personnel policies and procedures described on pages 109–110.
- *Securities processing group.* Is responsible for securities movement and control, asset custody and control, securities lending, income accrual and collection, and corporate actions.
- *Divisional support group.* Is responsible for liaising with the institutional trust division and the other divisions.
- *Benefit payment, disbursement, and participant record keeping group.*

## CONTROL ENVIRONMENT ELEMENTS

### Organization

Set forth in Figure 1 is the organization chart for Example Trust Organization at December 31, 19XX.

The Organization's trust activities are overseen by the trust committee of the board of directors. The trust committee has established the following committees to oversee the Organization's fiduciary activities relating to Accounts: trust policy committee, investment committee, administrative and investment review committee, and trust real estate investment committee. Each committee is charged with monitoring and establishing policy for the fiduciary activities under its oversight.

This report addresses the institutional trust division, which directly services Accounts. It also addresses the investment management and trust support divisions to the extent that these divisions support the activities of the institutional trust division. Activities of the corporate trust and personal trust divisions are beyond the scope of this report.

Trust activities are conducted in accordance with written policy and procedure guides that have been adopted by the trust policy committee. Policy and procedure guides are periodically updated. The responsibilities of the institutional trust and trust support divisions are allocated among personnel so as to segregate the following functions:

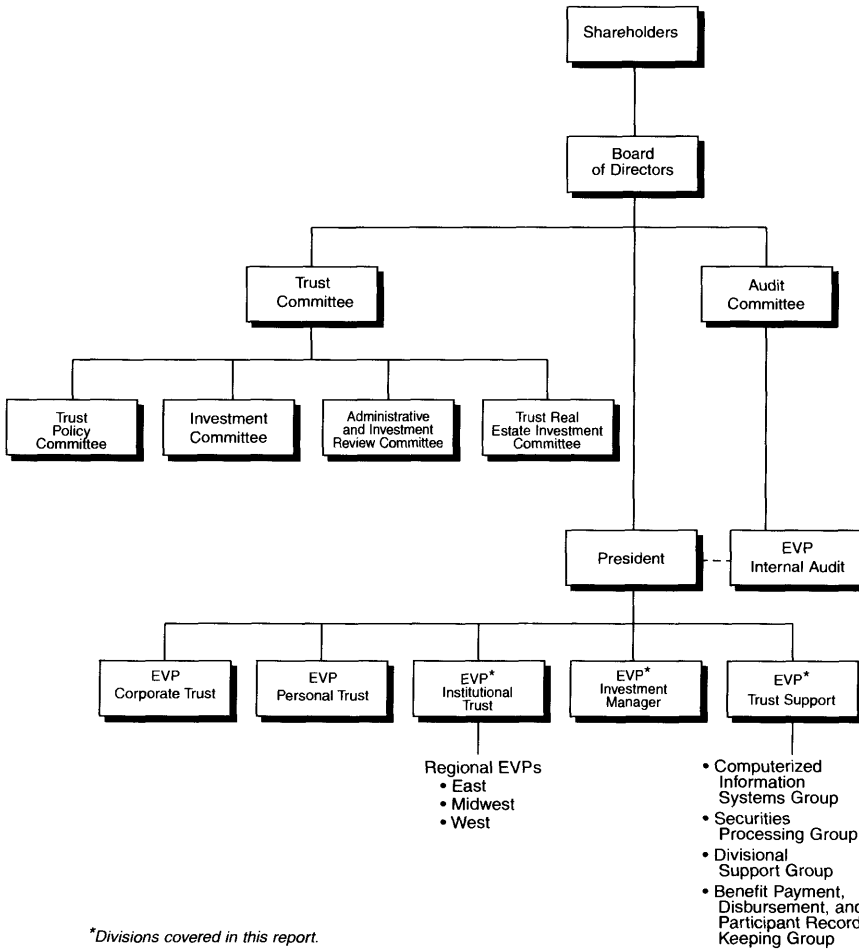
- Processing and recording transactions
- Maintaining custody of assets
- Reconciliation activities
- Compliance monitoring

### Management Control

The Organization has a formal management information and reporting system that enables management to monitor key control and performance measurements.

Adherence to trust policies and procedures is monitored through a self-assessment program that is overseen by the compliance unit of the institutional trust division. The assessment program has been designed to peri-

*Figure 1*
**Organization Chart for Example Trust Organization**




odically evaluate Account administration and support operations for compliance with the institutional trust division's authorizing document, the Organization's policies and procedures, and the applicable regulatory requirements. Results of the assessments are communicated to management and to the trust committee.

## Personnel Policies and Procedures

The Organization has formal hiring practices designed to ensure that new employees are qualified for their job responsibilities. Each new-position

hiring must be jointly approved by the human resources department and the manager of the department requiring the employee. Hiring policies include requiring that employees have minimum education and experience requirements, that written references be submitted, and that employees execute confidentiality statements. The Organization also performs background and credit investigations of potential employees.

Training of personnel is accomplished through supervised on-the-job training, outside seminars, and in-house courses. Certain positions require the completion of special training. For example, Account administrators are trained in ERISA rules and regulations. Department managers are responsible for ensuring that all Account administrators complete such training. Department managers are also responsible for encouraging the training and development of employees so that all personnel continue to qualify for their functional responsibilities.

Formal performance reviews are conducted on a periodic basis. Employees are evaluated on objective criteria based on performance. An overall rating (unsatisfactory, less than satisfactory, exceptional) is assigned. Employees rated less than satisfactory are placed on probation, and frequent reevaluations are performed. After being on probation for a specified period, the employee is terminated if no improvement has been made. The evaluations of employees rated unsatisfactory are reviewed to determine the validity of the rating as a measure of sustained performance. If the rating is substantiated, the employee is immediately terminated.

The Organization requires that each employee (including officers) take off at least ten consecutive workdays during each calendar year.

## Other Considerations

The Organization's control structure policies and procedures are documented in its corporate compliance manual (CCM). The CCM is organized by product and business unit and sets forth the Organization's control structure policies and procedures, the laws and regulations to which the product or business unit is subject, and the compliance responsibilities of specific positions within the Organization.

The Organization has a formal conflict-of-interest policy that, among other things, establishes rules of conduct for employees who service Accounts. Employees and their immediate families are prohibited from divulging confidential information about client affairs, trading in securities of clients or their affiliates, and taking any action that is not in the best interest of clients. In addition, investment advisors in the investment management division must provide periodic brokerage statements to a compliance officer who reviews the statements for transactions proscribed by Organization policy. Annually, each officer must confirm in writing his or her compliance with the Organization's conflict-of-interest policy.

The Organization is subject to regulation and supervision by the Office of the Comptroller of the Currency (OCC). Accordingly, the Organization is required to file periodic reports with the OCC and is subject to periodic examination by the OCC.

The Organization maintains insurance coverage against major risks. Insurance policies include an errors and omissions bond, employee fidelity bond, blanket-lost-original instruments bond, bankers' blanket bond, and trust-property-managers bond. Coverage is maintained at levels that the Organization considers reasonable given the size and scope of its operations, and is provided by insurance companies that management of the Organization believes are financially sound.

## Internal Audit

Trust activities are monitored by the internal audit group which reports to the audit committee of the board of directors. The internal audit program is designed to evaluate compliance with the Organization's policies and procedures and the laws and regulations to which the Organization is subject, including ERISA. The program also addresses the soundness and adequacy of accounting, operating, and administrative controls. Internal audits cover four broad areas of fiduciary services: account administration, regulatory compliance, transaction accounting, and asset custody. Internal audits of asset custody include periodic verification of assets held in trust through physical examination, confirmation, or review of reconciliations and underlying source documents. Formal reports of audit findings are prepared and submitted to management and to the audit committee.

## Description of Computerized Information Systems[1]

- *Processing environment.* The CISG operates a large scale computer facility that has two mainframe computers. One computer is primarily used to support application processing and the other is primarily used to support application maintenance, development and testing, and systems software maintenance and testing. The computers are supported by the manufacturer's operating system and related components . . . .
- *Security/access.* The CISG has a centralized security administration department. This department is responsible for ensuring that the Organization adheres to corporate security policy that . . . . Access to system resources and production data and program files are protected from unauthorized access by a global-access control system that . . . .
- *Application development/maintenance.* All requests for the development of new systems and changes to existing systems are submitted to the director of the CISG. All requests are processed within a software management system that includes the following processes: project request, . . . .

1. In an actual report, there would be a more comprehensive description of the computer applications and the general computer controls. Such information is not included in this sample report.

## TRANSACTION PROCESSING

### Basic Trust and Custody Services

Most of the transaction processing for Accounts is automated. Policies and procedures over access and changes to the automated systems are described in the section entitled "Description of Computerized Information Systems." Set forth in Figure 2 is an overview of the Organization's applications, interfaces, and relationships to investment advisors, brokers, depositories, and custodians.

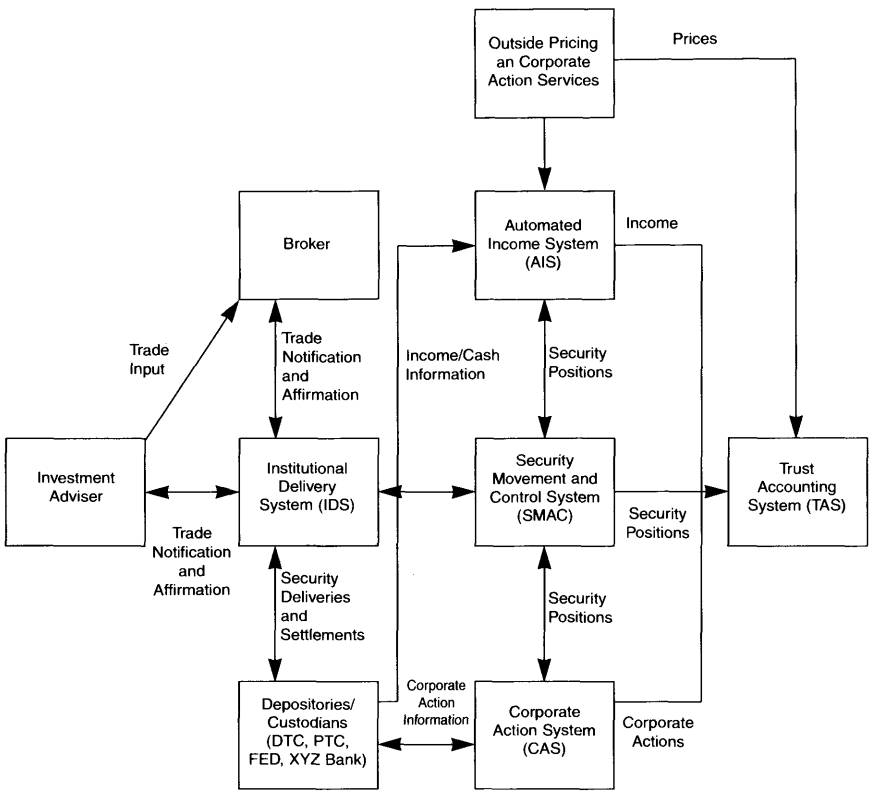
The application systems were developed by the Organization and are operated on the Organization's mainframe computer at its data center in New York City. The functions of each system are briefly described below.

- *Institutional delivery system (IDS).* Accepts automated trade inputs from terminals at outside investment advisers and advisers in the investment management division. Compares the trade inputs with broker trade notifications and interfaces with depositories or other custodians for trade delivery and settlement information, income collection, corporate actions, and security positions. Interfaces with the Organization's wire transfer system for payments and receipts related to security purchase and sale transactions, income receipts, and other cash transactions.
- *Security movement and control system (SMAC).* Maintains inventory records of the Organization's position in individual securities (including the physical location of such securities or the depository/custodian at which they are maintained) and the allocation of such positions to individual clients of the Organization, including, but not limited to, Accounts.
- *Automated income system (AIS).* Receives transmissions of dividend declarations from outside pricing and corporate action services. Computes interest accruals on fixed income securities. Tracks and processes the receipt of income. Allocates income to individual clients of the Organization, including, but not limited to, Accounts.
- *Corporate action system (CAS).* Receives transmissions of corporate actions, such as stock splits, reorganizations, and mergers. Supports the process of notification of security holders of actions and decision follow-ups (in the case of nonmandatory actions, such as tender offers).
- *Trust accounting system (TAS).* Obtains the prices of security holdings from outside sources. Performs analytical testing of the reasonableness of prices. Maintains records for accounts and generates accounting statements.

### Trade Execution

Security trades are initiated by the investment management division or by third-party advisors having investment discretion over particular Accounts. Trade information is input into the IDS via a terminal at the investment

***Figure 2***
**Transaction Processing of Accounts of Example Trust Organization**




advisor. Nonautomated-trade-execution instructions (received via facsimile transmission (fax) or telephone) are authenticated by signature verification or call-back procedure and are input into the IDS by authorized personnel in the securities processing group. Trade information is confirmed in writing by the Organization with the broker/dealer who placed the trade.

Executed trades are affirmed through an automated process that compares the IDS trade information to trade depository information that the depository receives from the trade counterpart. The IDS provides for automated securities settlement on the prearranged date, which is typically five days after the trade date or one day after the trade date for same day/next day settlements. Exceptions to the affirmation process are individually researched and resolved. Depositories include the Depository Trust Company (DTC), the Participants Trust Company (PTC), the Federal Reserve Bank (FED), and XYZ

Bank. Trade positions for settlement with outside depositories are reconciled daily and a net settlement is made with each depository.

Deliveries of securities (via depositories or via physical delivery of securities in the Organization's vault) in connection with security-sale transactions are only effected upon the receipt of cash. Similarly, cash is paid for security-purchase transactions only upon receipt of the securities. If the securities are not received or delivered on the settlement date, the settlement "fails." In that case, the purchase or sale of the security is reflected in the customer's portfolio, and a payable or receivable, respectively, is recorded for the future cash payment or receipt. The Organization monitors fails through the IDS and the SMAC to ensure that they are resolved on a timely basis.

Free deliveries of securities are sometimes required for securities pledged as collateral or for reregistration. Free deliveries of collateral are initiated by the investment manager through ordinary trade input. Free deliveries for reregistration are typically physical (that is, not via a depository).

The security movement and control department of the trust support division is responsible for the receipt and delivery of physical securities (other than purchase/sale transactions), the processing of maintenance entries, securities reregistration, and the transfer of securities between Accounts, as instructed by the account administrator. Securities are received via certified or registered mail. Hand-delivered securities are received under dual control. Securities being processed are maintained in a fireproof file that is secured in a vault during nonbusiness hours. Securities that must be delivered to external custodians are sent by insured courier. Receipt of the security is confirmed directly with the custodian. A log is maintained of all securities sent to a transfer agent for change of the nominee name. Follow-up is required if the security is not returned in 30 days. Mail-loss affidavits are prepared if the security is lost in transit to or from the transfer agent.

## Asset Custody and Control

The Organization maintains trust assets at three depositories, one custodian bank, and in the Organization's vault in New York City. The external depositories or custodian used and the approximate related percentage of total assets maintained on behalf of the Organization's trust customers are the DTC (60 percent), the PTC (20 percent), the FED (10 percent), and XYZ Bank (5 percent). Custodial relationships are reviewed on a periodic basis to ensure that the quality and extent of services is adequate for the Organization's needs.

Assets are recorded on the SMAC by location code. Asset-holding lists can be provided on an asset, account, or location code level. Asset-holding lists are used by the Organization to prepare custodian reconciliations and to resolve any out-of-balance positions. Assets are recorded on the SMAC and identified with individual Accounts. Physical holdings of securities or book-entry holdings at depositories are held in aggregate under the Example Trust Organization's name as trustee or nominee. Asset-holding lists provide detailed information by Account to permit the reconciliation of aggregate positions by security to the individual Account positions.

Reconciliations of asset positions between the DTC, the PTC, and the FED and the Organization's SMAC are performed on a daily basis. Reconciliations of asset positions between XYZ Bank and the Organization's SMAC are performed on a monthly basis. The reconciliations are produced by comparing the custodian's position, per custodian-provided computer tapes, to the SMAC's asset-position listing. An aged exception report is produced that is used for follow-up. Reconciling items aged over 30 days are reported to senior management.

The trust vaults, which contain 5 percent of the trust assets, are maintained under dual control at all times. Securities placed into or removed from the vaults are recorded in vault logs. Any security removed from the vaults must be returned to the main vault or placed in a night vault at the end of each business day. Quarterly vault counts are performed by internal auditors on a surprise basis.

## Income Accrual, Collections, and Corporate Actions

The income accrual and collection department of the securities processing group is responsible for processing and recording income accruals, collecting dividends and interest due on the payable date, processing income received, investigating underpayments and overpayments, and processing due bills and claims for income. Interest income is recorded to Accounts on an accrual basis. Discounts are accreted and premiums are amortized using the interest method. Dividend income is recorded to Accounts on the ex-dividend date, as directed by the corporate actions department of the securities processing group.

Income collections, accruals, and cash dividends are processed using the AIS. Other corporate actions, such as tender offers and stock splits, are processed using the CAS. Both the AIS and the CAS are fed data regarding corporate actions by independent sources. Information about trust-asset holdings of the Organization is obtained by the AIS and the CAS through an automated interface with the SMAC. The AIS reads the security-holdings files of the SMAC daily to identify securities for which dividends have been declared and to ensure that AIS files of fixed-income securities are complete and accurate. The AIS then prepares, by user, a file of expected-income collections or an "income map." These maps are matched against the paying agent's records prior to the expected payment date to research and correct any discrepancies before the payment date. For securities held at depositories, information on expected payments is received from the depositories and from an automated interface with the AIS. For securities held in the vault, a printout of the income map is generated by the AIS and manually compared to the paying agent's advice. Similarly, income collections are subsequently reconciled to the income maps in the AIS. Differences between actual and expected receipts are identified by the AIS and an exception report is generated and used for investigation. Once differences are resolved, the income maps are adjusted, if necessary, and then released to the TAS. This release causes the collection to be reflected in each user's account.

On a daily basis, the AIS provides information on income accruals to the SMAC so that the customer accounting records can be updated automatically.

On a daily basis, the CAS prepares a list of new and pending corporate actions. For mandatory actions, such as bond calls or stock splits, CAS updates the SMAC, the TAS, and the AIS to ensure that subsequent security pricings, income payments, and so on, are accurate. Nonmandatory actions, such as tender offers, are assigned to a client-service representative by the area supervisor. The client-service representative contacts the customer or investment manager to obtain instructions. The outstanding action is maintained on a "tickler file" within the CAS. As the deadline for the action approaches, the customer or investment manager is contacted at specified and increasingly shorter intervals. If no instructions are received by the day before the action is due, the matter is referred to the account administrator for resolution.

### Client Accounting

Periodic accounting statements are prepared for each Account by the TAS.

The TAS receives information on income and corporate actions affecting Accounts from interfaces with the SMAC, the AIS, and the CAS. Holdings of exchange-traded securities are recorded at market value in the accounting statements based on prices transmitted from independent pricing services. If prices are received from more than one pricing service, the prices are compared and any significant deviations are investigated. Nonexchange-traded securities or other types of investments are valued. . . .

## CONTROL OBJECTIVES, RELATED POLICIES AND PROCEDURES, AND TESTS OF OPERATING EFFECTIVENESS

This section presents the following information provided by the Organization:

- The control objectives specified by the management of the Organization
- The policies and procedures established and specified by the Organization to achieve the specified control objectives

Also included in this section is the following information provided by the service auditor:

- A description of the testing performed by the service auditor to determine whether the Organization's control structure policies and procedures were operating with sufficient effectiveness to achieve stated control objectives (The service auditor determined the nature, timing, and extent of the testing performed. Additional information about the nature, timing, and extent of the testing is contained in section III of this report.)

- The results of the service auditor's tests of operating effectiveness (Additional information about the results of testing is contained in section III of this report.)

## Transaction Processing

### *Control objective 1:* Control structure policies and procedures provide reasonable assurance that investment purchases and sales are properly authorized.

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| Only authorized users are able to input trades into the institutional delivery system (IDS). | Tested the logical access controls, as described in control objective X.* | See control objective X for the results of tests.* |
| | Tested the program change controls, as described in control objective Y.† | See control objective Y for the results of tests.† |
| Trades that are initiated via fax or telephone are authenticated by signature verification or call back. | Reviewed a sample of fax source documentation for evidence of signature verification. Compared the input documentation to the IDS output. | No relevant exceptions were noted. |
| | For a sample of transactions, observed the performance of the call-back procedure over five days. | No relevant exceptions were noted. |
| | Observed personnel in the securities processing group inputting transactions. | No relevant exceptions were noted. |

* This refers to a control objective that would include a description of the logical access control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

† This refers to a control objective that would include a description of the program change control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

***Control objective 2:*** **Control structure policies and procedures provide reasonable assurance that investment purchases and sales are recorded completely, accurately, and on a timely basis.**

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| The institutional delivery system (IDS) compares the trade information from the investment advisor with the trade notifications from the broker/dealer. Differences are identified by IDS and resolved within ten days. Items unresolved after ten days require review and approval by management. | Processed a sample of test purchase and sale transactions through the IDS to determine whether differences were properly identified by the system. The sample included matched and unmatched items. | No relevant exceptions were noted. |
| | Inspected the March 14, June 30, and November 8, 19XX, IDS trade difference reports noting the number and age of differences reported. | Noted that the number and age of differences appeared reasonable and within the Organization's guidelines. |
| | Observed personnel over two days in the execution of follow-up procedures to resolve trade differences. | The procedures observed were consistent with the written policy. No relevant exceptions were noted. |
| | To corroborate written evidential matter, made inquiries of the trade-settlement personnel regarding the procedures followed to resolve differences. | No relevant exceptions were noted. |
| | Made inquiries of the trade-settlement personnel regarding the operation of the procedures through December 31, 19XX. | No relevant exceptions were noted. |

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| | Tested the program change controls, as described in control objective Y.* | See control objective Y for the results of tests.* |
| The IDS compares the trade affirmations received from outside depositories with the trade input information received from the investment advisor. Differences are identified by the IDS and resolved on a timely basis. | Processed a sample of test purchase and sale transactions through the IDS to determine whether exceptions were properly identified and reported by the IDS. The sample included matched and unmatched items. | No relevant exceptions were noted. |
| | Inspected the March 14, June 30, and November 8, 19XX, IDS trade difference reports noting the number and age of the differences reported. | Noted that the number and age of the differences appeared reasonable and within the Organization's guidelines. |
| | Observed personnel over two days in the execution of follow-up procedures to resolve trade differences. | The procedures observed were consistent with written policies. No relevant exceptions were noted. |
| | Made inquiries of the trade-settlement personnel regarding the operation of the procedures through December 31, 19XX. | No relevant exceptions were noted. |
| | Tested the program change controls, as described in control objective Y.* | See control objective Y for the results of tests.* |

*(Continued)*

* This refers to a control objective that would include a description of the program change control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| Security positions with the Depository Trust Company (DTC), the Participants Trust Company (PTC), and the FED are reconciled on a daily basis, and security positions with XYZ Bank are reconciled monthly. The reconciliations are performed through a tape-to-tape computer-matching process (SMAC versus IDS). A report listing balancing positions and out-of-balance positions is produced for review and follow-up (as described below). | Obtained written confirmation of selected security holdings from the depository or custodian as of December 31, 19XX, and compared the information received to data used in the Organization's reconciliation. | No relevant exceptions were noted. |
| | Determined whether changes had been made to the computer programs that affect the SMAC and IDS reconciliations. (The program source code for the SMAC and IDS reconciliation logic was reviewed and tested in 19XX.) | No changes were noted. |
| | Inspected the balancing report at December 31, 19XX, noting the number and age of the SMAC/IDS security position differences. | No relevant exceptions noted in the review of the balancing report. Noted that the number and age of the differences appeared reasonable and within the Organization's guidelines. |
| | Tested the program change controls, as described in control objective Y.* | See control objective Y for the results of tests.* |

* This refers to a control objective that would include a description of the program change control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| The out-of-balance items between the depository or custodian and the Organization are manually reviewed to determine the cause of the out-of-balance condition. All out-of-balance positions are resolved and adjustments are supported by written documentation. An adjustment ticket is completed for each adjustment made. Only designated personnel who have no other security-processing responsibilities are able to authorize adjustments to the SMAC records. | Observed depository-balancing personnel over two days in the execution of follow-up procedures to resolve out-of-balance positions. | The procedures observed were consistent with written policy. No exceptions were noted. |
| | Made inquiries of depository-balancing personnel regarding the procedure followed to resolve differences. | No relevant exceptions were noted. |
| | Inspected a sample of adjustment tickets and noted whether the correction or the out-of-balance condition appeared reasonable and whether it was properly authorized. | In a sample of 100 adjustment tickets, written evidence of authorization was not present on two of the tickets. Through inquiry of management, determined that these two adjustments had been verbally authorized. |

*(Continued)*

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| | Selected a sample of out-of-balance positions from the computer report. For out-of-balance positions resolved through the adjustment process, inspected the adjustment ticket noting (1) the reasonableness of the resolution and (2) whether the ticket was properly authorized. | No relevant exceptions were noted. |
| | Made inquiries of the depository-settlement personnel regarding the operation of the procedure through December 31, 19XX. | No relevant exceptions were noted. |
| | Tested the logical access controls, as described in control objective X.† | See control objective X for the results of tests.† |
| Corporate actions are monitored and identified on a timely basis and are recorded in the corporate action system (CAS). The CAS properly values and records corporate actions including the following:<br>• Bond calls<br>• Returns of capital<br>• Stock splits<br>• Conversions of securities from debt to equity<br>• Stock rights and warrants | Observed the daily processing and made inquiries of the corporate-actions unit personnel regarding the CAS's ability to identify and process corporate actions and the third-party sources for corporate actions that are interfaced directly to CAS. | No relevant exceptions were noted. |

† This refers to a control objective that would include a description of the logical access control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| | Tested the proper recording for a sample of corporate actions per the CAS and the trust accounting system (TAS) and the validity of the reported corporate actions. Selected corporate actions occurring on ten days during 19XX that had been recorded in business publications to ascertain whether they were properly recorded by the CAS. | No relevant exceptions were noted. |
| | Tested the program change controls as described in control objective Y.* | See control objective Y for the results of tests.* |

* This refers to a control objective that would include a description of the program change control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

***Control objective 3:*** **Control structure policies and procedures provide reasonable assurance that investment income is recorded at the appropriate amount and in the appropriate period.**

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| The security movement and control system (SMAC) and the automated income system (AIS) security holdings are manually compared daily and, if necessary, reconciled by authorized individuals. | Made inquiries of management regarding the reconciliation procedures and the exception–resolution process. | No relevant exceptions were noted. |
| | Observed the performance of the daily reconciliation procedures for five days. | The procedures observed were consistent with management's description. |
| | Inspected the March 3, and December 31, 19XX, reconciliations to assess the reasonableness, number, and age of the reconciling items. | No relevant exceptions were noted. |
| | Made inquiries of the income-collection personnel regarding the operation of the procedure through December 31, 19XX. | No relevant exceptions were noted. |
| *Fixed Income Securities* | | |
| Assets with regular or fixed payments, such as corporate and government bonds, are set up on the SMAC at the time | For a sample of fixed income security positions, compared the details of the security holdings (for example, | No relevant exceptions were noted. |

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| of acquisition. The SMAC automatically passes information about such assets to the AIS. Only authorized personnel can set up securities on the SMAC at the time of acquisition. | coupon rate, maturity date, payment frequency and dates) per the SMAC to the AIS. | |
| | For a sample of securities set up on the SMAC during 19XX, compared the details of the security holding per the SMAC to the offering prospectus or comparable external documentation noting agreement. | Noted that the payment date for 1 of the securities included in a 60-item sample was incorrectly stated on the SMAC. Resampled an additional 40 items noting no exceptions. |
| | Tested the logical access controls as described in control objective X.* | See control objective X for the results of tests.* |
| The AIS accrues uncollected investment income and automatically passes the accrual information to the TAS. | For a sample of various types of securities, recalculated the income accruals at September 30, 19XX, and compared the accrual per the AIS to the accrual per the TAS. | No relevant exceptions were noted. |
| | Tested the program change controls as described in control objective Y.† | See control objective Y for the results of tests.† |

*(Continued)*

* This refers to a control objective that would include a description of the logical access control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

† This refers to a control objective that would include a description of the program change control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| *Equity Securities* | | |
| To properly record income on equity securities, a computer tape of dividends declared is prepared and transmitted to the AIS by an outside service on a daily basis. The computer tape of securities reporting dividends for the day is compared to asset holdings on the SMAC, and anticipated dividend maps are created by the AIS. | Made inquiries of the income-collection personnel regarding the source of daily dividend tapes and the procedures followed to interface with the SMAC and the AIS. Observed the daily processing. | No relevant exceptions were noted. |
| | Selected a sample of equity securities, and for each security determined that dividends declared during the period January 1, 19XX, to December 31, 19XX, were properly reflected in the AIS. | No relevant exceptions were noted. |
| | Tested the controls over data transmission, as described in Control objective Z.‡ | See control objective Z for the results of tests.‡ |
| Income is credited to the customer on the ex-dividend date for dividend income. | Selected a sample of dividends per the AIS and verified that they were recorded in the TAS on the ex-date. | No relevant exceptions were noted. |

‡ This refers to a control objective that would include a description of the data transmission control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

***Control objective 4:*** **Control structure policies and procedures provide reasonable assurance that investment income is collected on a timely basis.**

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| The AIS compares the income received from the depository or directly from the issuer to the anticipated income map on a security-by-security basis. Differences between the expected receipts and the actual receipts are reported, investigated, and resolved by authorized income-collection personnel on a timely basis. | Processed a sample of test collections and corrections through the AIS to determine whether the AIS properly processes and reports. | No relevant exceptions were noted. |
| | Inspected the anticipated income reports noting whether the nature and age of the outstanding differences were reasonable and within Organization guidelines. | No relevant exceptions were noted. |
| | Made inquiries of the income-collection personnel regarding the operation of the procedure through December 31, 19XX. | No relevant exceptions were noted. |
| | Observed the income-collection personnel investigating unresolved differences. | No relevant exceptions were noted. |

***Control objective 5:*** **Control structure policies and procedures provide reasonable assurance that the market value of exchange-traded securities are properly calculated using prices obtained from outside pricing services.**

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| Daily transmissions of prices of exchange-traded securities are received from independent sources. | Made inquiries of the Organization's personnel regarding the sources of prices for various kinds of securities (for example, governments, corporate bonds, equities, asset-backed) and the procedures followed for the transmission and verification of prices. Observed the daily processing. | No relevant exceptions were noted. |
| | Tested the controls over data transmission, as described in control objective Z.* | See control objective Z for the results of tests.* |
| Market prices obtained from independent sources are automatically compared daily to assess the reasonableness of the prices received. Discrepancies in the prices are identified, researched, and resolved by authorized personnel. | Observed the performance of the daily comparison and the resolution of discrepancies in prices. | No relevant exceptions were noted. |

* This refers to a control objective that would include a description of the data transmission control structure policies and procedures, the tests of the policies and procedures, and the results of the tests. Such information is not included in this sample report.

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor* | *Results of Tests* |
|---|---|---|
| Market prices are multiplied by the holdings in each customer's account on SMAC to determine the market value of the positions. | Used the CAT to recalculate the market value of the securities based on information provided by independent sources and the information contained on the SMAC. | No relevant exceptions were noted. |

***Note to Readers:*** *The control objectives included in this sample report are presented for illustrative purposes only and are not intended to represent a complete set of control objectives. Control objectives 1 through 5 and the related policies and procedures presented on the preceding pages cover certain aspects of transaction processing. Other control objectives related to transaction processing and control objectives related to CIS that might need to be included in an actual report, are not illustrated in this sample report.*

## Regulatory Compliance – ERISA

The major law applicable to employee benefit plans and trusts is the Employee Retirement Income Security Act (ERISA). ERISA covers most private sector employee benefit plans. Under ERISA, a fiduciary is generally defined as any person or organization that has or exercises power or control over the management of the plan or disposition of the plan's assets. Under ERISA, a fiduciary is required to discharge its duties solely in the interest of the plan's participants and beneficiaries and for the exclusive purpose of providing and defraying reasonable expenses of administrating the plan. Generally, ERISA fiduciaries are required to discharge their duties (1) in accordance with documents or instruments governing the plan, (2) with the care, skill, prudence, and diligence of a prudent person acting in like capacity, and (3) by diversifying assets of the plan to minimize the risk of large losses. In addition, plan fiduciaries are forbidden from engaging in certain "prohibited transactions," as defined by ERISA. A summary of the major provisions of Part 4 of Title 1 of ERISA, which establishes the fiduciary responsibilities that the Organization must comply with, are presented below:

- *Section 402* — Employee benefit plans are to be established and maintained in accordance with a written plan.
- *Section 404* — Fiduciaries are required to discharge their duties with respect to a plan solely in the interests of the participants and beneficiaries.
- *Section 406* — Parties-in-interest transactions are prohibited except where specifically exempted.

- *Sections 407 and 408* — Investments by a plan in qualifying employer securities or real property is generally limited to 10 percent of a plan's assets unless the plan agreement and ERISA permit a larger percentage.
- *Section 411* — Fiduciaries are required to ensure that the background of personnel employed in fiduciary services is suitable to the nature of trust activities.

The Organization's control objective related to regulatory compliance, the related control structure policies and procedures, and the service auditor's tests of operating effectiveness are presented below.

***Control objective 6:*** **Control structure policies and procedures provide reasonable assurance that when administering accounts subject to ERISA, the organization complies with the applicable requirements of ERISA.***

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor** | *Results of Tests** |
|---|---|---|
| New accounts are accepted only after the Organization's in-house counsel reviews the plan's document. Acceptance of new accounts must be approved by the Administrative and Investment Review Committee. | See footnote*. | See footnote*. |
| The background of personnel employed in fiduciary services is appropriately investigated. Account administrators are appropriately trained with respect to the requirements of ERISA including those pertaining to parties-in-interest transactions. | See footnote*. | See footnote*. |

* The testing performed by the service auditor and the results of the tests are not illustrated in this sample report.

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor** | *Results of Tests** |
|---|---|---|
| An annual review of each account is performed by the Administration and Investment Review Committee. The purpose of the review is to (1) assess compliance with the trust agreement (2) detect prohibited transactions, and (3) to assess prudence and investment performance for discretionary accounts. | See footnote*. | See footnote*. |
| In connection with the acceptance of a new account, the Organization requires that the plan administrator provide a list of parties-in-interest. This list is provided to the Organization's account administrator who is responsible for reviewing and approving transactions other than ordinary security trades. For companies (including the plan sponsor) with publicly traded securities, a restriction is placed on the security in the institutional delivery system (IDS) so that prohibited parties-in-interest transactions will be identified prior to their execution. | See footnote*. | See footnote*. |

*(Continued)*

| *Control Structure Policies and Procedures Specified by Example Trust Organization* | *Testing Performed by the Service Auditor** | *Results of Tests** |
|---|---|---|
| The annual statements prepared by the Organization are used in the preparation of each plan's Form 5500. Such statements, which are prepared by the TAS, also include supplemental schedules, such as the schedule of assets held for investment and the schedule of reportable (5 percent) transactions. Each annual accounting statement and each of the required schedules are reviewed by the account administrator prior to certifying that the statement is "complete and accurate." | See footnote*. | See footnote*. |
| Overall compliance with the requirements of ERISA relevant to the Organization is monitored by the trust compliance unit and the internal audit group. | See footnote*. | See footnote*. |

* The testing performed by the service auditor and the results of the tests are not illustrated in this sample report.

## USER CONTROL CONSIDERATIONS

The Organization's processing of transactions and the control structure policies and procedures over the processing were designed with the assumption that certain internal control structure policies and procedures would be placed in operation at user organizations. This section describes some of the internal control structure policies and procedures that should be in operation at user organizations to complement the control structure policies and procedures at the Organization. User auditors should determine whether user organizations have established internal control structure policies and procedures to ensure that —

- Instructions and information provided to the Organization from institutional trust users are in accordance with the provisions of the servicing agreement, trust agreement, or other applicable governing agreements or documents between the Organization and the user.
- Appropriate controls over physical and logical access to the Organization's systems via terminals at user locations are established, monitored, and maintained by the institutional trust user.
- Timely written notification of changes to the plan, its objectives, participants, and investment managers is adequately communicated to the Organization.
- Timely written notification of changes in the designation of individuals authorized to instruct the Organization regarding activities, on behalf of the institutional trust user, is adequately communicated to the Organization.
- Timely review of reports provided by the Organization of institutional trust account balances and related activities is performed by the institutional trust user, and written notice of discrepancies is provided to the Organization.
- Timely written notification of changes in related parties for purposes of identifying parties-in-interest transactions is adequately communicated to the Organization.

# III

# INFORMATION PROVIDED BY THE SERVICE AUDITOR

This report is intended to provide users of the institutional trust division of the Organization with information about the control structure policies and procedures at the Organization that may affect the processing of user organizations' transactions and also to provide users with information about the operating effectiveness of the policies and procedures that were tested. This report, when combined with an understanding and assessment of the internal control structure policies and procedures at user organizations, is intended to assist user auditors in (1) planning the audit of user organizations' financial statements and in (2) assessing control risk for assertions in user organizations' financial statements that may be affected by policies and procedures at the Organization.

Our testing of the Organization's control structure policies and procedures was restricted to the control objectives and the related policies and procedures listed in the matrices in section II of this report and was not extended to procedures described in section II but not included in the aforementioned matrices, or to procedures that may be in effect at user organizations. It is each user auditor's responsibility to evaluate this information in relation to the internal control structure policies and procedures in place at each user organization. If certain complementary controls are not in place at user organizations, the Organization's control structure polices and procedures may not compensate for such weaknesses.

## CONTROL ENVIRONMENT ELEMENTS

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specific policies and procedures. In addition to tests of the operating effectiveness of the policies and procedures in the matrices in section II of this report, our procedures also included tests of and consideration of the relevant elements of the Organization's control environment including —

- The Organization's organizational structure and the segregation of duties.
- The functioning of the board of directors and its committees, particularly the committees that oversee the Organization's trust activities.
- Management control methods.
- Personnel policies and practices.
- Internal audit.
- Regulation of the Organization by banking authorities.

Our tests of the control environment included the following procedures to the extent we considered necessary:

- A review of the Organization's organizational structure, including the segregation of duties, policy statements, accounting and processing manuals, personnel policies and the internal audit and compliance units' policies, procedures, and reports
- Discussions with management, operations, administrative, and other personnel who are responsible for developing, ensuring adherence to, and applying control structure policies, and procedures
- Observations of personnel in the performance of their assigned duties
- A review of the Organization's actions taken in response to recommendations to improve internal control structure policies and procedures made by the internal audit and compliance units and regulators having supervisory oversight over the Organization's fiduciary activities

The control environment was considered in determining the nature, timing, and extent of the tests of operating effectiveness of the control structure policies and procedures.

## TESTS OF OPERATING EFFECTIVENESS

The description of the tests of operating effectiveness and the results of those tests are included in section II of this report and are the responsibility of the service auditor.

# IV

# OTHER INFORMATION PROVIDED BY EXAMPLE TRUST ORGANIZATION

***Note to Readers:*** *Details of other information provided by Example Trust Organization are not included in this sample report.*

Appendix B

# Illustrative Representation Letter for a Service Auditor's Engagement

[*Date*]

To [*Name of Service Auditor*]

In connection with your engagement to report on Example Computer Service Organization's (the Organization) description of policies and procedures placed in operation, we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion on whether the description presents fairly, in all material respects, the relevant aspects of the Organization's policies and procedures that had been placed in operation as of [*specify date*], and whether the policies and procedures were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those policies and procedures were complied with satisfactorily, (and whether the control structure policies and procedures that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved for the [*specify the period covered by the tests of operating effectiveness*]).[1] Accordingly, we make the following representations, which are true to the best of our knowledge and belief.

## GENERAL

We recognize that, as members of management of the Organization, we are responsible for the fair presentation of the description of the Organization's control structure policies and procedures and for establishing and

1. Included only when reporting on the operating effectiveness of policies and procedures to achieve specified control objectives.

maintaining appropriate control structure policies and procedures related to the processing of transactions for user organizations.

We believe that the description of policies and procedures presents fairly, in all material respects, those aspects of the Organization's policies and procedures that may be relevant to user organizations' internal control structures.

We have responded fully to all inquiries made to us by you during your examination.

## DESCRIPTION OF POLICIES AND PROCEDURES PLACED IN OPERATION

The control objectives specified in our description of policies and procedures include all of the control objectives that we believe are relevant to users of the services described in the report and are appropriate based on the services provided to user organizations [or based on third-party criteria].

The control structure policies and procedures described in the description of policies and procedures had been placed in operation as of [*specify date*].

The control structure policies and procedures are suitably designed to achieve the control objectives specified in the description of policies and procedures.

We have disclosed to you any significant changes in control structure policies and procedures that have occurred since the Organization's last examination [or "within the last twelve months" for initial examinations].

We have disclosed to you all design deficiencies in control structure policies and procedures of which we are aware, including those for which we believe the cost of corrective action may exceed the benefits.

## OPERATING EFFECTIVENESS OF POLICIES AND PROCEDURES[2]

We have disclosed to you all instances of which we are aware of control structure policies and procedures not operating with sufficient effectiveness to achieve specified control objectives.

2. Included only when reporting on the operating effectiveness of policies and procedures to achieve specified control objectives.

## ILLEGAL ACTS, IRREGULARITIES, OR UNCORRECTED ERRORS

We are not aware of any illegal acts, irregularities, or uncorrected errors attributable to management or employees of the Organization who have significant roles relevant to the processing performed for user organizations.[3]

We understand that your examination was conducted in accordance with generally accepted auditing standards as defined and described by the American Institute of Certified Public Accountants and was, therefore, designed primarily for the purpose of expressing an opinion on (1) the Organization's description of policies and procedures, (2) the suitability of the design of the policies and procedures [and (3) the operating effectiveness of the policies and procedures[4]], as described in the first paragraph of this letter, and that your procedures were limited to those that you considered necessary for this purpose.

Very truly yours,

[*Signature of appropriate service organization personnel*]

The letter of representation should be dated as of the completion of fieldwork.

3. If there are such matters, management should include a representation as to whether the illegal acts, irregularities, or uncorrected errors are clearly inconsequential. If such matters are not clearly inconsequential, management should include a representation that such matters have been communicated to the affected organizations.

4. Included only when reporting on the operating effectiveness of policies and procedures to achieve specified control objectives.

Appendix C

# Responsibilities of Service Organizations, Service Auditors, and User Auditors If Subservice Organizations Perform Significant Functions for User Organizations and Control Objectives Are Established by the Service Organization

*Table appears on the following page.*

*Service Organization's Responsibilities*

Describe the service organization's policies and procedures that may be relevant to user organizations' internal control structures (SAS No. 70, paragraph 26).

Describe the control objectives established by the service organization (SAS No. 70, paragraph 34*a*).

Identify the functions and nature of the processing performed by the subservice organization, and either:

*Service Auditor's Responsibilities*

Disclose in the service auditor's report that the control objectives were established by the service organization (SAS No. 70, paragraphs 29*c* and 44*c*). The service auditor should be satisfied that the control objectives, as set forth by the service organization, are reasonable in the circumstances and consistent with the service organization's contractual obligations (SAS No. 70, paragraph 35).

Opine on (1) the fairness of the presentation of the description of policies and procedures placed in operation, (2) whether the policies and procedures were suitably designed to achieve specified control objectives [and, when the report includes tests of operating effectiveness, (3) whether the policies and procedures that were tested were operating with sufficient effectiveness to achieve the related control objectives], and either:

*User Auditor's Responsibilities*

Determine whether the report meets the user auditor's needs. If the user auditor requires further information about the functions performed by the subservice organization or about the subservice organization's policies and procedures, the user auditor should consider obtaining information about the subservice organization in a manner similar to that described in SAS No. 70, paragraphs 7 through 21.

*Carve-Out Method**

1. Omit from the description the subservice organization's relevant policies, procedures, and control objectives and state in the description that the policies, procedures, and control objectives have been omitted.

*Carve-Out Method*

1. Modify the scope paragraph of the service auditor's report to briefly summarize the functions and the nature of the processing performed by the subservice organization and to indicate that the policies, procedures, and related control objectives of the subservice organization were omitted from the description.

or

*Inclusive Method**

2. Include the subservice organization's relevant policies, procedures, and control objectives in the description. The control objectives will include all of the control objectives a user auditor would expect both the service organization and the subservice organization to achieve.

or

*Inclusive Method*

2. Identify the entities included in the scope of the examination. With respect to the policies and procedures of the subservice organization, follow procedures comparable to those described in paragraph 12 of SAS No. 70, which include:

- Performing procedures related to the service organization's controls over the activities of the subservice organization.
- Performing procedures at the subservice organization

The service auditor should consider the matters discussed in appendix A on pages 80–81 of this APS.



*This APS does not provide for the option of having a service auditor make reference to or rely on a subservice auditor's report as the basis, in part, for the service auditor's opinion.

Appendix D

# Responsibilities of Service Organizations, Service Auditors, and User Auditors If Subservice Organizations Perform Significant Functions for User Organizations and Control Objectives Are Established by an Outside Party

*Table appears on the following page.*

*Service Organization's Responsibilities*

Describe the service organization's policies and procedures that may be relevant to user organizations' internal control structures (SAS No. 70, paragraph 26).

Describe the control objectives established by the outside party (SAS No. 70, paragraph 34*a*).

Identify the functions and nature of the processing performed by the subservice organization, and either:

*Carve-Out Method**

1. Omit from the description the subservice organization's relevant policies and procedures and state in the description that the policies and procedures have been omitted.

*Service Auditor's Responsibilities*

Identify in the service auditor's report the source of the control objectives (SAS No. 70, paragraphs 29*c* and 44*c*). The service auditor does not need to determine whether the control objectives are reasonable in the circumstances and consistent with the service organization's contractual obligations because the control objectives have been established by an outside party (SAS No. 70, paragraph 35).

Opine on (1) the fairness of the presentation of the description of policies and procedures placed in operation, (2) whether the policies and procedures were suitably designed to achieve specified control objectives [and, when the report includes tests of operating effectiveness, (3) whether the policies and procedures that were tested were operating with sufficient effectiveness to achieve the related control objectives], and either:

*Carve-Out Method*

1. Modify the scope paragraph of the service auditor's report to briefly summarize the functions and the nature of the processing performed by the subservice organization and to indicate that the policies, procedures, and related control objectives of the subservice organization were omitted from the description.

*User Auditor's Responsibilities*

Determine whether the report meets the user auditor's needs. If the user auditor requires further information about the functions performed by the subservice organization or about the subservice organization's policies and procedures, the user auditor should consider obtaining information about the subservice organization in a manner similar to that described in SAS No. 70, paragraphs 7 through 21.

or

*Inclusive Method**

2. Include in the description the policies and procedures that the subservice organization is responsible for.

or

*Inclusive Method*

2. Identify the entities included in the scope of the examination. With respect to the policies and procedures of the subservice organization, follow procedures comparable to those described in paragraph 12 of SAS No. 70, which include:

- Performing procedures related to the service organization's controls over the activities of the subservice organization.
- Performing procedures at the subservice organization

The service auditor should consider the matters discussed in appendix A on pages 80–81 of this APS.



*This APS does not provide for the option of having a service auditor make reference to or rely on a subservice auditor's report as the basis, in part, for the service auditor's opinion.

Appendix E

# Statement on Auditing Standards No. 70, *Reports on the Processing of Transactions by Service Organizations*

**(*Supersedes Statement on Auditing Standards No. 44, AICPA,* Professional Standards, *vol. 1, AU sec. 324.*)**

## INTRODUCTION AND APPLICABILITY

**1.** This Statement provides guidance on the factors an independent auditor should consider when auditing the financial statements of an entity that uses a service organization to process certain transactions. This Statement also provides guidance for independent auditors who issue reports on the processing of transactions by a service organization for use by other auditors.

**2.** For purposes of this Statement, the following definitions apply:

- *User organization* — The entity that has engaged a service organization and whose financial statements are being audited
- *User auditor* — The auditor who reports on the financial statements of the user organization
- *Service organization* — The entity (or segment of an entity) that provides services to the user organization
- *Service auditor* — The auditor who reports on the processing of transactions by a service organization
- *Report on policies and procedures placed in operation* — A service auditor's report on a service organization's description of its control structure policies and procedures that may be relevant to a user organization's internal control structure, on whether such policies and procedures were suitably designed to achieve specified control objectives, and on whether they had been placed in operation as of a specific date

- *Report on policies and procedures placed in operation and tests of operating effectiveness* — A service auditor's report on a service organization's description of its control structure policies and procedures that may be relevant to a user organization's internal control structure,[1] on whether such policies and procedures were suitably designed to achieve specified control objectives, on whether they had been placed in operation as of a specific date, and on whether the policies and procedures 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

**3.** The guidance in this Statement is applicable to the audit of the financial statements of an entity that obtains either or both of the following services from another organization:

- Executing transactions and maintaining the related accountability
- Recording transactions and processing related data

Service organizations that provide such services include, for example, bank trust departments that invest and hold assets for employee benefit plans or for others, mortgage bankers that service mortgages for others, and electronic data processing (EDP) service centers that process transactions and related data for others. The guidance in this Statement may also be relevant to situations in which an organization develops, provides, and maintains the software used by client organizations. The provisions of this Statement are not intended to apply to situations in which the services provided are limited to executing client organization transactions that are specifically authorized by the client, such as the processing of checking account transactions by a bank or the execution of securities transactions by a broker. This Statement also is not intended to apply to the audit of transactions arising from financial interests in partnerships, corporations, and joint ventures, such as working interests in oil and gas ventures, when proprietary interests are accounted for and reported to interest holders.

**4.** This Statement is organized into the following sections:

*a.* The user auditor's consideration of the effect of the service organization on the internal control structure of the user organization and the availability of evidence to —
   - Obtain the necessary understanding of the user organization's internal control structure to plan the audit
   - Assess control risk at the user organization

1. In this Statement, a service organization's control structure policies and procedures that may be relevant to a user organization's internal control structure will be referred to as a service organization's *policies and procedures*.

- Perform substantive procedures

*b.* Considerations in using a service auditor's report

*c.* Responsibilities of service auditors

## THE USER AUDITOR'S CONSIDERATION OF THE EFFECT OF THE SERVICE ORGANIZATION ON THE INTERNAL CONTROL STRUCTURE OF THE USER ORGANIZATION AND THE AVAILABILITY OF AUDIT EVIDENCE

**5.** The user auditor should consider the discussion in paragraphs 6 through 21 when planning and performing the audit of an entity that uses a service organization to process its transactions.

### The Effect of a Service Organization on a User Organization's Internal Control Structure

**6.** When a user organization uses a service organization, transactions that affect the user organization's financial statements are subjected to policies and procedures that are, at least in part, physically and operationally separate from the user organization. The relationship of the policies and procedures of the service organization to those of the user organization depends primarily on the nature of the services provided by the service organization. For example, when those services are limited to recording user transactions and processing the related data, and the user organization retains responsibility for authorizing transactions and maintaining the related accountability, there is a high degree of interaction between the policies and procedures at the service organization and those at the user organization. In these circumstances, it may be possible for the user organization to implement effective internal control structure policies and procedures for those transactions. When the service organization executes the user organization's transactions and maintains the related accountability, there is a lower degree of interaction and it may not be practicable for the user organization to implement effective internal control structure policies and procedures for those transactions. The degree of interaction, as well as the nature and materiality of the transactions processed by the service organization, are the most important factors in determining the significance of the service organization's policies and procedures to the user organization's internal control structure.

## PLANNING THE AUDIT

**7.** SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 319), states that an auditor should obtain a sufficient understanding of each of the three elements of the entity's internal control structure to plan the

audit. This understanding should include knowledge about the design of relevant policies, procedures, and records and whether they have been placed in operation by the entity. In planning the audit, such knowledge should be used to —

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

**8.** If an entity uses a service organization, certain policies, procedures, and records of the service organization may be relevant to the user organization's ability to record, process, summarize, and report financial data consistent with the assertions embodied in the entity's financial statements. In determining the significance of these policies, procedures, and records to planning the audit, the user auditor should consider factors such as —

- The significance of the financial statement assertions that are affected by the policies and procedures of the service organization.
- The inherent risk associated with the assertions affected by the policies and procedures of the service organization.
- The nature of the services provided by the service organization and whether they are highly standardized and used extensively by many user organizations or unique and used only by a few.
- The extent to which the user organization's internal control structure policies and procedures interact with the policies and procedures of the service organization.
- The user organization's internal control structure policies and procedures that are applied to the transactions affected by the service organization's activities.
- The terms of the contract between the user organization and the service organization (for example, their respective responsibilities and the extent of the service organization's discretion to initiate transactions).
- The service organization's capabilities, including its —
  - — Record of performance.
  - — Insurance coverage.
  - — Financial stability.
- The user auditor's prior experience with the service organization.
- The extent of auditable data in the user organization's possession.
- The existence of specific regulatory requirements that may dictate the application of audit procedures beyond those required to comply with generally accepted auditing standards.

**9.** The user auditor should also consider the available information about the service organization's policies and procedures, including *(a)* the information in the user organization's possession, such as user manuals, system overviews, and technical manuals, and *(b)* the existence of reports on the

service organization's policies and procedures, such as reports by service auditors, internal auditors (the user organization's or the service organization's), or regulatory authorities.

**10.** After considering the above factors and evaluating the available information, the user auditor may conclude that he or she has the means to obtain a sufficient understanding of the internal control structure 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, to obtain specific information or request that a service auditor be engaged to perform procedures that will supply the necessary information, or the user auditor may visit the service organization and perform such procedures. If the user auditor is unable to obtain sufficient evidence to achieve his or her audit objectives, the user auditor should qualify his or her opinion or disclaim an opinion on the financial statements because of a scope limitation.

## Assessing Control Risk at the User Organization

**11.** After obtaining an understanding of the internal control structure, the user auditor assesses control risk for the assertions embodied in the account balances and classes of transactions, including those that are affected by the activities of the service organization. In doing so, the user auditor may identify certain internal control structure policies and procedures that, if effective, would permit the user auditor to assess control risk below the maximum for particular assertions. Such policies and procedures may be applied at either the user organization or the service organization. The user auditor may conclude that it would be efficient to obtain evidential matter about the operating effectiveness of these policies and procedures to provide a basis for assessing control risk below the maximum.

**12.** A service auditor's report on policies and procedures placed in operation at the service organization should be helpful in providing a sufficient understanding to plan the audit of the user organization. Such a report, however, is not intended to provide any evidence of the operating effectiveness of the relevant policies and procedures that would allow the user auditor to reduce the assessed level of control risk below the maximum. Such evidential matter should be derived from one or more of the following:

*a.* Tests of the user organization's controls over the activities of the service organization (for example, the user auditor may test the user organization's independent reperformance of selected items processed by an EDP service center or test the user organization's reconciliation of output reports with source documents)
*b.* A service auditor's report on policies and procedures placed in operation and tests of operating effectiveness, or a report on the application of agreed-upon procedures that describes relevant tests of controls

c. Appropriate tests of controls performed by the user auditor at the service organization

**13.** The user organization may establish effective controls over the service organization's activities that may be tested and that may enable the user auditor to reduce the assessed level of control risk below the maximum for some or all of the related assertions. If a user organization, for example, uses an EDP service center to process payroll transactions, the user organization may establish internal control structure policies and procedures over input and output data to prevent or detect material misstatements. The user organization might reperform the service organization's payroll calculations on a test basis. In this situation, the user auditor may perform tests of the user organization's controls over data processing that would provide a basis for assessing control risk below the maximum for the assertions related to payroll transactions. The user auditor may decide that obtaining evidence of the operating effectiveness of the service organization's policies and procedures, such as those over changes in payroll programs, is not necessary or efficient.

**14.** The user auditor may find that internal control structure policies and procedures relevant to assessing control risk below the maximum for particular assertions are applied only at the service organization. If the user auditor plans to assess control risk below the maximum for those assertions, he or she should evaluate the operating effectiveness of those policies and procedures by obtaining a service auditor's report that describes the results of the service auditor's tests of those policies and procedures (that is, a report on policies and procedures placed in operation and tests of operating effectiveness, or an agreed-upon procedures report) or by performing tests of controls at the service organization. If the user auditor decides to use a service auditor's report, the user auditor should consider the extent of the evidence provided by the report about the effectiveness of policies and procedures intended to prevent or detect material misstatements in the particular assertions. The user auditor remains responsible for evaluating the evidence presented by the service auditor and for determining its effect on the assessment of control risk at the user organization.

**15.** The user auditor's assessments of control risk regarding assertions about account balances or classes of transactions are based on the combined evidence provided by the service auditor's report and the user auditor's own procedures. In making these assessments, the user auditor should consider the nature, source, and interrelationships among the evidence, as well as the period covered by the tests of controls. The user auditor uses the assessed levels of control risk, as well as his or her understanding of the internal control structure, in determining the nature, timing, and extent of substantive tests for particular assertions.

**16.** The guidance in SAS No. 55, paragraphs 46 through 55, regarding the auditor's consideration of the sufficiency of evidential matter to support

a specific assessed level of control risk is applicable to user auditors considering evidential matter provided by a service auditor's report on policies and procedures placed in operation and tests of operating effectiveness. Because the report may be intended to satisfy the needs of several different user auditors, a user auditor should determine whether the specific tests of controls and results in the service auditor's report are relevant to assertions that are significant in the user organization's financial statements. For those tests of controls and results that are relevant, a user auditor should consider whether the nature, timing, and extent of such tests of controls and results provide appropriate evidence about the effectiveness of the policy or procedure to support the user auditor's desired assessed level of control risk. In evaluating these factors, user auditors should also keep in mind that, for certain assertions, the shorter the period covered by a specific test and the longer the time elapsed since the performance of the test, the less support for control risk reduction the test may provide.

### Audit Evidence From Substantive Audit Procedures Performed by Service Auditors

**17.** Service auditors may be engaged to perform procedures that are substantive in nature for the benefit of user auditors. Such engagements may involve the performance, by the service auditor, of procedures agreed upon by the user organization and its auditor and by the service organization and its auditor. In addition, there may be requirements imposed by governmental authorities or through contractual arrangements whereby service auditors perform designated procedures that are substantive in nature. The results of the application of the required procedures to balances and transactions processed by the service organization may be used by user auditors as part of the evidence necessary to support their opinions.

## CONSIDERATIONS IN USING A SERVICE AUDITOR'S REPORT

**18.** In considering whether the service auditor's report is satisfactory for his or her purposes, the user auditor should make inquiries concerning the service auditor's professional reputation. Appropriate sources of information concerning the professional reputation of the service auditor are discussed in SAS No. 1, *Codification of Auditing Standards and Procedures* (AICPA, *Professional Standards,* vol. 1, AU sec. 543, "Part of Audit Performed by Other Independent Auditors," paragraph 10*a*).

**19.** In considering whether the service auditor's report is sufficient to meet his or her objectives, the user auditor should give consideration to the guidance in AU sec. 543.12. If the user auditor believes that the service auditor's report may not be sufficient to meet his or her objectives, the user auditor may supplement his or her understanding of the service auditor's procedures and conclusions by discussing with the service auditor the scope and results of the service auditor's work. Also, if the user auditor

believes it is necessary, he or she may contact the service organization, through the user organization, to request that the service auditor perform agreed-upon procedures at the service organization, or the user auditor may perform such procedures.

**20.** When assessing a service organization's policies and procedures and how they interact with a user organization's internal control structure policies and procedures, the user auditor may become aware of the existence of reportable conditions. In such circumstances, the user auditor should consider the guidance provided in SAS No. 60, *Communication of Internal Control Structure Related Matters Noted in an Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 325).

**21.** The user auditor should not make reference to the report of the service auditor as a basis, in part, for his or her own opinion on the user organization's financial statements. The service auditor's report is used in the audit, but the service auditor is not responsible for examining any portion of the financial statements as of any specific date or for any specified period. Thus, there cannot be a division of responsibility for the audit of the financial statements.

## RESPONSIBILITIES OF SERVICE AUDITORS

**22.** The service auditor is responsible for the representations in his or her report and for exercising due care in the application of procedures that support those representations. Although a service auditor's engagement differs from an audit of financial statements conducted in accordance with generally accepted auditing standards, it should be performed in accordance with the general standards and with the relevant fieldwork and reporting standards. Although the service auditor should be independent from the service organization, it is not necessary for the service auditor to be independent from each user organization.

**23.** As a result of procedures performed at the service organization, the service auditor may become aware of illegal acts, irregularities, or uncorrected errors attributable to the service organization's management or employees that may affect one or more user organizations. The terms *errors, irregularities,* and *illegal acts* are defined in SAS No. 53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities,* and SAS No. 54, *Illegal Acts by Clients* (AICPA, *Professional Standards,* vol. 1, AU secs. 316 and 317); the definitions therein are relevant to this section. When the service auditor becomes aware of such matters, he or she should determine from the appropriate level of management of the service organization whether this information has been communicated appropriately to affected user organizations, unless those matters are clearly inconsequential. If the management of the service organization has not communicated the infor-

mation to affected user organizations and is unwilling to do so, the service auditor should inform the service organization's audit committee or others with equivalent authority or responsibility. If the audit committee does not respond appropriately to the service auditor's communication, the service auditor should consider whether to resign from the engagement. The service auditor may wish to consult with his or her attorney in making this decision.

**24.** The type of engagement to be performed and the related report to be prepared should be established by the service organization. However, when circumstances permit, discussions between the service organization and the user organizations are advisable to determine the type of report that will be most suitable for the user organizations' needs. This Statement provides guidance on the two types of reports that may be issued:

a. *Reports on policies and procedures placed in operation* — A service auditor's report on a service organization's description of the policies and procedures that may be relevant to a user organization's internal control structure, on whether such policies and procedures were suitably designed to achieve specified objectives, and on whether they had been placed in operation as of a specific date. Such reports may be useful in providing a user auditor with an understanding of the policies and procedures necessary to plan the audit and to design effective tests of controls and substantive tests at the user organization, but they are not intended to provide the user auditor with a basis for reducing his or her assessments of control risk below the maximum.
b. *Reports on policies and procedures placed in operation and tests of operating effectiveness* — A service auditor's report on a service organization's description of the policies and procedures that may be relevant to a user organization's internal control structure, on whether such policies and procedures were suitably designed to achieve specified control objectives, on whether they had been placed in operation as of a specific date, and on whether the policies and procedures 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 the user auditor with an understanding of the policies and procedures necessary to plan the audit and may also provide the user auditor with a basis for reducing his or her assessments of control risk below the maximum.

## Reports on Policies and Procedures Placed in Operation

**25.** The information necessary for a report on policies and procedures placed in operation ordinarily is obtained through discussions with appropriate service organization personnel and through reference to various forms of documentation, such as system flowcharts and narratives.

**26.** After obtaining a description of the relevant policies and procedures, the service auditor should determine whether the description provides sufficient information for user auditors to obtain an understanding of those aspects of the service organization's policies and procedures that may be relevant to a user organization's internal control structure. The description should contain a discussion of the features of the service organization's policies and procedures that would have an effect on a user organization's internal control structure. Such features are relevant when they directly affect the service provided to the user organization. They may include features generally considered to be part of the control environment, specific activities that may represent a user organization's accounting system or a portion thereof, or specific policies and procedures designed to control such functions. Control environment elements may include hiring practices and the involvement of internal auditors. Accounting system elements would include the ways in which user transactions are initiated and processed. Control structure policies and procedures employed by a service organization, such as policies and procedures over the modification of computer programs, ordinarily are designed to meet specific control objectives. The specific control objectives of the service organization should be set forth in the service organization's description of policies and procedures.

**27.** Evidence of whether policies and procedures have been placed in operation is ordinarily obtained through previous experience with the service organization and through procedures such as inquiry of appropriate management, supervisory, and staff personnel; inspection of service organization documents and records; and observation of service organization activities and operations. For the type of report described in paragraph 24*a*, these procedures need not be supplemented by tests of the operating effectiveness of the service organization's policies and procedures.

**28.** Although a service auditor's report on policies and procedures placed in operation is as of a specified date, the service auditor should inquire about changes in the service organization's policies and procedures that may have occurred before the beginning of fieldwork. If the service auditor believes that the changes would be considered significant by user organizations and their auditors, those changes should be included in the description of the service organization's policies and procedures. If the service auditor concludes that the changes would be considered significant by user organizations and their auditors and the changes are not included in the description of the service organization's policies and procedures, the service auditor should describe the changes in his or her report. Such changes might include —

- Procedural changes made to accommodate provisions of a new FASB Statement of Financial Accounting Standards.
- Major changes in an application to permit on-line processing.
- Procedural changes to eliminate previously identified deficiencies.

Changes that occurred more than twelve months before the date being reported on normally would not be considered significant, because they generally would not affect user auditors' considerations.

**29.** A service auditor's report expressing an opinion on a description of policies and procedures placed in operation at a service organization should contain —

*a.* A specific reference to the applications, services, products, or other aspects of the service organization covered.
*b.* A description of the scope and nature of the service auditor's procedures.
*c.* Identification of the party specifying the control objectives.
*d.* An indication that the purpose of the service auditor's engagement was to obtain reasonable assurance about whether (1) the service organization's description presents fairly, in all material respects, the aspects of the service organization's policies and procedures that may be relevant to a user organization's internal control structure, (2) the policies and procedures were suitably designed to achieve specified control objectives, and (3) such policies and procedures had been placed in operation as of a specific date.
*e.* A disclaimer of opinion on the operating effectiveness of the policies and procedures.
*f.* The service auditor's opinion on whether the description presents fairly, in all material respects, the relevant aspects of the service organization's policies and procedures that had been placed in operation as of a specific date and whether, in the service auditor's opinion, the policies and procedures were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those policies and procedures were complied with satisfactorily.
*g.* A statement of the inherent limitations of the potential effectiveness of policies and procedures at the service organization and of the risk of projecting to future periods any evaluation of the description.
*h.* Identification of the parties for whom the report is intended.

**30.** If the service auditor believes that the description is inaccurate or insufficiently complete for user auditors, the service auditor's report should so state and should contain sufficient detail to provide user auditors with an appropriate understanding.

**31.** It may become evident to the service auditor, when considering the service organization's description of policies and procedures placed in operation, that the system was designed with the assumption that certain internal control structure policies and procedures would be implemented by the user organization. If the service auditor is aware of the need for such complementary user organization internal control structure policies and

procedures, these should be delineated in the description of policies and procedures. If the application of internal control structure policies and procedures by user organizations is necessary to achieve the stated control objectives, the service auditor's report should be modified to include the phrase "and user organizations applied the internal control structure policies and procedures contemplated in the design of the Service Organization's policies and procedures" following the words "complied with satisfactorily" in the scope and opinion paragraphs.

**32.** The service auditor should consider conditions that come to his or her attention that, in the service auditor's judgment, represent significant deficiencies in the design or operation of the service organization's policies and procedures that preclude the service auditor from obtaining reasonable assurance that specified control objectives would be achieved. The service auditor should also consider whether any other information, irrespective of specified control objectives, has come to his or her attention that causes him or her to conclude *(a)* that design deficiencies exist that could adversely affect the ability to record, process, summarize, or report financial data to user organizations without error, and *(b)* that user organizations would not generally be expected to have policies and procedures in place to mitigate such design deficiencies.

**33.** The description of policies and procedures and control objectives required for these reports may be prepared by the service organization. If the service auditor prepares the description of policies and procedures and control objectives, the representations in the description remain the responsibility of the service organization.

**34.** For the service auditor to express an opinion on whether the policies and procedures were suitably designed to achieve the specified control objectives, it is necessary that —

*a.* The service organization identify and appropriately describe such control objectives and the relevant policies and procedures.
*b.* The service auditor consider the linkage of the policies and procedures to the stated control objectives.
*c.* The service auditor obtain sufficient evidence to reach an opinion.

**35.** The control objectives may be designated by the service organization or by outside parties such as regulatory authorities, a user group, or others. When the control objectives are not established by outside parties, the service auditor should be satisfied that the control objectives, as set forth by the service organization, are reasonable in the circumstances and consistent with the service organization's contractual obligations.

**36.** The service auditor's report should state whether the policies and procedures were suitably designed to achieve the specified control objec-

tives. The report should not state whether they were suitably designed to achieve objectives beyond the specifically identified control objectives.

**37.** The service auditor's opinion on whether the policies and procedures were suitably designed to achieve the specified control objectives is not intended to provide evidence of operating effectiveness or to provide the user auditor with a basis for concluding that control risk may be assessed below the maximum.

**38.** The following is a sample report on policies and procedures placed in operation at a service organization. The report should have, as an attachment, a description of the service organization's policies and procedures that may be relevant to a user organization's internal control structure. This report is illustrative only and should be modified as appropriate to suit the circumstances of individual engagements.

To XYZ Service Organization:

We have examined the accompanying description of the _____ application of XYZ Service Organization. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of XYZ Service Organization's policies and procedures that may be relevant to a user organization's internal control structure, (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if those policies and procedures were complied with satisfactorily,[2] and (3) such policies and procedures had been placed in operation as of _____. The control objectives were specified by _____. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

We did not perform procedures to determine the operating effectiveness of policies and procedures for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of XYZ Service Organization's policies and procedures, individually or in the aggregate.

In our opinion, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's policies and procedures that had been placed in operation as of _____. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily.

2. If the application of internal control structure policies and procedures by user organizations is necessary to achieve the stated control objectives, the service auditor's report should be modified to include the phrase "and user organizations applied the internal control structure policies and procedures contemplated in the design of XYZ Service Organization's policies and procedures" following the words "complied with satisfactorily" in the scope and opinion paragraphs.

> The description of policies and procedures at XYZ Service Organization is as of _____ and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specific policies and procedures at the Service Organization is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.
>
> This report is intended solely for use by the management of XYZ Service Organization, its customers, and the independent auditors of its customers.

**39.** If the service auditor concludes that the description is inaccurate or insufficiently complete for user auditors, the service auditor should so state in an explanatory paragraph preceding the opinion paragraph. An example of such an explanatory paragraph follows:

> The accompanying description states that XYZ Service Organization uses operator identification numbers and passwords to prevent unauthorized access to the system. Based on inquiries of staff personnel and inspections of activities, we determined that such procedures are employed in Applications A and B but are not required to access the system in Applications C and D.

In addition, the first sentence of the opinion paragraph would be modified to read as follows:

> In our opinion, except for the matter referred to in the preceding paragraph, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's policies and procedures that had been placed in operation as of _____.

**40.** If, after applying the criteria in paragraph 32, the service auditor concludes that there are significant deficiencies in the design or operation of the service organization's policies and procedures, the service auditor should report those conditions in an explanatory paragraph preceding the opinion paragraph. An example of an explanatory paragraph describing a significant deficiency in the design or operation of the service organization's policies and procedures follows:

> As discussed in the accompanying description, from time to time the Service Organization makes changes in application programs to correct deficiencies or to enhance capabilities. The procedures followed in determining whether to make changes, in designing the changes, and in implementing them do not include review and approval by authorized individuals who are independent from those involved in making the changes. There are also no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes.

In addition, the second sentence of the opinion paragraph would be modified to read as follows:

Also in our opinion, except for the deficiency referred to in the preceding paragraph, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily.

## Reports on Policies and Procedures Placed in Operation and Tests of Operating Effectiveness

*Paragraphs 41 through 56 repeat some of the information contained in paragraphs 25 through 40 to provide readers with a comprehensive, standalone presentation of the relevant considerations for each type of report.*

**41.** The information necessary for a report on policies and procedures placed in operation and tests of operating effectiveness ordinarily is obtained through discussions with appropriate service organization personnel, through reference to various forms of documentation, such as system flowcharts and narratives, and through the performance of tests of controls. Evidence of whether policies and procedures have been placed in operation is ordinarily obtained through previous experience with the service organization and through procedures such as inquiry of appropriate management, supervisory, and staff personnel; inspection of service organization documents and records; and observation of service organization activities and operations. The service auditor applies tests of controls to determine whether specified policies and procedures are operating with sufficient effectiveness to achieve specified control objectives. SAS No. 39, *Audit Sampling* (AICPA, *Professional Standards,* vol. 1, AU sec. 350), provides guidance on the application and evaluation of audit sampling in performing tests of controls.

**42.** After obtaining a description of the relevant policies and procedures, the service auditor should determine whether the description provides sufficient information for user auditors to obtain an understanding of the aspects of the service organization's policies and procedures that may be relevant to a user organization's internal control structure. The description should contain a discussion of the features of the service organization's policies and procedures that would have an effect on a user organization's internal control structure. Such features are relevant when they directly affect the service provided to the user organization. They may include features generally considered to be part of the control environment, specific activities that may represent a user organization's accounting system or a portion thereof, or specific policies and procedures designed to control such functions. Control environment elements may include hiring practices and the involvement of internal auditors. Accounting system elements would include the ways in which user transactions are initiated and processed. Control structure policies and procedures employed by a service organization, such as policies and procedures over the modification of computer programs, ordinarily are designed to meet specific control objec-

tives. The specific control objectives of the service organization should be set forth in the service organization's description of policies and procedures.

**43.** The service auditor should inquire about changes in the service organization's policies and procedures that may have occurred before the beginning of fieldwork. If the service auditor believes the changes would be considered significant by user organizations and their auditors, those changes should be included in the description of the service organization's policies and procedures. If the service auditor concludes that the changes would be considered significant by user organizations and their auditors and the changes are not included in the description of the service organization's policies and procedures, the service auditor should describe the changes in his or her report. Such changes might include —

- Procedural changes made to accommodate provisions of a new FASB Statement of Financial Accounting Standards.
- Major changes in an application to permit on-line processing.
- Procedural changes to eliminate previously identified deficiencies.

Changes that occurred more than twelve months before the date being reported on normally would not be considered significant, because they generally would not affect user auditors' considerations.

**44.** A service auditor's report expressing an opinion on a description of policies and procedures placed in operation at a service organization and tests of operating effectiveness should contain —

*a.* A specific reference to the applications, services, products, or other aspects of the service organization covered.
*b.* A description of the scope and nature of the service auditor's procedures.
*c.* Identification of the party specifying the control objectives.
*d.* An indication that the purpose of the service auditor's engagement was to obtain reasonable assurance about whether (1) the service organization's description presents fairly, in all material respects, the aspects of the service organization's policies and procedures that may be relevant to a user organization's internal control structure, (2) the policies and procedures were suitably designed to achieve specified control objectives, and (3) such policies and procedures had been placed in operation as of a specific date.
*e.* The service auditor's opinion on whether the description presents fairly, in all material respects, the relevant aspects of the service organization's policies and procedures that had been placed in operation as of a specific date and whether, in the service auditor's opinion, the policies and procedures were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those policies and procedures were complied with satisfactorily.

*f.* A reference to a description of tests of specified service organization policies and procedures designed to obtain evidence about the operating effectiveness of those policies and procedures in achieving specified control objectives. The description should include the policies and procedures that were tested, the control objectives the policies and procedures were intended to achieve, the tests applied, and the results of the tests. The description should include an indication of the nature, timing, and extent of the tests, as well as sufficient detail to enable user auditors to determine the effect of such tests on user auditors' assessments of control risk. To the extent that the service auditor identified causative factors for exceptions, determined the current status of corrective actions, or obtained other relevant qualitative information about exceptions noted, such information should be provided.

*g.* A statement of the period covered by the service auditor's report on the operating effectiveness of the specified policies and procedures.

*h.* The service auditor's opinion on whether the policies and procedures 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.

*i.* When all of the control objectives listed in the description of policies and procedures placed in operation are not covered by tests of operating effectiveness, a statement that the service auditor does not express an opinion on control objectives not listed in the description of tests performed at the service organization.

*j.* A statement that the relative effectiveness and significance of specific service organization policies and procedures and their effect on assessments of control risk at user organizations are dependent on their interaction with the policies, procedures, and other factors present at individual user organizations.

*k.* A statement that the service auditor has performed no procedures to evaluate the effectiveness of policies and procedures at individual user organizations.

*l.* A statement of the inherent limitations of the potential effectiveness of policies and procedures at the service organization and of the risk of projecting to the future any evaluation of the description or any conclusions about the effectiveness of policies and procedures in achieving control objectives.

*m.* Identification of the parties for whom the report is intended.

**45.** If the service auditor believes that the description is inaccurate or insufficiently complete for user auditors, the service auditor's report should so state and should contain sufficient detail to provide user auditors with an appropriate understanding.

**46.** It may become evident to the service auditor, when considering the service organization's description of policies and procedures placed in

operation, that the system was designed with the assumption that certain internal control structure policies and procedures would be implemented by the user organization. If the service auditor is aware of the need for such complementary user organization internal control structure policies and procedures, these should be delineated in the description of policies and procedures. If the application of internal control structure policies and procedures by user organizations is necessary to achieve the stated control objectives, the service auditor's report should be modified to include the phrase "and user organizations applied the internal control structure policies and procedures contemplated in the design of the Service Organization's policies and procedures" following the words "complied with satisfactorily" in the scope and opinion paragraphs. Similarly, if the operating effectiveness of policies and procedures at the service organization is dependent on the application of policies and procedures at user organizations, this should be delineated in the description of tests performed.

**47.** The service auditor should consider conditions that come to his or her attention that, in the service auditor's judgment, represent significant deficiencies in the design or operation of the service organization's policies and procedures that preclude the service auditor from obtaining reasonable assurance that specified control objectives would be achieved. The service auditor should also consider whether any other information, irrespective of specified control objectives, has come to his or her attention that causes him or her to conclude *(a)* that design deficiencies exist that could adversely affect the ability to record, process, summarize, or report financial data to user organizations without error, and *(b)* that user organizations would not generally be expected to have policies and procedures in place to mitigate such design deficiencies.

**48.** The description of policies and procedures and control objectives required for these reports may be prepared by the service organization. If the service auditor prepares the description of policies and procedures and control objectives, the representations in the description remain the responsibility of the service organization.

**49.** For the service auditor to express an opinion on whether the policies and procedures were suitably designed to achieve the specified control objectives, it is necessary that —

*a.* The service organization identify and appropriately describe such control objectives and the relevant policies and procedures.
*b.* The service auditor consider the linkage of the policies and procedures to the stated control objectives.
*c.* The service auditor obtain sufficient evidence to reach an opinion.

**50.** The control objectives may be designated by the service organization or by outside parties such as regulatory authorities, a user group, or others. When the control objectives are not established by outside parties,

the service auditor should be satisfied that the control objectives, as set forth by the service organization, are reasonable in the circumstances and consistent with the service organization's contractual obligations.

**51.** The service auditor's report should state whether the policies and procedures were suitably designed to achieve the specified control objectives. The report should not state whether they were suitably designed to achieve objectives beyond the specifically identified control objectives.

**52.** The service auditor's opinion on whether the policies and procedures were suitably designed to achieve the specified control objectives is not intended to provide evidence of operating effectiveness or to provide the user auditor with a basis for concluding that control risk may be assessed below the maximum. Evidence that may enable the user auditor to conclude that control risk may be assessed below the maximum may be obtained from the results of specific tests of operating effectiveness.

**53.** The management of the service organization specifies whether all or selected applications and control objectives will be covered by the tests of operating effectiveness. The service auditor determines which policies and procedures are, in his or her judgment, necessary to achieve the control objectives specified by management. The service auditor then determines the nature, timing, and extent of the tests of controls needed to evaluate operating effectiveness. Testing should be applied to policies and procedures in effect throughout the period covered by the report. To be useful to user auditors, the report should ordinarily cover a minimum reporting period of six months.

**54.** The following is a sample report on policies and procedures placed in operation at a service organization and tests of operating effectiveness. It should be assumed that the report has two attachments: *(a)* a description of the service organization's policies and procedures that may be relevant to a user organization's internal control structure and *(b)* a description of policies and procedures for which tests of operating effectiveness were performed, the control objectives the policies and procedures were intended to achieve, the tests applied, and the results of those tests. This report is illustrative only and should be modified as appropriate to suit the circumstances of individual engagements.

To XYZ Service Organization:

We have examined the accompanying description of the _____ application of XYZ Service Organization. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of XYZ Service Organization's policies and procedures that may be relevant to a user organization's internal control structure, (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if those policies and proce-

dures were complied with satisfactorily,[3] and (3) such policies and procedures had been placed in operation as of _____. The control objectives were specified by _____. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's policies and procedures that had been placed in operation as of _____. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific policies and procedures, listed in Schedule X, to obtain evidence about their effectiveness in meeting the control objectives, described in Schedule X, during the period from _____to _____. The specific policies and procedures and the nature, timing, extent, and results of the tests are listed in Schedule X. This information has been provided to user organizations of XYZ Service Organization and to their auditors to be taken into consideration, along with information about the internal control structure at user organizations, when making assessments of control risk for user organizations. In our opinion the policies and procedures that were tested, as described in Schedule X, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Schedule X were achieved during the period from _____ to _____. [However, the scope of our engagement did not include tests to determine whether control objectives not listed in Schedule X were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Schedule X.][4]

The relative effectiveness and significance of specific policies and procedures at XYZ Service Organization and their effect on assessments of control risk at user organizations are dependent on their interaction with the policies, procedures, and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of policies and procedures at individual user organizations.

---

3. If the application of internal control structure policies and procedures by user organizations is necessary to achieve the stated control objectives, the service auditor's report should be modified to include the phrase "and user organizations applied the internal control structure policies and procedures contemplated in the design of XYZ Service Organization's policies and procedures" following the words "complied with satisfactorily" in the scope and opinion paragraphs.

4. This sentence should be added when all of the control objectives listed in the description of policies and procedures placed in operation are not covered by the tests of operating effectiveness. This sentence would be omitted when all of the control objectives listed in the description of policies and procedures placed in operation are included in the tests of operating effectiveness.

> The description of policies and procedures at XYZ Service Organization is as of _____, and information about tests of the operating effectiveness of specified policies and procedures covers the period from _____ to _____. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specified policies and procedures at the Service Organization is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.
>
> This report is intended solely for use by the management of XYZ Service Organization, its customers, and the independent auditors of its customers.

**55.** If the service auditor concludes that the description is inaccurate or insufficiently complete for user auditors, the service auditor should so state in an explanatory paragraph preceding the opinion paragraph. An example of such an explanatory paragraph follows:

> The accompanying description states that XYZ Service Organization uses operator identification numbers and passwords to prevent unauthorized access to the system. Based on inquiries of staff personnel and inspection of activities, we determined that such procedures are employed in Applications A and B but are not required to access the system in Applications C and D.

In addition, the first sentence of the opinion paragraph would be modified to read as follows:

> In our opinion, except for the matter referred to in the preceding paragraph, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's policies and procedures that had been placed in operation as of _____.

**56.** If, after applying the criteria in paragraph 47, the service auditor concludes that there are significant deficiencies in the design or operation of the service organization's policies and procedures, the service auditor should report those conditions in an explanatory paragraph preceding the opinion paragraph. An example of an explanatory paragraph describing a significant deficiency in the design or operation of the service organization's policies and procedures follows:

> As discussed in the accompanying description, from time to time the Service Organization makes changes in application programs to correct deficiencies or to enhance capabilities. The procedures followed in determining whether to make changes, in designing the changes, and in implementing them do not include review and approval by authorized individuals who are independent from those involved in making the changes. There are also no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes.

In addition, the second sentence of the opinion paragraph would be modified to read as follows:

> Also in our opinion, except for the deficiency referred to in the preceding paragraph, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the related control objectives would be achieved if the described policies and procedures were complied with satisfactorily.

## Written Representations of the Service Organization's Management

**57.** Regardless of the type of report issued, the service auditor should obtain written representations from the service organization's management that —

- Acknowledge management's responsibility for establishing and maintaining appropriate policies and procedures relating to the processing of transactions for user organizations.
- Acknowledge the appropriateness of the specified control objectives.
- State that the description of policies and procedures presents fairly, in all material respects, the aspects of the service organization's policies and procedures that may be relevant to a user organization's internal control structure.
- State that the policies and procedures, as described, had been placed in operation as of a specified date.
- State that management believes its policies and procedures were suitably designed to achieve the specified control objectives.
- State that management has disclosed to the service auditor any significant changes in policies and procedures that have occurred since the service organization's last examination.
- State that management has disclosed to the service auditor any illegal acts, irregularities, or uncorrected errors attributable to the service organization's management or employees that may affect one or more user organizations.
- State that management has disclosed to the service auditor all design deficiencies in policies and procedures of which it is aware, including those for which management believes the cost of corrective action may exceed the benefits.

If the scope of the work includes tests of operating effectiveness, the service auditor should obtain a written representation from the service organization's management stating that management has disclosed to the service auditor all instances, of which it is aware, when policies and procedures have not operated with sufficient effectiveness to achieve the specified control objectives.

## Reporting on Substantive Procedures

**58.** The service auditor may be requested to apply substantive procedures to user transactions or assets at the service organization. In such circumstances, the service auditor may make specific reference in his or her report to having carried out the designated procedures or may provide a separate report in accordance with SAS No. 35, *Special Reports—Applying Agreed-Upon Procedures to Specified Elements, Accounts, or Items of a Financial Statement* (AICPA, *Professional Standards,* vol. 1, AU sec. 622). Either form of reporting should include a description of the nature, timing, extent, and results of the procedures in sufficient detail to be useful to user auditors in deciding whether to use the results as evidence to support their opinions.

## EFFECTIVE DATE

**59.** This Statement is effective for service auditors' reports dated after March 31, 1993. Earlier application of this Statement is encouraged.