AICPA®

Information for management of a service organization in a SOC 1® engagement

Information for Management of a Service Organization in a SOC 1® Engagement

This document was prepared by the Service Organizations Task Force of the American Institute of Certified Public Accountants.

Service Organizations Task Force

David L. Palmer, *Chair*
Robert F. Dacey
Anthony M. Graziano
Chris K. Halterman
Craig P. Linnell
James R. Merrill
Kirt Seale
Sheryl K. Skolnik
Julie Winger

AICPA Staff

Robert Dohrer
Chief Auditor

Judith M. Sherinsky
Senior Technical Manager
Audit and Attest Standards

Table of Contents

Paragraph

Executive Summary

Preface **1–11**
Introduction and Purpose 1–5
Summary of Management's Responsibilities in a SOC 1® Engagement 6
Overview of SOC 1® Engagements 7–8
Types of Service Organizations 9
Identifying and Assessing Risks When a User Entity Outsources Services to a Service Organization 10–11

Planning a SOC 1® Engagement **12–103**
Defining the Scope of the Engagement 13
Determining Whether a Type 1 or Type 2 Engagement Will Be Performed 14–16
Determining the Period to Be Covered by the Report 17–21
Selecting the Criteria to Be Used 22–26
Criteria for Management's Description of the Service Organization's System 23
Criteria for the Suitability of the Design of Controls 24
Criteria for the Operating Effectiveness of Controls 25
Additional Criteria 26
Specifying the Control Objectives 27–49
Control Objectives and Assertions in User Entities' Financial Statements 27–28
Assertions in User Entities' Financial Statements 29–30
Attributes of Control Objectives That Are Reasonable in the Circumstances 31–40
IT General Control Objectives and Related Risks 41–43
Control Objectives Specified by Law, Regulation, or an Outside Party 44–49
Identifying Subservice Organizations and Determining Whether Subservice Organizations Will Be Carved Out or Included in the Description of the Service Organization's System 50–59
Determining if an Entity is a Subservice Organization 50–54
Determining Whether Subservice Organizations Will Be Carved Out or Included in the Description 55–56
Factors for Service Organization Management to Consider in Determining Whether Services Provided by a Subservice Organization Should Be Presented Using the Carve-Out or Inclusive Method 57–59
Preparing the Description of the Service Organization's System 60–101
Method of Presentation of the Description 61–63
Completeness and Accuracy of the Description 64–65
Other Information 66–67
Content of the Description 68–101
Types of Services Provided, Procedures to Provide Services,

Information Used to Provide Services, Process Used to Prepare Reports, and Significant Events ... 69–72
Control Environment, Risk Assessment Process, Information and Communications and Monitoring Activities ... 73–74
Consideration of the 2013 COSO Framework ... 75–76
Presenting Specified Control Objectives and Controls Designed to Achieve Those Objectives ... 77–78
Complementary User Entity Controls ... 79–81
Content of the Description When the Service Organization Uses the Carve-Out Method ... 82
Complementary Subservice Organization Controls ... 83–86
Examples of Complementary Subservice Organization Controls (CSOCs) ... 87
Monitoring the Subservice Organization ... 88–90
Content of the Description When the Service Organization Uses the Inclusive Method ... 91–100
Changes to the System During the Period ... 101
New Reports Versus Recurring Reports ... 102–103

Evaluation ... 104–141
Coordination With the Service Auditor ... 104–114
Determining Whether Internal Auditors Will Assist the Service Auditor and Whether the Service Auditor Will Use the Work of the Internal Audit Function ... 108
Management's Considerations ... 109
Use of Direct Assistance ... 110–111
Using the Work of Internal Audit ... 112–114
Preparing Management's Assertion ... 115–125
Establishing a Basis for Management's Assertion ... 126–141
Illustrative Approach to the Risk Assessment Process ... 130–141

Reporting ... 142–153
Finalizing Management's Description and Assertion ... 142–146
Reading and Understanding the Service Auditor's Report ... 147
Preparing Written Representations ... 148–153

Appendix A: Illustrative Outline for a Description of the Service Organization's System ... 154

Appendix B: Illustrative Assertion by Management of a Service Organization for a Type 2 Report ... 155

Appendix C: Financial Statement Assertions and Risks That Threaten the Achievement of the Service Organization's

Control Objectives 156
Table 1: Types of Financial Statement Assertions About Classes of Transactions and Events During a Period, Related Service Organization Control Objectives, and Risks That Threaten the Achievement of the Control Objectives

Table 2. Types of Financial Statement Assertions About Account Balances at the Period End, Related Service Organization Control Objectives, and Risks That Threaten the Achievement of the Control Objectives

Appendix D: Illustrative Control Objectives for Various Types of Service Organizations 157

Appendix E: IT General Control Objectives and Risks That Threaten the Achievement of the Control Objectives 158

Appendix F: Glossary 159

Information for Management of a Service Organization in a SOC 1® Engagement

Executive Summary

The AICPA prepared this guide to help management of a service organization understand its responsibilities in a SOC 1®[1] engagement. The guide is intended to be used as a reference document and contains illustrations and answers to questions frequently asked by management of a service organization. Although the guide may be read in its entirety, the authors believe it is most useful when used to research specific topics in conjunction with discussions with the service auditor.

In today's business environment, it is common for an entity to outsource certain functions to third parties. In such situations, the entity that provides the services is referred to as a *service organization* and the entity that outsources the functions is referred to as a *user entity* because that entity uses the services provided by the service organization.

The service organization provides the services, and the user entity uses the services of the service organization.

When a user entity outsources functions that affect its *internal control over financial reporting* (ICFR), management of the user entity needs to gain an understanding of the design and operating effectiveness of certain controls that are performed by the service organization. This is generally accomplished through a SOC 1®[2] engagement, which is an engagement performed by a CPA (a service auditor) to report on the service organization's description of its system, the suitability of the design of the service organization's controls included in the description, and, in a type 2 engagement, the operating effectiveness of those controls.

This guide is designed to help management of a service organization understand its responsibilities in a SOC 1® engagement and contains illustrations and answers to frequently asked questions so management can prepare for and facilitate the SOC 1® engagement.

[1] In 2017, the AICPA introduced the term *system and organization controls* (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization and system or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the AICPA enables the introduction of new internal control examinations that may be performed (*a*) for other types of organizations, in addition to service organizations, and (*b*) on either system-level or entity-level controls of such organizations.

[2] *SOC 1® — SOC for Service Organizations: ICFR*.

In a SOC 1® engagement, management's responsibilities may be grouped into the following three phases:

- **Planning**
- **Evaluation**
- **Reporting**

SOC 1® Phases
Reporting
Planning
Evaluation

Planning
During the planning phase, management will need to define and discuss with the service auditor the scope of the engagement. Some of the key elements of this phase include defining the period to be covered by the report (or the "as of date" in a type 1 engagement), specifying the control objectives, and preparing or updating the service organization's description of its system. To more fully understand its responsibilities and considerations during this phase, including understanding the different required components of the description, management should refer to paragraphs 12–103 of this guide.

Evaluation
During the second phase, the evaluation phase, management is responsible for preparing and establishing a basis for its assertion and coordinating testing with the service auditor. This phase includes managing the interaction of the service auditor with service organization personnel (including internal audit), preparing management's assertion, establishing a basis for management's assertion, and providing evidence of the design and operating effectiveness of controls to the service auditor. This phase may occur over a period of time, sometimes several months. Paragraphs 104–141 provide guidance on management's responsibilities during the evaluation phase.

Reporting
In the final phase of a SOC 1® engagement, the reporting phase, management is responsible for finalizing its assertion; understanding the effect of issues (for example, control deficiencies) that may have been identified during the engagement; reading and understanding the service auditor's report; and providing a letter of representations to the service auditor. Paragraphs 142–153 provide guidance for management to appropriately close out the SOC 1® engagement and begin planning for the next cycle.

Preface

Introduction and Purpose

1. The outsourcing of tasks or functions to service providers continues to evolve as entities look for ways to reduce costs and streamline operations. However, outsourcing also presents risks and challenges for management of a user entity because, even though a task or function is outsourced, management retains ultimate responsibility for managing these risks. To meet those responsibilities, management needs to monitor the services provided by the service provider and may need assurance that the controls at the service provider that affect the services it uses are operating effectively. (Appendix F contains a glossary that defines certain terms used in this guide.)

2. This publication, *Information for Management of a Service Organization in a SOC 1® Engagement*, is intended to assist management of a service organization in understanding its responsibilities in a SOC 1® engagement. The advantage of having this information prior to beginning the SOC 1® engagement is that it enables management to identify the various tasks that must be completed to successfully undergo a SOC 1® engagement, for example, determining whether the description of the service organization's system includes all the components that should be included.

3. An effective way for management of a user entity to address the outsourcing-related risks that are relevant to the user entity's ICFR is to request that the service organization provide a SOC 1® report.

4. SOC 1® reports address controls at a service organization that are likely to be relevant to a user entity's ICFR. Such controls may address the following:

- Information processed by the service organization for user entities and incorporated in the user entities' financial statements, such as amounts paid for medical claims when a service organization processes claims for a user entity
- The user entities' financial statement assertions about existence and ownership, for example, a financial institution that maintains custody of securities for user entities
- The information technology general computing controls supporting transaction processing relevant to a user entity's financial statements, such as a hosting organization that performs access administration and system maintenance for user entities

5. The other commonly used service auditor's report is a SOC 2® report, which is intended to meet the needs of a broad range of users who need information and assurance about controls at a service organization that affect security, availability, or processing integrity of the systems that the service organization uses to process users' data, or the confidentiality or privacy of the information processed by these systems. Examples of stakeholders who may need a SOC 2® report are customers or suppliers of the service organization, regulators, or business partners. Although these reports do not provide an opinion on controls at a service organization relevant to user entities' ICFR, these reports can play an important role in the following:

- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory compliance

Summary of Management’s Responsibilities in a SOC 1® Engagement

6. The following is a summary of management’s responsibilities in a SOC 1® engagement, presented in the order of the phases of the engagement. Next to each item are the paragraphs in this guide where that topic is discussed in greater detail.

Planning

- Defining the scope of the engagement (par. 13)
- Determining the type of engagement to be performed (par. 14–16):
  - *Type 2 engagement.* Covers the suitability of the design and operating effectiveness of controls over a period of time (This is the type of engagement that is usually performed.)
  - *Type 1 engagement.* Covers the suitability of the design of controls only as of a specific date (This type of engagement is performed very infrequently.)
- Determining the period to be covered by the SOC 1® engagement (par. 17–21):
  - Assuming it is a type 2 engagement, the period during which controls will be assessed (for example, a 12-month or 6-month period)
  - Generally, reports are most useful to user entities[3] and their auditors when they cover a substantial portion of the period covered by the user entities’ financial statements being audited. In some cases, multiple reports are issued during a calendar year (for example, semiannually or quarterly, depending on the fiscal year-end of the user entities).
- Selecting the criteria to be used to assess the controls:
  - The criteria are used to evaluate whether the description of the service organization’s system is fairly presented and whether the controls are suitably designed and operating effectively (par. 22–26).
- Specifying the control objectives and controls (par. 27–49):

[3] Controls at the service organization are likely to be relevant to a user entity’s internal control over financial reporting.

- Identify the control objectives that are relevant to users of the service organization's SOC 1® report and their auditors and the controls that are designed and implemented to achieve the control objectives.

- A *control objective* is the aim or purpose of specified controls at a service organization. Control objectives should address the risks that controls are intended to mitigate.

- Control objectives should have each of the following attributes:

    - *Relevance*. Control objectives are relevant to the types of assertions commonly embodied in the broad range of user entities' financial statements to which controls at the service organization could reasonably be expected to relate.
    - *Objectivity*. Control objectives are free from bias.
    - *Measurability*. Control objectives permit reasonably consistent measurements — qualitative or quantitative — of the design and operating effectiveness of service organization controls.
    - *Completeness*. Control objectives are complete when they do not omit relevant factors that could reasonably be expected to affect decisions of the intended users made based on the control objectives.

See paragraphs 41–42 and appendixes C, D, and E for illustrative control objectives, related assertions in users' financial statements, and risks.

- Identifying subservice organizations (par. 50–54):
    - *A subservice organization* is an entity that provides services to a service organization that are relevant to user entities' ICFR.
    - The service organization identifies subservice organizations that are used to process user information.
- Determining whether subservice organizations will be carved out or included in the description (par. 55–59):

    - *Carved out.* Subservice organization controls will not be included in the service organization's description of the system.
    - *Included.* Subservice organization controls will be included in the service organization's description of the system and covered by the service auditor's report (requires coordination with the subservice organization).

- Assigning or confirming responsibilities of service organization personnel for preparation of the description of the service organization's system and coordination and communication with the service auditor (par. 60).

- Determining whether members of the service organization's internal audit function will assist the service auditor in performing certain tasks under the supervision of the service auditor and whether the service auditor will use work independently performed by the internal audit function to obtain evidence (for example, evaluations performed by the internal audit function as part of its assessment of the effectiveness of controls) (par. 112–114).

- Preparing the description of the service organization's system, which includes the following (par. 60–103):
  - Services provided, procedures by which services are provided, and information used in performing the procedures
  - Services performed by subservice organizations and their relevance to the control objectives identified by management
  - Control objectives and controls designed to achieve those objectives, including complementary user entity and subservice organization controls
  - Other relevant aspects of the service organization's system of internal control

Evaluation

- Coordinating with the service auditor. Examples include service organization personnel (including internal audit) (par. 104–114)

  - facilitating the auditor's testing, including walk-throughs of the service organization's processes;
  - providing the service auditor with evidence of the design and operating effectiveness of controls; and
  - providing the service auditor with the results of testing performed by internal audit.
- Preparing management's assertion, which includes management's assessment of the (par. 115–125)

  - fairness of the presentation of the description in relation to the criteria;
  - suitability of the design of the controls; and
  - operating effectiveness of the controls.
- Establishing a basis for management's assertion (par. 126–141).

Reporting

- Finalizing management's description and assertion (par. 142–146).
- Reading and understanding the service auditor's report (par. 147).
- Providing the service auditor with a letter of representations (par. 148–153).

Overview of SOC 1® Engagements

7. This guide is meant for management of an entity that provides services to other entities that may affect the other entities' financial statements. The entities that provide the services are referred to as *service organizations,* and the entities that use the services are referred to as *user entities*. This guide contains information for management of a service organization undergoing a SOC 1® engagement, which is an engagement performed by a CPA to report on the service organization's description of its system, suitability of the design of the service organization's controls included in the description, and (in a type 2 engagement) operating effectiveness of those controls.

8. A SOC 1® report addresses controls at a service organization are likely to affect user entities' financial statements (for example, controls at the service organization that affect the processing of data that will be incorporated in the user entities' financial statements). Financial statements are a form of financial reporting, so a SOC 1® engagement is said to address user entities' ICFR. This guide contains illustrations and answers to common questions from management of a service organization so that service organization management can prepare for and facilitate the SOC 1® engagement.

Types of Service Organizations

9. Many entities outsource aspects of their business or technology activities to service organizations that provide services ranging from performing a specific task under the direction of the entity to replacing entire business units or functions of the entity. The following are examples of service organizations that provide services that may be relevant to user entities' ICFR:

- *Health insurance claims processing companies.* When the medical claims processing function for a self-insured health plan is outsourced, the participants in the self-insured health plan are instructed to submit their claims directly to the medical claims processor. The medical claims processor provides claims data to the companies that have self-insured health plans. The self-insured companies use this data to record their claims expense and the related liability. That information flows through to the self-insured companies' financial statements. Controls at the claims processor will affect the quality of the data provided to the self-insured health plans. As such, the claims processor is a service organization to the self-insured health plan.

- *Custodians for investment companies.* Custodians for investment companies are responsible for the receipt, delivery, and safekeeping of an investment company's portfolio of securities; the receipt and disbursement of cash resulting from transactions in these securities; and the maintenance of records of the securities held for the investment company. The custodian may also perform other services for the investment company, such as collecting dividend and interest income and distributing that income to the investment company. The custodian is a service organization to the investment company.

- *Application service providers (ASPs).* ASPs provide packaged software applications and a technology environment that enables customers to process financial and operational transactions. An ASP may specialize in providing a particular software package solution to its users, may perform business processes for user entities that the user entities had traditionally performed themselves, or may provide some combination of these services. As such, an ASP may be a service organization if it provides services that are part of the user entity's information system relevant to its ICFR.

- *Cloud service provider*. Organizations providing cloud-based services deliver computing services over the internet (cloud), enabling on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released. The typical types of cloud computing service models include: software as a service, platform as a service, and infrastructure as a service. A cloud-based service provider implements certain controls over the functions performed, typically IT general controls (logical access, change management, and computer operations), to maintain data in a secure manner and provide computing services that support processing. Therefore, the cloud service provider may be a service organization for entities that use cloud-based services that are relevant to its ICFR.

Identifying and Assessing Risks When a User Entity Outsources Services to a Service Organization

10. One of the critical roles of management and those charged with governance in any entity is to identify and assess risks to the entity and address such risks through effective internal control. When an entity outsources tasks or functions to a service organization and becomes a user entity, it shifts some of the risks associated with performing those tasks or functions to risks associated with outsourcing, particularly risks related to how the service organization performs the tasks or functions and how that may affect the user entity's ICFR. However, even though a task or function is outsourced, management of the user entity retains the ultimate responsibility for managing these risks and needs to monitor the services provided by the service organization.

11. A user entity's need for a SOC 1® report depends on whether controls at the service organization have a significant effect on assertions in the user entities'financial statements to which controls at the service organization could reasonably be expected to relate. Services provided by a service organization are relevant to the audit of a user entity's financial statements when those services and the controls over them affect the user entity's information system, including related business processes relevant to financial reporting. As described in AICPA professional standards, a service organization's services are part of a user entity's information system relevant to financial reporting if these services affect any of the following:

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

b. The procedures within both IT and manual systems, by which the user entity's transactions are initiated, authorized, recorded, processed, corrected as necessary, transferred to the general ledger, and reported in the financial statements *c*. The related accounting records, supporting information, and specific accounts in the user entity's financial statements that are used to initiate, authorize, record, process, and report the user entity's transactions (This includes the correction of incorrect information and how information is transferred to the general ledger. The records may be in either manual or electronic form.)

d. How the user entity's information system captures events and conditions, other than transactions, that are significant to the financial statements

e. The financial reporting process used to prepare the user entity's financial statements, including significant accounting estimates and disclosures

f. Controls surrounding journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments

Planning

Planning a SOC 1® Engagement

12. In the planning phase of a SOC 1® engagement, management is responsible for the following: (See the identified paragraphs for additional detail about these responsibilities.)

- Defining the scope of the engagement (par. 13)
- Determining the type of engagement to be performed (a type 1 or type 2 engagement) (par. 14–16)
- Determining the period to be covered by the report or, in the case of a type 1 report, the specified "as of" date of the report (par. 17–21)
- Selecting the criteria to be used and determining that the criteria are appropriate for management's purposes (par. 22–26)
- Specifying the control objectives (par. 27–49)
- Identifying subservice organizations and determining whether subservice organizations will be carved out or included in the description of the service organization's system (par. 50–59)
- Preparing the description of the service organization's system and marshaling resources to do that (par. 60–103)

Defining the Scope of the Engagement

13. In defining the scope of a SOC 1® engagement, management considers which services (including the classes of transactions processed), functions performed, business units, functional areas, or applications are likely to be relevant to user entities' ICFR. In the case of a recurring or existing engagement, the prior report provides a useful starting point for defining the scope of the engagement. In general, the scope will be identified in management's description of the service organization's system.

Determining Whether a Type 1 or Type 2 Engagement Will Be Performed

14. Management is responsible for determining whether the SOC 1® engagement will be a type 1 or type 2 engagement. The following is a brief description of what the service auditor's opinion addresses in the CPA's reports resulting from each of these engagements:

- *Type 1 report.* A report in which the service auditor expresses an opinion on whether management's description of the service organization's system is fairly presented, and the controls included in the description are suitability designed as of a specified date
- *Type 2 report.* A report in which the service auditor expresses an opinion on whether management's description of the service organization's system is fairly presented, and the controls included in the description are suitability designed and operating effectively for a period of time (This report also includes a detailed description of the tests of controls performed by the service auditor and the results of those tests.)

15. Because auditors of user entities' financial statements (user auditors) may need evidence of the operating effectiveness of controls at a service organization, a service organization generally will choose to provide its user entities with a type 2 report rather than a type 1 report. If a type 2 report is not available, a greater likelihood exists that user auditors will visit the service organization to perform their own tests or will request that another CPA perform such tests, likely increasing the demands placed on management and others at the service organization. In a type 1 engagement, the service auditor does not obtain assurance that the control objectives stated in management's description of the service organization's system were achieved because the service auditor's objective in a type 1 engagement does not include obtaining evidence about the operating effectiveness of controls.

16. Typically, a type 1 engagement may be appropriate in either of the following instances:

- User entities can exercise effective user entity controls over the services performed by the service organization.
- The service organization is issuing a report on controls at the service organization for the first time and the service auditor is unable to perform the procedures necessary to issue a type 2 report.

Determining the Period to Be Covered by the Report

17. Management is also responsible for determining the period to be covered by the report (or in the case of a type 1 report, the specified as of date). Generally, type 2 reports are most useful to user entities and their auditors when they cover a substantial portion of the period covered by the user entity's financial statements being audited, for example, a report or reports that cover at least nine months of the period covered by the audit of the user entity's financial statements. To increase the likelihood that the report will be useful to user entities and their auditors, management may wish to determine the financial reporting period of the user entities so that management can select a period or periods that correspond with the financial reporting period of the majority of its user entities.

18. If the various user entities have differing fiscal year-ends, in determining the appropriate period to be covered by the type 2 report, management and the service auditor may wish to discuss strategies for identifying reporting periods that best meet the needs of user entities. A service organization may better meet the needs of its user entities if it provides more frequent type 2 reports. For example, a service organization might provide semiannual reports that cover either contiguous 6- or 12-month periods.

19. In some situations, a service organization may elect to have a gap between the periods covered by the service organization's SOC 1® reports. Management should discuss with the service auditor the potential implications of a gap between reports.

20. Certain circumstances, such as the following, may result in a situation in which a service organization is unable to provide a single type 2 report that covers a substantial portion of the period covered by its user entities' financial statements:

- The service auditor is engaged close to the date by which the report is needed and evidence of the operating effectiveness of controls cannot be obtained retroactively. For example, testing the control requires that the service auditor observe the control being performed.
- The service organization's system or controls have been in operation for less than a substantial portion of the period covered by the user entities' financial statements.
- Significant changes have been made to the controls and it is not practical to
    - — wait to issue a report until a substantial portion of the user entities' financial reporting periods has passed or
    - — issue a report that covers the system before and after the changes.
- The service organization is issuing a report on controls at the service organization for the first time.
- A new or modified law or regulation has an effective date that results in a report that covers a period that is less than a substantial portion of the period covered by the user entities' financial statements in the first year of the law or regulation's enactment.

21. When any of the circumstances in the preceding paragraph exist, management may decide to expand subsequent reporting periods to cover a substantial portion of the period covered by its user entities' financial statements.

Selecting the Criteria to Be Used

22. In a SOC 1® engagement, the criteria are the benchmarks used to measure or evaluate the fairness of the presentation of the description of the service organization's system, the suitability of the design of the controls included in the description, and in a type 2 engagement, the operating effectiveness of those controls. Management is responsible for selecting the criteria to be used in evaluating whether the description of the service organization's system is fairly presented, and whether the controls are suitably designed and operating effectively.

Criteria for Management's Description of the Service Organization's System

23. The following are the minimum criteria for preparing and evaluating whether a description of the service organization's system is fairly presented:

a. Management's description of the service organization's system presents how the service organization's system was designed and implemented, including the following information about the service organization's system, if applicable:

   i. The types of services provided, including, as appropriate, the classes of transactions processed.
   ii. The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities.
   iii. The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions. This includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
   iv. How the service organization's system captures and addresses significant events and conditions other than transactions (for example, depreciation and amortization of assets and changes in the recoverability of accounts receivable).
   v. The process used to prepare reports and other information for user entities, including processes for providing complete and accurate reports and other information.
   vi. Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
   vii. The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls (CSOCs) assumed in the design of the service organization's controls.
   viii. Other aspects of the service organization's control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b. In the case of a type 2 report, management's description of the service organization's system includes relevant details of changes to the service organization's system during the period covered by the description.

c. Management's description of the service organization's system does not omit or distort information relevant to the service organization's system, while acknowledging that management's description of the service organization's system is prepared to meet the common needs of a broad range of user entities and their user auditors, and may not, therefore, include every aspect of the service organization's system that each individual user entity and its user auditor may consider important in its own particular environment.

Criteria for the Suitability of the Design of Controls

24. The following are the minimum criteria for identifying and evaluating whether controls are suitably designed:

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

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

Criteria for the Operating Effectiveness of Controls

25. The minimum criteria for evaluating whether controls operated effectively to provide reasonable assurance that the control objectives stated in management's description of the service organization's system were achieved is whether the controls were consistently applied as designed throughout the specified period, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Additional Criteria

26. Additional criteria may be needed, for example, to meet a regulatory requirement (such as SEC Rule 206(4)-2, "Custody of Funds or Securities of Clients by Investment Advisers") or a customer requirement. Management may wish to consult with the service auditor about whether it is appropriate to include additional criteria in the SOC 1® report.

Specifying the Control Objectives

Control Objectives and Assertions in User Entities' Financial Statements

27. A control objective is the aim or purpose of specified controls at a service organization. Management is responsible for specifying control objectives that address the risks that controls are intended to mitigate. Control objectives assist the user auditor in determining how the service organization's controls affect the user entity's financial statement assertions. In determining the control objectives to be included in the description, management selects control objectives that relate to the types of assertions commonly embodied in the broad range of user entities' financial statements. Table 1, "Examples of Assertions in User Entities' Financial Statements and Related Service Organization Control Objectives," identifies some of the control objectives that may be specified by a service organization and the types of assertions in the user entities' financial statements to which they relate.

Table 1: Examples of Assertions in User Entities' Financial Statements and Related Service Organization Control Objectives

Assertions in User Entities' Financial Statements	**Service Organization's Control Objectives**
	Controls provide reasonable assurance that the following control objectives are achieved:
Existence	Recorded investment transactions are valid
Completeness	Investment purchases and sales are recorded completely, accurately, and on a timely basis
Valuation or allocation	Investment income is recorded accurately and timely
Rights and obligations	The service organization's records accurately reflect securities held by third parties, for example, depositories or subcustodians

28. To assist in developing control objectives, appendix D, *Illustrative Control Objectives for Various Types of Service Organizations*, contains typical control objectives related to the following:

- General business processes
- IT general controls
- Specific types of service organizations, including
  - — application service providers;
  - — claims processors;
  - — credit card payment processors;
  - — defined contribution plan recordkeepers;
  - — investment managers;
  - — payroll processors; and
  - — transfer agents
- Custodians subject to SEC Rule 206(4)-2, "Custody of Funds or Securities of Clients by Investment Advisers"

Assertions in User Entities' Financial Statements

29. A relevant matter in assessing the reasonableness of the control objectives is whether the control objectives relate to the types of assertions commonly embodied in a broad range of user entity financial statements to which controls at the service organization could reasonably be expected to relate (for example, assertions about existence and accuracy that are affected by access controls that prevent or detect unauthorized access to the system).

30. Table 1, "Types of Financial Statement Assertions About Classes of Transactions and Events During a Period, Related Service Organization Control Objectives, and Risks That

Threaten the Achievement of the Control Objectives," and table 2, "Types of Financial Statement Assertions About Account Balances at the Period End, Related Service Organization Control Objectives, and Risks That Threaten the Achievement of the Control Objectives" in appendix C present the types of assertions that may exist in a user entity's financial statements, illustrative service organization control objectives that relate to those types of assertions, and the risks that threaten the achievement of those control objectives. Because the control objectives in the table are illustrative, they would need to be tailored to the specific circumstances of the service organization.

Attributes of Control Objectives That Are Reasonable in the Circumstances

31. The control objectives stated in management's description of the service organization's system should be reasonable in the circumstances. Control objectives are reasonable in the circumstances when they relate to the types of assertions commonly embodied in the broad range of user entities' financial statements to which controls at the service organization could reasonably be expected to relate. For example, such assertions may include assertions about existence and accuracy that are affected by controls over transaction processing that prevent, or detect and correct, misstatements in user entities' financial statements.

32. There is not one set of control objectives that would be appropriate for all service organizations. The control objectives should be tailored to the specific services provided and the industry in which the service organization primarily operates (for example, financial services vs. government), to reflect control objectives that are likely to be relevant to controls over financial reporting at user entities of the specific service organization. Management may wish to discuss relevant user entity assertions and control objectives with service auditor and with user entities and their auditors.

33. Although management may be unable to determine how controls at a service organization specifically relate to the assertions embodied in individual user entities' financial statements, management considers matters such as the following when identifying the types of assertions to which the controls are likely to relate:

- The types of services provided by the service organization, including the classes of transactions processed
- The contents of reports and other information prepared for user entities
- The information used in the performance of procedures
- The types of significant events other than transactions (for example, depreciation and amortization of assets and changes in the recoverability of accounts receivable) that occur in providing the services
- Services performed by a subservice organization, if any
- The range of controls the service organization is responsible for implementing, including responsibilities established in contracts and agreements with user entities
- The risks to a user entity's ICFR arising from IT used or provided by the service organization

34. In a SOC 1® engagement, the control objectives serve as part of the criteria used for determining whether the controls are suitably designed and operating effectively. Suitable criteria related to control objectives have each of the following attributes, which are described in paragraphs 35–40 in more detail:

- *Relevance*. Control objectives are relevant to the types of assertions commonly embodied in the broad range of user entities' financial statements to which controls at the service organization could reasonably be expected to relate.
- *Objectivity*. Control objectives are free from bias.
- *Measurability*. Control objectives permit reasonably consistent measurements, qualitative or quantitative, of the design and operating effectiveness of service organization controls.
- *Completeness*. Control objectives are complete when they do not omit relevant factors that could reasonably be expected to affect decisions of the intended users made based on the control objectives.

Relevance

35. As noted previously, the control objectives should relate to the types of assertions commonly embodied in the broad range of user entities' financial statements to which controls at the service organization could reasonably be expected to relate (for example, assertions about existence and accuracy that are affected by controls over transaction processing that prevent or detect unauthorized transactions). Although management may be unable to determine how controls at a service organization specifically relate to the assertions embodied in individual user entities' financial statements, they should consider whether the control objectives are likely to be relevant to user entities of the service organization.

36. Control objectives that are not likely to be relevant to user entities' ICFR may be included in a separate section of the report that is not covered by the service auditor's report, such as a section entitled "Other Information Provided by the Service Organization." An example of such a control objective is one that addresses the service organization's business continuity and contingency planning. Such information generally is of interest to management of the user entities. Including such information in a separate section of the report provides the means for service organization management to communicate its plans related to business continuity and contingency planning. If the control objectives are relevant to the security, availability, processing integrity, confidentiality, or privacy of a system, management may consider undergoing a SOC 2® engagement. Paragraphs 67–66 address other information provided by the service organization.

Objectivity

37. Another characteristic of suitable criteria for control objectives is objectivity (the criteria are free from bias). If control objectives are drafted so that the results of evaluating the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls would always be positive for that service organization, the control objectives would not have the attribute of objectivity.

Measurability

38. Control objectives should be measurable, which means they permit reasonably consistent conclusions about whether the control objectives have been achieved. For example, the following control objective would not be measurable:

> Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is adequate.

This objective could be reworded as follows to meet the measurability attribute of suitable criteria:

> Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is limited to authorized personnel.

Another example of a control objective that is not measurable is the following:

> Controls provide reasonable assurance that logical security policies and procedures adhere to management's intentions.

User entities would have no way of knowing what management's intentions are, and management would have no basis for determining whether the control objective had been achieved. This control objective is worded in a manner that would not permit report users to arrive at reasonably similar conclusions about the achievement of the control objective and the wording of the control objective should be modified. Such a control objective could be reworded as follows:

> Controls provide reasonable assurance that logical access to programs, data, and computer resources relevant to user entities' ICFR is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

Completeness

39. Control objectives should be complete. As noted previously, although a complete set of control objectives can provide a broad range of user auditors with a framework to assess the effect of controls at the service organization on assertions commonly embodied in user entities' financial statements, the service organization may be unable to determine how controls at a service organization specifically relate to the assertions embodied in individual user entities' financial statements and cannot, therefore, determine whether control objectives are complete from the viewpoint of individual user entities or user auditors. It is the responsibility of individual user entities or user auditors to assess whether the service organization's description addresses the particular control objectives that are relevant to their needs. As part of the service auditor's evaluation of the description, the service auditor is responsible for identifying omissions in the control objectives; but it is management's responsibility to establish the control objectives.

40. Whether a set of control objectives is complete will depend on the services provided to the user entities. For example, consider a service organization that provides computer services primarily to user entities in the financial services industry. Its application software enables user entities to process savings, mortgage loan, consumer loan, commercial loan, and general ledger transactions. The following are illustrations of how management evaluates the completeness of the control objectives for this service organization.

> *Example 1*. Example Service Organization wants to provide its user entities with a type 2 report that addresses the savings application and the related underlying IT general controls, but the report does not address any of the other applications provided by Example Service Organization. In evaluating whether the control objectives are complete, management determines that most user entities use only the savings application. As such, the report contains a complete set of control objectives for user entities that use only the savings application.
>
> *Example 2*. Example Service Organization wants to include only those control objectives related to the savings application and excludes control objectives and controls that address the underlying IT general controls. The control objectives related to IT general controls should be included because of their relevance to user entities' ICFR. Consequently, the control objectives are not complete without IT general controls because IT general controls and the related control objectives are critical to the achievement of the control objectives relevant to the savings application and would be relevant to user entities that use the savings application.
>
> *Example 3*. Example Service Organization is considering a control objective that "Controls provide reasonable assurance that savings and withdrawal transactions received from user entities are recorded completely and accurately." This control objective does not address timeliness and no other control objective addresses timeliness. The control objectives would be incomplete without addressing timeliness because the timeliness with which transactions are recorded would be likely to be relevant to user entities' ICFR.

IT General Control Objectives and Related Risks

41. In addition, a service organization's control objectives would include IT general control objectives that are necessary to achieve the application control objectives (related to classes of transactions and events as well as account balances) and are therefore likely to be relevant to controls over financial reporting at user entities. IT general controls are assessed in relation to their effect on applications and data that are likely to be relevant to financial reporting at user entities. IT general control objectives and related controls are typically reported separately from application controls. Appendix E, "IT General Control Objectives and Risks That Threaten the Achievement of the Control Objectives," presents illustrative IT general control objectives and the risks that threaten their achievement.

42. The service organization's control objectives may also include other conditions that affect the effectiveness of application controls (related to classes of transactions, events, or account balances). For example, the effectiveness of application controls generally depends on the reliability of master data. Master data provide key information that is relatively constant and referenced or shared between multiple functions or applications (for example, a customer master record, which contains the customer number, shipping address, billing address, key contact information, and payment terms). Consequently, an additional control objective that may be necessary is “Controls provide reasonable assurance that master data are valid, authorized, and established and maintained in a complete, accurate, and timely manner.” The following are examples of risks that threaten the achievement of the master data control objective:

- Unauthorized or invalid master data records are created.
- Master data records contain incomplete or incorrect data.
- Not all authorized master data records are included in the master files.
- Unauthorized changes are made to master data.
- Authorized changes to master data are not made or are not made on a timely basis.
- Unauthorized, invalid, or incorrect master data files are not detected and corrected on a timely basis.
- Unauthorized, invalid, or incorrect master data exists as a result of compromises in IT general controls.

43. Risks that threaten the achievement of the control objectives stated in management’s description of the service organization’s system encompass the risks of fraud (intentional acts) and unintentional acts. Risks related to fraud may include management override of controls at the service organization; misappropriation of user entity assets by service organization personnel; creation, by service organization personnel, of false or misleading documents or records of user entity transactions processed by the service organization; and fraud by parties outside the service organization, for example, vendors and user entities. Risk assessment is further discussed in paragraphs 130–141.

Control Objectives Specified by Law, Regulation, or an Outside Party

44. Service organizations operate in various business environments, such as information technology processing or financial services and may be subject to governmental or regulatory oversight. This is particularly visible in the financial services industry. Such oversight activities may extend to inspection of the service organization’s controls by the regulatory authorities. For example, the SEC requires the issuance of an annual SOC 1® report on certain aspects of service organizations in the trust and custody industry as a result of publicly known financial malfeasance. In conjunction with the AICPA and other industry groups, the SEC instituted a set of control objectives for a SOC 1®. Other types of attest reports may be appropriate in other industries, but the common theme is the scope and content of the report is specified by parties other than service organization management.

45. Applicable professional standards refer to such control objectives as “control objectives specified by law, regulation, or an outside party.” For example, an outside party may be a user group relying on a shared business application processed by a service organization, such as retail banking or loan servicing. The applicable professional standards state that if the control objectives are specified by an outside party, including control objectives specified by law or regulation, the outside party is responsible for their completeness and reasonableness.

46. Management of the service organization needs to ensure that it is aware of such situations and to discuss the potential effects with the service auditor. Such discussions should be held during the planning phase of the service auditor’s examination activities. Documentation of the final set of control objectives, including any changes or additions to meet applicable professional standards, should be prepared by service organization management because it is relevant to both management's assertion and the service auditor's examination procedures.

47. However, even when the control objectives are specified by an outside party, the service auditor still needs to exercise professional judgment in evaluating the completeness and reasonableness of the control objectives in the circumstances. The service auditor should discuss their conclusions with service organization management and the effect, if any, on the service auditor's report.

48. For example, if an outside party specifies control objectives that only address application controls, but the proper functioning of IT general controls is necessary for the application controls to operate effectively, the service organization would be expected to include the relevant IT general controls in its description of the service organization's system as they relate to the specified control objectives. The service auditor's opinion would be modified if the service organization's control objectives are established by an outside party and control objectives are omitted that the service auditor believes are necessary to achieve the control objectives established by the outside party. An example of such an omission is a set of control objectives that does not address the authorization, testing, documentation, and implementation of changes to existing computerized applications.

49. Because the service organization may be operating in an industry that is subject to regulatory oversight, regulatory examinations may also be required in addition to the service auditor's activities. Professional standards require the service auditor to request a written representation from management of the service organization that it has disclosed to the service auditor such regulatory examinations and their results, occurring and reported on during the period covered by the service auditor's report. Depending on the effect of such regulatory activities, additional disclosures may be needed in the service auditor's report. See paragraphs 148–153 for an additional discussion of representation letters.

Identifying Subservice Organizations and Determining Whether Subservice Organizations Will Be Carved Out or Included in the Description of the Service Organization's System

Determining if an Entity Is a Subservice Organization

50. Service organizations often find it efficient or necessary to outsource certain business functions to other organizations (service providers). Those service providers may be affiliates or independent third parties. In some instances, the operations at those service providers will affect the delivery of services to user entities, and, in some cases, the operations at those service providers will affect user entities' ICFR.

51. In some instances, the ability of the service organization to achieve its control objectives depends on the suitability of design and operating effectiveness of controls at a service provider. For example, a service organization may rely on a cloud service provider for the infrastructure used to host its applications. Because the service organization does not have the ability to implement controls over the cloud service provider’s operations, it depends on effective controls at the service provider to address the risks that the infrastructure represents to user entities’ ICFR. When this type of dependence on a service provider’s controls exists, the service provider is referred to as a subservice organization.

52. Management of a service organization should understand the factors that cause a service provider to be considered a subservice organization because that categorization affects the content of the service organization’s description of its system, management’s assertion, and the service auditor’s report in a SOC 1® engagement.

53. Table 2, “Determining Whether a Service Provider Is a Subservice Organization,” presents matters to consider in determining whether a service provider used by a service organization is a subservice organization. This table does not contain a comprehensive list of matters to be considered and is presented for illustrative purposes only. In any engagement, when determining whether a service provider is a subservice organization, management of the service organization should discuss the facts and circumstances about the other organization with the service auditor.

Table 2*:* Determining Whether a Service Provider Is a Subservice Organization

1 **What Service Does the Organization Provide to the Service Organization?**	**2** **Is the Service Provided by the Organization Relevant to User Entities’ ICFR?**	**3** **Is the Organization a Subservice Organization?**
Report printing and mailing This organization prints the service organization’s electronic files containing financial reports for user entities and mails the reports to the user entities. The information in the reports is incorporated into the user entities’ financial statements. The organization is responsible for controls over the completeness and accuracy of the reports.	Yes. The service provided by this organization is relevant to user entities’ ICFR because the information in the reports is incorporated into the user entities’ financial statements.	Yes
Report printing and mailing This organization prints the service organization’s electronic files containing financial reports for user entities and mails the reports to the user entities. The information in the reports is incorporated into the user entities’ financial statements. The organization prints and mails the statements, but the service organization retains responsibility	No. Because the service organization retains responsibility for controls over the completeness and accuracy of the reports, controls at this organization are not likely to be relevant to user entities’ ICFR.	No

1 **What Service Does the Organization Provide to the Service Organization?**	2 **Is the Service Provided by the Organization Relevant to User Entities' ICFR?**	3 **Is the Organization a Subservice Organization?**
for the completeness and accuracy of the reports.		
Document storage and record retention This organization picks up boxes of documents from the service organization and stores them at its facility.	No. Although this service is important to the service organization's business and enables the service organization to meet certain regulatory requirements, document storage and record retention services do not relate to user entities' ICFR.	No
Electric power This organization provides electric service to the service organization.	No. Although important for the service organization's continuing operations, the electric service does not relate to user entities' ICFR.	No
Pharmacy claims processing This organization processes pharmacy claims for a medical claims processing service organization. Pharmacy claims are a subset of all the claims the medical claims processing service organization receives. The information in the reports provided by the organization are incorporated in the financial statements of user entities that submit pharmacy claims to the medical claims processor.	Yes. The processing performed by the pharmacy claims processor is relevant to the ICFR of user entities that submit pharmacy claims to the organization for processing.	Yes
Application hosting This organization manages all the IT systems for the service organization.	Yes. The service provided by the application hosting organization relates to user entities' ICFR because controls at the application hosting organization are necessary for the service organization's application controls to operate effectively.	Yes
Software development The service organization outsources the development of its application changes to a software development organization. This organization receives the authorized changes from the service organization, develops the changes, and sends them back to the service organization. The	No. In this scenario the organization would be considered a vendor because the service organization's controls alone are sufficient to meet the needs of a user entity's ICFR.	No

1 What Service Does the Organization Provide to the Service Organization?	2 Is the Service Provided by the Organization Relevant to User Entities' ICFR?	3 Is the Organization a Subservice Organization?
service organization authorizes all changes to be developed, reviews the accuracy of the changes, performs all user acceptance testing, and approves all changes prior to implementing them in production.		
Cloud-based data processing The service organization operates its internet sales application at a cloud-based data processing entity. Although the service organization implements certain controls over the functions performed by the cloud-based data processing entity, the service organization's controls alone are not sufficient to enable the service organization to achieve the related control objectives because it relies on the effectiveness of certain controls at the cloud-based data processing entity, specifically, the IT general controls.	Yes. The services provided by the cloud-based data processing entity are relevant to user entities' ICFR because controls at the data processing entity are necessary for the service organization's controls to operate effectively.	Yes

54. As noted in Table 2, controls at a service provider may appear to be relevant to user entities' ICFR. However, if the service organization's controls alone are sufficient to achieve its control objectives (the service organization is not dependent on the service provider's controls to achieve the related control objectives), management of the service organization may conclude that the service provider is not a subservice organization. In these circumstances, management of the service organization would not need to, but may, indicate in its description of the service organization's system and in management's assertion that it uses the services of a service provider. Likewise, the service auditor would not be required to disclose the services provided by the service provider or refer to the service provider in the service auditor's report.

Determining Whether Subservice Organizations Will Be Carved Out or Included in the Description

55. Generally, a service organization will engage a service auditor to examine and report on only those policies and procedures designed and implemented by the service organization itself and will exclude from the engagement any policies and procedures performed by subservice organizations, even if those controls are necessary to achieve one or more control objectives. This approach is known as the carve-out method and is defined as follows:

> **Carve-out method.** Method of addressing the services provided by a subservice organization, whereby management's description of the service organization's system identifies the nature of the services performed by the subservice organization and excludes from the description and from the scope of the service auditor's engagement the subservice organization's relevant control objectives and related controls. When using the carve-out method, controls at the subservice organization are not subject to the service auditor's examination procedures.

56. In some situations, management of a service organization may decide to include the policies and procedures of one or more subservice organizations as part of the engagement, after obtaining agreement of the subservice organization or organizations to participate in the engagement. This method of presentation is known as the inclusive method and is defined as follows:

> **Inclusive method.** Method of addressing the services provided by a subservice organization whereby management's description of the service organization's system includes a description of the nature of the services provided by the subservice organization as well as the subservice organization's relevant control objectives and related controls. When using the inclusive method, controls at the subservice organization are subject to the service auditor's examination procedures. An inclusive report generally is most useful in the following circumstances:
>
> - The services provided by the subservice organization are extensive.
> - A type 1 or type 2 report that meets the needs of user entities and their auditors is not available from the subservice organization.
> - Information about the subservice organization is not readily available from other sources.

Factors for Service Organization Management to Consider in Determining Whether Services Provided by a Subservice Organization Should Be Presented Using the Carve-Out or Inclusive Method

57. Although the inclusive method provides more information for user entity auditors than the carve-out method does, the inclusive method may not be appropriate or feasible in all circumstances. Factors that are relevant in determining which approach to use include the following:

a. The nature and extent of the information about the subservice organization that user auditors may need

b. The challenges entailed in implementing the inclusive method, which are described in paragraphs 57–59 and paragraph 97 *c.* Whether the service auditor is independent of the subservice organization (In an inclusive method engagement, the service auditor's report covers the service organization and the subservice organization, and the service auditor would need to be independent of both entities.)

d. The availability of a type 1 or type 2 service auditor's SOC 1® report on the subservice organization that meets the needs of user entities[4] and their auditors

58. The inclusive method is more easily facilitated if the service organization and the subservice organization are related parties or if the contract between the service organization and the subservice organization provides for an inclusive description of the service organization's and subservice organization's system and report by the service auditor.

59. However, the inclusive method is frequently difficult to implement and for a number of reasons may not be feasible in certain circumstances. This approach generally requires extensive planning and communication between the service auditor, the service organization, and the inclusive subservice organization. Both the service organization and the subservice organization should agree on the inclusive approach before it is implemented.

Preparing the Description of the Service Organization's System

60. Management of the service organization is responsible for preparing the description of the service organization's system, including the completeness, accuracy, and method of presentation of the description. As part of this activity, management should assign or confirm responsibilities of service organization personnel for preparation of the description of the service organization's system.

Method of Presentation of the Description

61. Management is responsible for documenting the service organization's system. No one form of documenting the service organization's system is prescribed, and the extent of the documentation may vary depending on the size and complexity of the service organization and the complexity of the services provided.

62. The description of the service organization's system can be organized in a variety of ways. For example, the description may be organized by the components of internal control (the control environment, risk assessment process, information and communications, control activities, and monitoring processes). The description should permit a reader to understand the flow of transactions or information through the service organization's system. To accomplish this, a

[4] Paragraph .A70 of AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting,* in AICPA *Professional Standards,* indicates that a user entity is also considered a user entity of the service organization's subservice organizations if controls at subservice organizations are relevant to internal control over financial reporting of the user entity. In such a case, the user entity is referred to as an *indirect* or *downstream* user entity of the subservice organization. Consequently, an indirect or downstream user entity may be included in the group to whom use of the service auditor's report is restricted if controls at the service organization are relevant to internal control over financial reporting of such indirect or downstream user entity.

description may contain narratives that describe the processes and controls that the service organization has placed in operation to address control risk associated with those processes. Diagrams or flowcharts may be used to supplement the narratives contained in the description. Appendix A includes an illustrative outline for management's description of the service organization's system.

63. Typically, the description of the service organization's system is organized as follows:

- Overview of the service organization (for example, types of services provided, relevant locations)
- Relevant services provided to user entities
- Discussion of the service organization's control environment, risk assessment, monitoring, information and communications and control activities as it relates to the services provided and in scope for the report
- The specific procedures followed by the service organization in carrying out its responsibilities for user entities (The description is most helpful if it follows a logical transaction flow from initiation to reporting of a transaction and includes details on the process, people, systems and controls in place. The control objectives and related control activities may be presented directly in the description or, to reduce repetition, may be referred to and presented only in the section that presents the service auditor's test results. If the control objectives and related activities are presented with the service auditor's test results only, management should make it clear that the control objectives and control activities remain an integral part of the description of the service organization's system.) The following is an example of that disclosure:

  > ***Control Objectives and Related Controls***
  >
  > Example Service Organization has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives and related controls are presented in section 4, "Description of Example Service Organization's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results," and are an integral component of Example Service Organization's description of its system.

- Complementary subservice organization controls, if applicable
- Complementary user entity controls, if applicable

Although CSOCs and complementary user entity controls are included as part of the description in the outline previously, they could alternatively be presented in the section that presents the service auditor's tests of controls and results, following the same approach outlined previously for control objectives and related control activities.

Completeness and Accuracy of the Description

64. The description of the system is intended to provide readers with information about the service organization's system that is likely to be relevant to the user entities' ICFR. Services provided by a service organization are relevant to an audit of a user entity's financial statements when those services and the controls over them affect the user entity's information system, including related processes relevant to financial reporting.

65. Management ultimately asserts that the description fairly presents the system and identifies the criteria used in making its assertion. Because management is making its assertion about the fairness of the presentation of the description in accordance with the criteria, the service auditor is also expressing an opinion on the fairness of presentation of the description in accordance with the criteria.

Other Information

66. Management may wish to include information in the description of the service organization's system that is not covered by the service auditor's report. The service auditor is required to identify information included in a document containing the service auditor's report that is not covered by the service auditor's report as such. Generally, such other information may be presented in a section of the type 2 or type 1 report entitled "Other Information Provided by the Service Organization." Information in this section is not covered by the service auditor's report; however, the service auditor is required to perform certain procedures on the other information. Typically, this would be information the service organization wishes to communicate to user entities that is beyond the scope of the engagement. Such information may be prepared by the service organization or by another party. Examples of such information include the following:

- Future plans for new systems or system conversions
- Other services provided by the service organization that are not included in the scope of the engagement
- Information related to the privacy of personally identifiable or medical information
- Information that would not be considered relevant to user entities' ICFR, such as information about the service organization's business continuity plans
- Responses from management regarding deviations in tests of controls, such as information about causative factors for deviations identified in the service auditor's tests of controls, the controls that mitigate the effect of the deviations, corrective actions taken, and expected future plans to correct controls
- A report comparing the service organization's performance to its commitments to user entities per service level agreements, or a newsletter containing information about events at the service organization
- A description of a subsequent event that does not affect the functions and processing performed by the service organization during the period covered by the service auditor's report but may be of interest to user entities

67. Other information included in a SOC 1® report should

- not be inconsistent with the description of the service organization's system, management's assertion, or the service auditor's report and
- not contain a material misstatement of fact (for example, information that is not objective, measurable, or verifiable).

Content of the Description

68. The description of the service organization's system should include the information outlined in paragraphs 69–101.

Types of Services Provided, Procedures to Provide Services, Information Used to Provide Services, Process Used to Prepare Reports, and Significant Events

69. The description should include the types of services provided, including, as appropriate, the classes of transactions processed. Examples of classes of transactions are distributions (for example, lump-sum payments, periodic payments, forfeitures, loans) or investment income (for example, stock sales, interest income, dividend income).

70. The description should also include how significant events other than transactions are captured and addressed. For example, include the process and controls for a customer conversion from another service provider or new customer initiation.

71. An effective way to present the information clearly and concisely may be to provide a transaction flow within the description so that readers can visualize the various types of transactions and events as well as understand the procedures to process relevant information and transactions and prepare reports for user entities.

72. The procedures should be described in enough detail to explain for each applicable class of transaction how the transactions are initiated, authorized, processed, recorded and corrected as necessary. The description should include the people (in other words, the titles of individuals or groups) that are responsible for the procedures and controls. In describing the procedures, management should outline the information used such as accounting records or other supporting information. The description should also include how information is provided to user entities via reports or other methods (for example, web portal). The description should outline management's controls in place supporting the completeness and accuracy of reports and information. Management may consider including a list of key reports that are provided to user entities.

Control Environment, Risk Assessment Process, Information and Communications, and Monitoring Activities

73. The service organization's description should include other aspects of the service organization's internal control components (control environment, risk assessment process, information and communications [including the related business processes], control activities, and monitoring activities) that are relevant to the services provided. Service organization management should use judgment in determining what aspects of the other components of internal control should be included in the description, depending on the unique facts and circumstances.

74. The following is a brief description of the components of a service organization's internal control, other than its control activities.

- *Control environment*. The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all the other components of internal control, providing discipline and structure. Aspects of a service organization's control environment may affect the services provided to user entities. For example, management's hiring and training practices generally would be considered an aspect of the control environment that may affect the services provided to user entities because those practices affect the ability of service organization personnel to provide services to user entities.

- *Risk assessment*. Aspects of a service organization's risk assessment process may affect the services provided to user entities. Example risk assessment factors that might relate to a relevant risk in the services provided include changes in the operating environment, new personnel who are responsible for executing manual controls, new or revamped information systems, change in workload for individuals responsible for controls as a result of rapid growth or new business model, products or activities, or corporate restructurings.

- *Information and communications*. Activities of a service organization that may represent part of a user entity's information and communications component of internal control include the information system relevant to financial reporting objectives, consisting of the procedures — whether automated or manual — and records established by the service organization to initiate, authorize, record, process, and report a user entity's transactions (as well as events and conditions) and maintain accountability for the related assets, liabilities, and equity. Communication involves how the entity communicates financial reporting roles and responsibilities and significant matters relating to financial reporting.

- *Monitoring*. Many aspects of monitoring may be relevant to the services provided to user entities. For example, a service organization may employ internal auditors or other personnel to evaluate the effectiveness of controls over time, through ongoing activities, periodic evaluations, or various combinations of the two. Monitoring external communications, such as customer complaints and communications from regulators, generally would be relevant to the services provided to user entities. These monitoring activities are frequently included as control activities for achieving a specific control objective. If the service organization utilizes a subservice organization, the service organization's monitoring of the subservice organization's activities that affect user entities' ICFR is another example of monitoring. This form of monitoring may be accomplished through visits to the subservice organization or, alternatively, by obtaining and reading a type 1 or type 2 report on the subservice organization.

Consideration of the 2013 COSO Framework

75. Various frameworks can be used as established criteria for designing, implementing, and evaluating the effectiveness of internal control. One such framework that may be used is COSO's *Internal Control—Integrated Framework* (2013 COSO framework).[5] The 2013 COSO framework retains the 5 components of internal control included in the 1992 COSO framework (as explained previously) and formalizes the concepts into 17 principles associated with the components.

76. The service organization control objectives and controls do not need to be based on a specific internal control framework; therefore, the management of a service organization is not required to use the 17 principles when designing and implementing internal control. However, management of a service organization may find it useful to consider the principles included in the 2013 COSO framework, especially when one or more of the user entities uses the 2013 COSO framework to evaluate their ICFR. In such cases, user entity management may be looking to the service organization's description of its system to provide information relevant to those principles that may affect the user entity's adherence to the 2013 COSO framework requirements. Therefore, during planning, management of the service organization may consider whether and how it will communicate relevant aspects of the principles in the description of the service organization's system.

Presenting Specified Control Objectives and Controls Designed to Achieve Those Objectives

77. There are multiple formats for presenting the control objectives and controls in management's description of the service organization's system and no one format is required. A frequently used format is the placement of three-column matrixes in the section of the type 2 report that is usually reserved for the service auditor's description of tests of controls and results (usually identified as section 4, "Service Organization's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results"). A separate matrix is presented for each control objective, and the control objective is identified above the matrix. The controls that management has identified to achieve that control objective are placed in the column 1 of the matrix. Both the control objective and the controls to achieve that objective are considered an extension of management's description of the service organization system (usually identified as section 3). Columns 2 and 3 of the matrix belong to the service auditor and include a description of the service auditor's tests of controls and the results of those tests, respectively. A note is placed in the description of the service organization's system indicating that, although management's control objectives and controls are included in the service auditor's description of tests of controls and results, they are part of management's description. This obviates the need to repeat the control objectives and controls in management's description. For clarity, the matrixes may also indicate that the control objectives and controls are part of management's description and that the descriptions of tests of controls and results are provided by the service auditor.

[5] ©2019, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

78. To be useful to user entities and user auditors, when describing a service organization's controls, the description should include information about the frequency with which a control is performed or the timing of its occurrence, the person or parties responsible for performing the control, the activity being performed, and the source of the information to which the control is applied. The following control description is an example that includes all these elements:

> The cash reconciliation group (*persons responsible for performing the control*) reconciles (*activity performed*) money movement reflected in the ABC application output report (*source of the information*) to the fund's custodian bank report (*source of the information*) on a monthly basis (*frequency*).

Characteristics of Control Activities

FRASA	Description
Frequency	The frequency or timing of occurrence (for example, daily or weekly)
Responsible Party	The party responsible for conducting the risk-mitigating activity (for example, the director of trading reviews, the accounting associate compares)
Activity	The specific risk-mitigating activity — Procedures must have a risk-mitigating impact to be considered a control activity as opposed to a procedure (for example, reconciliations are performed and reviewed between bank account balance and general ledger cash account balance and adjustments are recorded, if needed).
Source	The sources of information (if applicable) ─ The control should either define how management has addressed the completeness and accuracy of the information used in the control or there should be separate controls that address the completeness and accuracy of the information.
Action Taken	The action taken with the results of the control activity (for example, adjustments are made to the general ledger cash accounts, if needed, based on reconciliation to the bank balances)

Complementary User Entity Controls

79. Complementary user entity controls are controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by user entities and are necessary to achieve the control objectives stated in management's description of the service organization's system. Said another way, these are controls that if not performed by the user entity, would have a detrimental impact on the service organization's ability to meet the control objectives in the report. It is important that the description indicates that the user entities are responsible for implementing those complementary user entity controls. Although there may be many responsibilities outlined within contracts between the service organization and the user, a responsibility of a user entity would only be a complementary user entity controls to be included within the report if the service organization is dependent upon the user entity to perform the control to achieve a control objective in the report.

80. Some examples of complementary user entity controls include the following:

- In situations where the user entity is responsible for administering user's access to the application for their employees, when a service organization is providing an application system used by the user entity, a complementary user entity control might be "The design of XYZ Service Organization's controls assumes that user entities have implemented controls that address logical access by user entity personnel to the service organization's application, and that these controls are suitably designed and operating effectively throughout the period."

- When a service organization is responsible for the expenditure cycle (for example, processing invoices, accruals and payments) on behalf of the user entity, a complementary user entity control might be "The design of XYZ Service Organization's controls assumes that user entities have implemented controls that address the authorization of new vendors and communication of changes to the vendor master file to the service organization in a timely manner and that those controls are designed and operating effectively throughout the period."

- When a service organization is responsible for recording fixed asset transactions into the subledger of the user entity, but the user entity maintains responsibility for transactional decisions, a complementary user entity control might be "The design of XYZ Service Organization's controls assumes that user entities have implemented controls that address the communication of fixed assets projects, additions, and disposals to the service organization in a timely manner and that those controls are designed and operating effectively throughout the period."

81. There is no prescribed format for presenting the complementary user entity controls. They may be listed in a table as part of the description (typically included at the end of the description) or following the service organization's description of control objectives and related controls, and the service auditor's description of test of controls and results in the testing matrix to which they apply. Complementary user entity controls should identify the specific control objective to which they are linked.

Content of the Description When the Service Organization Uses the Carve-Out Method

82. When the carve-out method is used, the description should include the nature of the services performed by the subservice organization but would not describe the detailed processing or controls at the subservice organization. The description of the service organization's system carves out those control objectives for which related controls operate only or primarily at the subservice organization. However, the description should contain sufficient information concerning the carved out services to enable user entities and their auditors to

- understand the significance and relevance of the subservice organization’s services to user entities’ ICFR and

- determine what additional information they may need to obtain from the subservice organization to assess the risks of material misstatement of the user entity’s financial statements.

When the carve-out method is used, AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting,*[6] is silent about whether disclosure of the identity of the subservice organization is required. However, typically that information would be needed by user auditors to obtain information and perform procedures related to the subservice organization.

Complementary Subservice Organization Controls

83. When using the carve-out method, instances may exist in which the achievement of one or more control objectives is dependent on one or more controls at the subservice organization. Such controls are termed *complementary subservice organization controls* and are defined as “controls that management of the service organization assumes, in the design of the service organization’s system, will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management’s description of the service organization’s system.” Management’s description of the service organization’s system should identify such CSOCs.

84. Because CSOCs are necessary to achieve certain control objectives, it is important that the description of the service organization’s system describe the subservice organization’s responsibilities for implementing those CSOCs and also indicate that the related control objectives can be achieved only if the complementary subservice organization’s controls are suitably designed and operating effectively throughout the period. To be meaningful to user entities and their auditors, CSOCs should be specific to the services provided but may be presented as broad control categories or objectives. The service organization may wish to include a table in the description that identifies those instances in which control objectives are met solely by the service organization and those in which controls at the service organization and CSOCs re needed to meet the control objectives. Paragraph 86 includes an example of a situation in which a control objective is not included in management’s description of the service organization’s system, but the application of CSOCs at the subservice organization is necessary to achieve the control objectives stated in management’s description.

85. ABC Company, a claims transaction processor, uses Alternative Hosting, a subservice organization, to manage all its IT controls, including controls that address program changes, logical access, and computer operations and infrastructure. The subservice organization is responsible for all aspects of IT controls related to these areas. Although not a complete list, the

[6] All AT-C sections can be found in AICPA *Professional Standards*.

following are examples of CSOCs that ABC Company assumes Alternative Hosting is responsible for:

- Access to the applications and related infrastructure is restricted to authorized individuals.
- Access to the data center is restricted to authorized individuals.
- Changes to application programs and related data management systems are authorized, tested, documented, and approved for implementation into production.
- Application and system processing are authorized and executed in a complete, accurate, and timely manner.

86. ABC Company may determine that it will not include a control objective related to IT in its description of the service organization's system because the related controls are performed by Alternative Hosting. However, in this example, the IT controls at the subservice organization are deemed CSOCs because they are necessary to achieve the business process control objectives related to the complete, accurate, and timely processing of claims and support the functioning and maintenance of the applications included in the scope of the engagement, automated application controls, and aspects of claims business processing.

Examples of Complementary Subservice Organization Controls

87. The following are some examples of CSOCs related to transaction processing:

- XYZ Service Organization outsources its claims processing activities to a subservice organization. The subservice organization enters, adjudicates, and disburses claim payments on behalf of the service organization. Therefore, a CSOC should be included in the description and could be presented as follows:

  > The design of XYZ Service Organization's controls assumes that the subservice organization has implemented controls that address the completeness and accuracy of claims transaction processing (entering, adjudicating, and disbursing performed on behalf of XYZ Service Organization) and assumes that those controls were suitably designed and operating effectively throughout the period.

- XYZ Service Organization outsources the data entry of accounts payable invoices to a subservice organization. The subservice organization is responsible only for data entry and XYZ Service Organization's controls address the remaining information processing objectives related to accounts payable. Therefore, a CSOC should be included within the description and could be presented as follows:

  > The design of XYZ Service Organization's controls assumes that the subservice organization has implemented controls that address the completeness and accuracy of accounts payable data entry and assumes that those controls were suitably designed and operating effectively throughout the period.

- XYZ Service organization outsources trade execution monitoring to a subservice organization. The subservice organization is responsible for confirming that all trade requests received prior to the market cutoff are processed the same day. If XYZ Service Organization's control objective addresses the timeliness of trade execution, a CSOC should be included in the description and could be presented as follows:

  > The design of XYZ Service Organization's controls assumes that the trade execution monitoring subservice organization has implemented controls to ensure that trade requests received prior to 4pm are processed completely, accurately, and on the same day received and assumes that those controls were suitably designed and operating effectively throughout the period.

The following are examples of CSOCs related to logical access:

- XYZ Service Organization outsources the management of IT infrastructure to a subservice organization. Using the service organization's systems, subservice organization personnel manage the access administration for the IT infrastructure components. Therefore, a CSOC should be included in the description and could be presented as follows:

  > The design of XYZ Service Organizations controls assumes that the subservice organization has implemented controls over the administration of logical access at the operating system and database layers and assumes that those controls were suitably designed and operating effectively throughout the period.

- XYZ Service Organization outsources promotion to production responsibilities to a subservice organization. The service organization has granted subservice organization users privileged access to the operating system and databases to facilitate the movement of code into the production environment. Therefore, a CSOC should be included in the description and could be presented as follows:

  > The design of XYZ Service Organization's controls assumes that the subservice organization has implemented a control requiring periodic review of users with privileged access at the operating system and database layers to determine that such access is restricted to appropriate and authorized personnel and requiring notification of the service organization of necessary changes in access and assumes that those controls were designed and operating effectively throughout the period.

Monitoring the Subservice Organization

88. Although the service organization may have outsourced certain functions to a subservice organization, the service organization remains responsible for the overall system of internal control. As a result, the service organization needs to have monitoring controls in place over the subservice organization. Management's description of the service organization's system and the scope of the service auditor's engagement includes controls at the service organization that monitor the effectiveness of controls at the subservice organization, which may include some combination of ongoing monitoring to determine that potential issues are identified timely and separate evaluations to determine that the effectiveness of internal control is maintained over time. As part of its monitoring, management should timely review a SOC report or perform other procedures to ensure that the subservice organization has effective controls in place to achieve the CSOCs.

89. Management's description of the service organization's system should include a description of such monitoring controls and the persons responsible for performing them.

90. For example, XYZ Service Organization uses ABC Subservice Organization to provide hosting services. Management and the internal audit department of XYZ Service Organization receive and review the type 2 SOC 1® report of ABC Subservice Organization on an annual basis. As part of the review, management confirms that the CSOCs identified in their own report are covered within the scope of ABC Subservice Organization's SOC 1® report. Any deficiencies identified in ABC Subservice Organization's SOC 1® report are analyzed for relevance to and effect on XYZ Service Organization and its users. Additionally, if the ABC Subservice Organization's SOC 1® report has identified complementary user entity controls, XYZ Service Organization determines if those are included within the scope of their own SOC 1® report either as management controls that are tested by the service auditor or controls that are the responsibility of their users and identified as complementary user entity controls. In addition, through its daily operational activities, management of XYZ Service Organization monitors the services performed by ABC Subservice Organization to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also holds periodic calls with the subservice organization to monitor compliance with the service level agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to subservice organization management.

Content of the Description When the Service Organization Uses the Inclusive Method

91. When the inclusive method is used, management of the service organization should discuss the requirements for describing the controls with the service auditor. In addition, management of the service organization should determine with the service auditor whether it will be possible to obtain evidence that supports the portion of the opinion that addresses the subservice organization and obtain a written assertion and representation letter from the subservice organization.

92. Management of the service organization generally coordinates the use of the inclusive method with the subservice organization. If the inclusive method is used, matters to be agreed upon or coordinated by the service organization and the subservice organization include the following:

- The scope of the examination and the period to be covered by the service auditor's report
- Acknowledgment from management of the subservice organization that it will provide the service auditor with a written assertion and representation letter (Management of the service organization and management of the subservice organization are each responsible

for providing the service auditor with a written assertion and representation letter.)

- The planned content and format of the inclusive description of the system
- The representatives of the management of both the subservice organization and the service organization, and the assigned responsibility for
    - — providing each entity's description and
    - — integrating the descriptions
- For a type 2 report, the timing of the tests of controls performed by the service auditor

93. When the service organization uses the inclusive method to present the services provided by a subservice organization, management of the service organization is responsible for evaluating the service organization's description of its system as well as the subservice organization's description of its system. In addition, in most inclusive method engagements, the service organization is the engaging party (and not the subservice organization); and, when the subservice organization is a non-engaging party, management of the service organization should acknowledge and accept responsibility for obtaining the subservice organization's written assertion and letter of representation.

94. If the inclusive method is used, the description includes the nature of the services provided by the subservice organization and the relevant control objectives and related controls performed by the subservice organization. Relevant controls at the subservice organization may also include aspects of the subservice organization's control environment, risk assessment process, information and communications, and monitoring activities. The description should separately identify controls at the service organization and controls at the subservice organization. However, no prescribed format exists for differentiating between controls at the service organization and controls at the subservice organization.

95. When the inclusive method is used, both the service organization and the subservice organization should provide the service auditor with a written assertion covering the services performed. The written assertions accompany management's description of the service organization's system. Management of the service organization should include both assertions in, or attach them to, the description of the service organization's system. If the assertions are included in the description rather than accompanying the description, the assertions should be clearly segregated from the description (for example, using headings) because they are not a part of the description and the service auditor is not reporting on management of the service organization's and management of the subservice organization's assertions. As noted in paragraph 57, when the service organization uses the inclusive method, the service auditor needs to be independent of both the service organization and the subservice organization.

96. The service organization's assertion ordinarily would be expected to address the fairness of presentation of the description, the suitability of the design of the controls, and the operating effectiveness of the controls. However, in some circumstances, the achievement of a control objective may be dependent on a combination of the service organization's controls and the subservice organization's controls. In such circumstances, if the service organization designed the controls for the subservice organization, it may be possible when using the inclusive method for the service organization to take responsibility for the fair presentation of the description and for the suitability of the design of its own controls and the subservice organization's controls. In such cases, the subservice organization’s assertion may be limited to the operating effectiveness of its controls.

97. If management of the service organization chooses to use the inclusive method of presentation, but management of the subservice organization refuses to provide a written assertion, the service organization will not be able to use the inclusive method but may be able to use the carve-out method instead.

98. Using the inclusive method becomes more complex when the service organization uses multiple subservice organizations. When the services of more than one subservice organization are likely to be relevant to user entities’ ICFR, management of the service organization may use the inclusive method for one or more subservice organizations and the carve-out method for other subservice organizations. In these instances, management’s description needs to clearly state which subservice organizations and related functions are included in the description and which are carved out. The presentation of any subservice organizations should adhere to the approach that management of the service organization has selected, whether that approach is the inclusive or the carve-out method.

99. If the description includes organizations that provide services to the service organization that are considered vendors and subservice organizations, it may be helpful if the description distinguishes between vendors and subservice organizations.

100. In most inclusive engagements, the service organization is the only engaging party (not both the service organization and the subservice organization). When a subservice organization is not an engaging party, the condition of being an engaging party does not exist for the subservice organization, and therefore, any requirements related only to an engaging party do not apply to the subservice organization — for example, management of the service organization must agree upon the terms of the engagement with the service auditor. A non-engaging party subservice organization in an inclusive engagement has no contractual relationship with the service auditor. When using the inclusive method in these circumstances, management of both the service organization and the subservice organization determine who will be responsible for providing each entity’s description and integrating the descriptions. When the subservice organization is a non-engaging party, management of the service organization should acknowledge and accept responsibility for obtaining several documents such as the subservice organization’s portion of the description, written assertion, and letter of representations.

Changes to the System During the Period

101. The description of the service organization’s system in a type 2 engagement includes relevant details of changes to the service organization’s system during the period covered by the description. Changes would be included in the description if they are likely to be relevant to the user entities’ ICFR, for example, the service organization’s migration to a cloud infrastructure. The changes may be described as part of the controls throughout the description or outlined separately within the description. For example, if management automated the processing of removing users that no longer require access due to termination and this process used to be a manual control by system administrators to remove access, this type of change might logically be described within the description of the logical security controls. Conversely, if the changes are broad such as changes in the systems used to provide the services which resulted in changes in the functionality or reports provided to user entities, it might be described under a separate heading within the description to highlight all the relevant changes.

New Reports Versus Recurring Reports

102. If preparing management's description of the service organization's system for the first time, developing an outline and determining the format to present the information (narrative, flowcharts, and the like) is a good starting point. Management may be able to leverage existing documentation such as contracts with user entities, control narratives, flowcharts, and risk and control matrixes to assist in developing the description of the system.

103. Once developed, in future reports the level of effort will be focused more specifically on identifying changes that have occurred that need to be reflected in the report. Changes could have been made to the processes, people, systems, locations or controls. However, there may also have been changes in the services that are provided by the service organization that are relevant to a user entity's ICFR. Additionally, the service organization may have changed relationships with subservice organizations that need to be considered.

Evaluation

Evaluation

Coordination With the Service Auditor

104.

Service organization management may find it helpful to assign designated personnel to assist in facilitating the performance of the SOC 1® procedures by the service auditor. During the service auditor's engagement, the service auditor will likely make inquiries of various service organization personnel and perform tests of the service organization's controls across several business functional areas, such as accounting, transaction processing, and information technology. These functional areas will have responsibilities for supporting the service organization's ongoing business operations while providing information to the service auditor. Coordination of such activities by designated personnel to support the service auditor may be an efficient management technique.

105. Assisting the service auditor in performing walk-throughs is one way in which service organization personnel can facilitate the performance of a SOC 1® engagement. In a walk-through, the service auditor traces one or more transactions from initiation to the transfer of information to user entities. This assists the service auditor in determining whether procedures are actually performed as stated in the description of the service organization's system. When performing a walk-through, the service auditor will ask relevant members of the service organization's management and staff to describe and demonstrate their actions in performing a procedure.

106. The assigned coordinator of such activities should have a broad understanding of the service organization's business within the scope of the report and possess project management skills. Example of responsibilities include the following:

- Reviewing requests from the service auditor for information and evidence and identifying or coordinating with appropriate points of contact
- Assisting the service auditor in identifying key control owners and relevant sources of information at potentially multiple locations for the control activities specified by service organization management
- Assisting in the timely identification, collection, and initial quality review of information related to the in-scope control activities
- Assisting the business functional areas in identifying and documenting complementary user entity control considerations that are relevant to the scope of the service auditor's examination
- If subservice organizations are relevant to the scope of the report, assisting the business functional areas in documenting CSOCs, for example, the dependence on a subservice organization for controls over custody of financial assets, or reliance on outsourced information technology data centers
- Coordination and resolution of matters that may affect the service auditor's report, for example, such as control deviations identified by the service auditor (This may include additional efforts to coordinate the service auditor's activities in those situations where there may be an inclusive subservice organization in the scope of the examination.)
- Coordinating timely updates to management's written assertion and description of the system
- Coordinating management of the service organization and the service auditor to discuss the examination results, the effect on the report, and the completion of the required letter of representations prior to report issuance
- Educating others in the service organization regarding their responsibilities in supporting the service auditor's examination (Such education may be performed together with the service auditor.)

107. In smaller or less complex service organizations, it may be more efficient for some of these responsibilities to be performed by the business control owners interacting directly with the service auditor. In more complex or geographically dispersed service organizations, such coordination activities may be more effectively performed by multiple persons. Some service organizations have determined that these activities require a commitment of time by the coordinator. Such additional resources may be needed when there are multiple teams of service auditors performing examination procedures for multiple locations.

Determining Whether Internal Auditors Will Assist the Service Auditor and Whether the Service Auditor Will Use the Work of the Internal Audit Function

108. The internal audit function may assist the service auditor in performing a SOC 1® engagement in the following ways:

a. Members of the internal audit function may assist the service auditor by performing certain tasks under the supervision of the service auditor (known as direct assistance).

b. The service auditor may use the work independently performed by the internal audit function to obtain evidence about the design and operating effectiveness of the applicable controls (known as using the work of internal audit).

Management's Considerations

109. In deciding whether to offer the assistance of members of the internal audit function to the service auditor, management should weigh the benefits versus the costs of doing so. Some of the benefits include the cost savings associated with using internal resources instead of external resources (the service auditor's team) and the transfer of knowledge from the service auditor to members of the internal audit function about how the service auditor evaluates controls covered by the SOC 1® report. The primary cost of using internal auditors is diverting internal audit resources away from other audits, special projects, and the approved annual audit plan without increasing the internal audit staff. Additional training of internal audit personnel may be needed for them to perform certain tasks. If using the work of internal auditors, the internal audit plan will need to be adjusted to meet the specific scope and timeframe required for the SOC 1® report. Further considerations include the qualifications of the internal audit staff and the independence of the internal audit function. If management decides to provide internal audit resources, planning and coordination with the service auditor will be required to ensure optimum use of the resources. The ultimate decision about whether to use internal audit resources during the examination resides with the service auditor.

Use of Direct Assistance

110. When internal auditors provide direct assistance to the service auditor, the service auditor directs, supervises, and reviews the work of the internal auditors, including testing some of the work performed by the internal auditors. Management should expect the service auditor, as part of directing and supervising internal auditors, to discuss the following with the internal auditors:

- Their responsibilities
- The objectives of the procedures they are to perform
- Matters that may affect the nature, timing, and extent of examination procedures, including any potential issues
- The need for the internal auditors to bring any issues identified during the examination to the attention of the service auditor

111. Prior to using internal auditors to provide direct assistance, management will be asked to provide the service auditor with written acknowledgment that internal auditors providing direct assistance will be allowed to follow the practitioner's instructions and that management will not intervene in the work the internal auditors perform for the service auditor**.**

*Using the Work of Internal Audi*t

112. Management should expect the service auditor to perform procedures on the work of the internal audit function to determine its adequacy for the purpose of their examination. Such work may include

- retesting some of the items already tested by the internal auditors;
- examining other similar items; and
- observing procedures performed by the internal audit function.

113. Although the internal audit function may perform the following activities as part of its internal audit work, for the purposes of the SOC 1® engagement, the service auditor is responsible for assessing the following:

- Risks of material misstatement
- Pervasiveness of the control
- Potential for management override of the control
- Sufficiency of the procedures performed
- Deficiencies identified during testing.

114. The service auditor will read the reports of the internal audit function and any regulatory examinations that relate to the services provided to user entities and the scope of the engagement and will take the results into consideration in determining the procedures to be performed.

Preparing Management's Assertion

115. Management's assertion about the fairness of the presentation of the description, suitability of the design of controls, and operating effectiveness of the controls accompanies management's description of the service organization's system and is a key element of a SOC 1® report. Generally, management's assertion is placed on the service organization's letterhead. AT-C section 320 does not require that management's assertion be signed. Management's assertion is segregated from the description because it is not part of the description, and the service auditor is not reporting on management's assertion.

116. An illustrative management assertion is included in appendix B and are also included in various AICPA publications. In developing its assertion, management may find it helpful to refer to these illustrations and to customize them for the service organization and its system. Illustrative management assertions for a type 1 and type 2 engagement are provided in exhibit B, "Illustrative Assertions by Management of a Service Organization," of AT-C section 320.

117. Management's assertion should describe the scope of the engagement (for example, the services and systems included in the description and the period covered by the description.) If the illustrative assertions identified in paragraph 116 are used as a template for management's assertion, management should tailor its assertion to reflect the scope of the engagement and service organization. The language used to describe the scope of the engagement in management's assertion should be the same as the language used to describe the scope in the description of the service organization’s system and in the service auditor’s report. Contracts with user entities may provide a good source of language for describing the scope of the engagement. The goal is to ensure that readers of the report know very quickly what is and what is not included in the report. The following is an example of a sentence in management’s assertion that describes the scope of the engagement:

> We have prepared the description of XYZ Service Organization’s defined contribution recordkeeping system entitled “Description of XYZ Service Organization’s Defined Contribution Recordkeeping System” for processing user entities’ transactions throughout the period January 1, 201X, to December 31, 201X, (description) for user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities’ financial statements or ICFR and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities’ financial statements.

118. If applicable, the assertion should include a statement regarding the nature of the services provided by any subservice organizations and whether the subservice organization is included in or carved out of the description of the service organization’s system. The description of the services provided by a subservice organization need not be overly detailed in the assertion because if the carve-out method is used, small amount of additional detail may be provided in the description of the service organization’s system, and if the inclusive method is used, additional detail is required in the description of the service organization’s system. The assertion should highlight to the reader that the service organization uses a subservice organization, the nature of the service provided by the subservice organization, whether the description includes or carves out the services provided by the subservice organization, and that the service is relevant to the scope of the engagement.

119. When the service organization uses the inclusive method to present a subservice organization, a statement such as the following may be added to the assertion to describe the scope of the engagement:

> XYZ Service Organization uses ABC Subservice Organization, a subservice organization, to provide application maintenance and support services. XYZ Service Organization’s description includes a description of ABC Subservice Organization’s application maintenance and support services used by XYZ Service Organization to process transactions for user entities, including controls relevant to the control objectives stated in the description.[7]

120. Management’s assertion should indicate whether complementary user entity controls and CSOCs are assumed in the design of the service organization’s system. This is a critical element

[7] If the subservice organization’s control objectives and related controls are presented separately in the description, the wording of this sentence would read: “XYZ Service Organization’s description includes a description of ABC Subservice Organization’s application maintenance and support services used by XYZ Service Organization to process transactions for user entities, including relevant control objectives and related controls of ABC Subservice Organization.”

of management's assertion because it provides management with an opportunity to inform users of the report that complementary controls at the user entity or CSOCs at the subservice organization are needed for the control objectives to be achieved.

121. Finally, management's assertion should present its statement regarding all the matters covered in the service auditor's opinion and should also include a list of the criteria for evaluating the fairness of the presentation of the description, the suitability of the design of the controls, and in a type 2 engagement, the operating effectiveness of the controls. The following is an example of the portion of management's assertion in which management makes a statement about the matters covered in the service auditor's opinion and identifies the criteria for evaluating the fairness of the presentation of the description, the suitability of the design of the controls, and in a type 2 engagement, the operating effectiveness of the controls:

> We confirm the following to the best of our knowledge and belief:
>
> *a.* The description fairly presents the defined contribution recordkeeping system made available to user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, for processing their transactions as it relates to controls that are likely to be relevant to user entities' ICFR. The criteria we used in making this assertion were that the description
>
> i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,
>
> (1) the types of services provided including, as appropriate, the classes of transactions processed.
>
> (2) the procedures, within both automated and manual systems, by which those services are provided including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
>
> (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions. This includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
>
> (4) how the system captures and addresses significant events and conditions other than transactions.
>
> (5) the process used to prepare reports and other information for user entities.

(6) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.

(8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to the service organization's system during the period covered by the description.

iii. does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the defined contribution recordkeeping system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X, to achieve those control objectives if user entities applied the complementary user entity controls assumed in the design of XYZ Service Organization's controls throughout the period January 1, 201X, to December 31, 201X. The criteria we used in making this assertion were that

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

122. Management's omission or modification of the criteria identified in paragraph 121 (unless the criteria are not applicable) in its assertion about the matters covered by the service auditor's report (the fairness of the presentation of the description, suitability of the design of the controls, and in a type 2 report, operating effectiveness of the controls), may result in the service auditor withdrawing from the engagement or disclaiming an opinion. For example, if a service organization uses a subservice organization but prefers not to mention that information in its description of the service organization's system, and therefore omits that information, the service auditor may conclude that the description is not fairly presented. The description criteria identify the information that is required to be included in the description therefore all the criteria need to be addressed in the description, unless they are not applicable.

123. When preparing management’s assertion, the criteria in paragraph 121 may be used as a checklist to confirm that the description of the service organization’s system includes all the information that should be included. If management finds that the description omits information (for example, a system change is not included) or distorts information, management should revise the description and bring this to the attention of the service auditor.

124. Management’s assertion would be expected to mirror the service auditor’s opinion. If the service auditor determined that controls relating to a control objective were not operating effectively and the related control objective was not met, management would add a paragraph to the assertion, indicating that the specified controls were not operating effectively to achieve the related control objective. (It would be inconsistent for management’s assertion to state that all the controls were operating effectively, and all the control objectives were met and the service auditor’s opinion to state that specified controls were not operating effectively). As a result, it is important for management to discuss any modifications to the service auditor’s opinion with the service auditor, understand the rationale for them, and incorporate them in management’s assertion.

125. Management is responsible for having a reasonable basis for its assertion. Although there are a variety of activities and approaches that management may use to establish that it has a reasonable basis for its assertion, the following are key elements for doing so:

- Monitoring the performance of the controls through an effective internal audit function or targeted testing performed within the business unit providing the services. For some service organizations, this may also include a review of performance or key performance indicator reports generated by the operations group that would highlight errors indicative of control failures in the processing cycle.
- Having a process that enables management to capture changes to the service organization or its system that might need to be included in the description of the service organization’s system. For some organizations, the easiest way to accomplish this is to include a checkpoint within its change management process reminding management to consider the need to update policies, procedures, or even information technology. For other organizations, it may be easier to have a quarterly review of the description of the system by the line managers to ascertain the accuracy and completeness of the description for that quarter. This could help ensure that changes made throughout the period are not missed because of a single, rushed review at the end of the reporting period.
- Active participation in the risk assessment or mitigation process associated with the services covered by the SOC 1® report. Risk assessment is described in paragraphs 126–141.

Other means of establishing a reasonable basis for its assertion include inquiries of control owners, self-certifications, and tests of controls. Management should establish a suitable approach for gathering evidence that will support management's assertion. The work performed by the service auditor as part of a type 1 or type 2 engagement would not be considered a basis for management's assertion because the service auditor is not part of the service organization's internal control.

Establishing a Basis for Management's Assertion

126. Management of the service organization is responsible for identifying the relevant control objectives, determining the risks that threaten the achievement of these control objectives, and identifying the controls that mitigate these risks.

127. Management should select a framework (criteria) for evaluating the effectiveness of controls at the service organization. Because the purpose of a SOC 1® report is to report on controls at a service organization that are relevant to user entities' ICFR, most service organization will use the COSO framework to evaluate its controls. The COSO framework also provides guidance for designing, implementing, and establishing internal control.

128. The 2013 COSO framework indicates that risk assessment "involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed." It further indicates that managing risks involves developing strategies including the design, implementation, and operation of appropriate control activities.

129. To properly assess the risks, the risk assessment should be conducted by appropriate levels of management with sufficient knowledge and understanding of the service organization's business, its organization, operations, and processes. The risk assessment should also be performed annually and when there have been significant changes in processes, risks and controls. Examples of significant changes include changes in technology, key personnel, and the scope of services.

Illustrative Approach to the Risk Assessment Process

130. As management develops the description of the service organization's system, the first thing to be considered are the business processes that make up the services provided. Through discussions with the process owners and observations of the processes, management should gain a sufficient understanding of the process activities and flow of data from initiation to reporting. This will be needed to document the description of the system and define the control objectives. The understanding of the process should include the activities used to identify and prevent errors, the process for correcting errors, and any overrides to the control activities that could take place. For each of these objectives, management should then determine the risks of achieving the objectives (identifying the "what could go wrongs") and the control activities that manage these risks. How management performs its risk assessment will vary. The following is one method of doing so.

Step 1: Identifying the Risks

131. Using the control objectives identified by management, identify the risks that could prevent the achievement of the control objective, including fraud risks and risks related to the completeness and accuracy of the reports used in the process and controls. Risks should be specific and clear so that management can effectively design controls that are appropriately responsive to that particular risk and evaluate the controls.

Step 2: Calculating the Level of Inherent Risk

132. Inherent risk is what could go wrong if there were no controls at the service organization. Inherent risk is a function of (*a*) the likelihood that an event (what could go wrong) will occur and (*b*) the effect the event would have if it did occur. The combination of these two results in the total inherent risk level. This is generally the worst-case scenario for risk because it does not consider any mitigating controls at this point.

Step 3: Describing Controls and Evaluating the Design of Controls

133. When identifying the controls, management should determine whether the controls are preventive, detective, monitoring, manual, automated, or computer dependent. If they are management review controls, what reports are used in the execution of the control, and how does management know that the reports used are complete and accurate? Examples of controls include

- authorization of transactions;
- management review and approval;
- reconciliation;
- safeguarding assets;
- implementation of access security; and
- separation of duties.

Management review controls are often key controls and include

- reviews of exception reports;
- reports that analyze variances;
- detailed calculations performed by the process owners; and
- reports containing management estimates or judgments.

134. It is important to note that some controls will address a single risk and others will address a number of risks. When identifying controls, it is also important to make a distinction between processes and controls. A *process* refers to activities that happen from the initiation of the transaction until the transaction is recorded and reported in the user entities' financial statements. *Controls* refer to activities put in place by management of the service organization to mitigate risks that may affect the transaction and result in an error. Generally, the processes and controls are performed by different individuals.

135. Consideration should also be given to whether the controls are dependent upon other controls, such as those that rely on IT general controls for the completeness and accuracy of the data used in the performance of the control.

136. Management also should try to determine the types of assertions that would commonly be found in user entities' financial statements that would be affected by controls at the service organization (for example, controls at a service organization that processes accounts receivable and ages them for user entities will affect the accuracy of accounts receivable and the allowance for doubtful accounts in user entities' financial statements). Appendix D, "Financial Statement Assertions and Risks That Threaten the Achievement of the Service Organization's Control Objectives," contains more detailed information about financial statement assertions.

137. Once the controls are identified, they will need to be analyzed to determine if collectively the design of the controls is adequate to address the identified risks. If not, gaps in control should be identified and remediated before a SOC 1® engagement is undertaken.

Step 4: Testing the Operating Effectiveness of Controls and Evaluating the Results

138. In a type 2 engagement, management provides an assertion about whether the controls are operating effectively. To provide support for that assertion, management may consider performing tests of the controls during the examination period. Tests may be performed on a representative sample of the transactions to which the control is applied, and the tests performed and results of the tests should be documented so that an independent review can take place. Management may also set up a process to monitor its controls on an ongoing basis through ongoing monitoring activities, which are often built into the normal recurring activities of an entity. Internal auditors or personnel performing similar functions may contribute to the monitoring of a service organization's controls. Monitoring activities may also include using information communicated by external parties, such as customer complaints which may indicate problems or highlight areas in need of improvement. The greater the degree and effectiveness of ongoing monitoring, the less need for separate evaluations. Usually, some combination of ongoing monitoring and separate evaluations will ensure that internal control maintains its effectiveness over time. (The service auditor's report on controls is not a substitute for the service organization's own processes to provide a reasonable basis for its assertion.)

139. If management determines that a control is not operating effectively, management should analyze the ineffective control to determine whether it can be remediated for use in future periods and whether there are other controls that are sufficient to mitigate the risk. Such controls should be included in the description of the service organization's system and should be tested. Controls that do not operate effectively cannot be used as mitigating controls.

Step 5: Analyzing the Controls

140. Once the controls have been mapped to the risks and tested, management should analyze the controls to determine if they mitigate the risks sufficiently to achieve the control objectives. The characteristics of the controls, particularly the financial statement assertions that are addressed will help determine if the controls are sufficient or if some of the controls are duplicative and unnecessary. In evaluating the design of a control, management should also consider whether the control, individually or in combination with other controls, can effectively prevent, or detect and correct, material misstatements. Based on this analysis, management will determine how effective the control is in mitigating the risk.

Step 6: Calculating Residual Risk

141. The residual risk is the level of risk remaining after factoring in all the controls that are operating effectively. It is determined by taking the inherent risk level and subtracting the strength of the controls that mitigate the particular risk. A tolerable residual risk should be determined by management and each risk measured against that tolerance. If the residual risk is not within tolerance, management should consider designing additional controls or making sure that existing controls are operating effectively.

Reporting

Reporting

Finalizing Management's Description and Assertion

142. As previously stated in this guide, management is responsible for the description of the service organization's system and its assertion. Prior to providing a final assertion, management should perform, a final review of the description to ensure the following:

a. The description is fairly presented, and information in the description is accurate, complete, measurable, and relevant.

b. Changes in the system during the period are accurately reflected.

c. The system covered by the report, and the dates that identify the period covered by the report are accurate and consistent throughout the document.

d. Other statements in the description are accurate, complete, measurable, and relevant.

143. Management should also review the section that includes the service auditor's tests of the operating effectiveness of controls and results to ensure that the control objectives and description of controls are accurate, and to fully understand the nature of the testing and the nature of any exceptions noted by the service auditor.

144. If the service auditor noted exceptions during the testing of controls, management may include a response to those exceptions. Such responses must be factual and should focus on the root cause of the exception and what management has done, or plans to do, to address the root cause. If the response includes forward-looking statements such as statements about plans for future remediation activities, they should be presented in a section labeled “Other Information Provided by the Service Organization.”

145. Management is responsible for any information that is presented in a section labeled, “Other Information Provided by the Service Organization.” This section is specifically excluded from the service auditor’s opinion but may include relevant information for readers of the report. Management may choose to include in this section such items as responses to identified exceptions, including its remediation plans; forward-looking statements regarding new product releases or future changes to the services covered by the scope of the report; or information regarding topics not directly relevant to user entities’ ICFR (for example, business continuity or disaster recovery plans).

146. In addition, management should ensure that the information in this section is accurate and consistent with management’s description and assertion. Although such information will not be covered by the service auditor’s opinion, the service auditor may not permit its inclusion if the service auditor believes the information is misleading or otherwise inappropriate for inclusion in the SOC 1® report.

Reading and Understanding the Service Auditor’s Report

147. Prior to providing a final assertion, management should also discuss with the service auditor whether the service auditor intends to issue a modified SOC 1® opinion. If the service auditor’s opinion will be modified, management should understand the reason for the modification. Possible modifications include a disclaimer of opinion (no opinion), a scope limitation, and a qualified or adverse opinion if certain control objectives were not achieved. Management should also discuss whether it needs to incorporate similar modifications in its assertion.

Preparing Written Representations

148. Like the requirement for the service organization to provide a written assertion, AICPA professional standards require the service auditor to request from management of the service organization a written representation at the conclusion of the engagement. Such written representations are requested by the service auditor from service organization management in the form of a signed letter addressed to the service auditor.

149. Because service organization management typically makes many oral and written representations to the service auditor in response to specific inquiries during the engagement or through presentation of the description and management’s assertion, the written representation letter at the conclusion of the examination ordinarily confirms the representations explicitly or implicitly given to the service auditor by service organization management during the examination. Additionally, such written representations also indicate and document the continuing appropriateness of such representations made by service organization management during the examination and reduce the possibility of a misunderstanding concerning matters that are the subject of the representations.

150. Typically, during the planning phase of the engagement, the service auditor will coordinate with service organization management to determine who will sign the representation letter at the conclusion of the engagement. Generally, those service organization management personnel responsible for the subject matter of the examination will be requested to sign the representation letter. In addition, in certain circumstances, the service auditor may obtain written representations from other parties in addition to management of the service organization, such as those charged with governance.

151. Written representations are separate from and in addition to the assertion that accompanies management’s description of the service organization’s system and should be dated as the same date of the service auditor’s report. Also, because management’s written representations are an important consideration when forming the service auditor’s opinion, the service auditor would not ordinarily be able to issue the service auditor’s report until the service auditor has received the representation letter.

152. Management should be aware that failure to provide the representation letter to the service auditor constitutes a limitation on the scope of the examination sufficient to preclude the service auditor from issuing an unmodified opinion and may be sufficient to cause the service auditor to withdraw from the engagement.

153. Finally, when the service organization uses the inclusive method with respect to a subservice organization used by the entity, the service auditor is also required to request a written representation letter from subservice organization management. If the service auditor is unable to obtain written representations regarding relevant control objectives and related controls at the subservice organization, management of the service organization may not use the inclusive method but, in certain circumstances, may be able to use the carve-out method.

154.

Appendix A: Illustrative Outline for a Description of the Service Organization’s System

Management of the service organization is responsible for preparing the description of the service organization’s system, including the completeness, accuracy, and method of presentation of the description. The description of the service organization’s system is intended to provide user entities and their auditors with information about the service organization’s system that is relevant to the user entities’ internal control over financial reporting (ICFR).

The following is a suggested outline for use in preparing a description of the service organization’s system in a type 1 or type 2 report.

1. Overview of the Service Organization

Provides an overview of the service organization and the types of services provided by the entity.

2. Scope of the Description

Provides a brief description of the scope of the system description including services provided within the scope of the description, and whether subservice organizations are used in the delivery of the services provided by the service organization as well as the related services provided by the subservice organizations.

3. Internal Control Framework

AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting,*[8] requires the service organization’s description to include other aspects of the service organization’s internal control components (control environment, risk assessment process, information and communications, monitoring activities, and control activities). The attestation standards are not based on a specific internal control framework, and management of the service organization may use the COSO framework or other suitable and available internal control framework. The following outline identifies the 5 components and the 17 principles of the 2013 COSO framework.

A. Control Environment

Describes at a high level how the service organization achieves the principles of COSO and how the control environment sets the tone of the service organization, influencing the

[8] All AT-C sections can be found in AICPA *Professional Standards*.

control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. It describes how the entity

1. demonstrates commitment to integrity and ethical values;
2. exercises oversight responsibility;
3. establishes structure, authority, and responsibility;
4. demonstrates commitment to competence; and
5. enforces accountability.

B. Risk Assessment

Identifies and analyzes aspects of the service organization’s risk assessment process that may affect the services provided to user entities including how management addresses risks that could affect the achievement of the control objectives as well as the financial reporting of the user entities. It describes how the entity

1. specifies suitable objectives;
2. identifies and analyzes risk;
3. assesses fraud risk; and
4. identifies and analyzes significant changes (for example, regulatory, environmental, and technology changes).

C. Information and Communications

Describes how the entity communicates relevant policies and procedures internally and externally. Describes the information systems (application systems and related hardware) used by the service organization in delivery of its services including those automated or manual to initiate, authorize, record, process, and report user entity transactions. It describes how the entity

1. uses relevant quality information;
2. communicates internally; and
3. communicates externally.

D. Monitoring Activities

Describes how the entity monitors the effectiveness of controls and services provided to user entities including any deficiency in controls. It also describes how the entity monitors the activities of any subservice organizations used in the delivery of services to user entities. It describes how the entity

1. conducts ongoing or separate evaluations, or both and
2. evaluates and communicates deficiencies.

E. Control Activities

Describes the procedures, within both automated and manual systems, by which services are provided and transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information for user entities of the system. It describes how the entity

1. selects and develops control activities;
2. selects and develops general controls over technology; and
3. deploys control activities through policies and procedures.

This section describes the control activities related to the delivery of services to and transaction processing for the user entities of the system. The control activities are typically grouped by control objective area (control objectives are not typically described here and are instead listed in section 4 of the type 1 or type 2 report).

Transaction Processing

1. New plan setup and maintenance (control objective 1)[9]

2. Enrollments and changes (control objective 2)

3. Contributions (control objective 3)

4. Distributions (control objective 4)

5. Investments and related transactions (control objective 5)

6. Pricing (control objective 6)

7. Investment income (control objective 7)

8. Corporate actions (control objective 8)

9. Reconciliations (control objective 9)

10. Statements (control objective 10)

IT General Controls

11. Logical security (control objective 11)

12. Change management – Application programs and data base management systems (control objective 12)

[9] The control objectives in this example are for a custodian and would need to be customized for the actual services performed.

13. Change management – Network infrastructure (control objective 13)

14. Computer operations (control objective 14)

15. Data transmissions (control objective 15)

16. Physical security (control objective 16)

17. Data and system backup (control objective 17)

Complementary User Controls (CUECs)

This section identifies and describes the complementary user entity controls that management assumes will be implemented by user entities and that are necessary to achieve the control objectives. In addition, the CUECs are typically linked to each relevant control objective.

Complementary Subservice Organization Controls (CSOCs)

This section identifies and describes the CSOCs that management assumes will be implemented by subservice organizations and that are necessary to achieve the control objectives. In addition, the CSOCs are typically linked to each relevant control objective.

155.

Appendix B: Illustrative Assertion by Management of the Service Organization

Management of the service organization is required to provide the service auditor with a written assertion about the matters covered in the service auditor's report. The service organization has the option of attaching the assertion to the description of the service organization's system or including it in the description and clearly segregating the assertion from the description (for example, using headings). Segregating the assertion from the description clarifies that the assertion is not part of the description.

The following illustrative management assertion contains text in boldface italics that would be added to management's assertion if the situation described in the text is applicable. This illustrative assertion is for guidance only and is not intended to be exhaustive or applicable to all situations.

Illustrative Assertion by Management of a Service Organization for a Type 2 Report

XYZ Service Organization's Assertion

We have prepared the description of XYZ Service Organization's [*type or name of*] system entitled, "XYZ Service Organization's Description of Its [*type or name of*] System," for processing user entities' transactions [*or identification of the function performed by the system*] throughout the period [*date*] to [*date*] (description) for user entities of the system during some or all of the period [*date*] to [*date*], and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, ***including information about controls implemented by subservice organizations and user entities of the system themselves,*** when assessing the risks of material misstatement of user entities' financial statements.

[*A statement such as the following is added to the assertion when the service organization uses a subservice organization, the carve-out method is used to present the subservice organization, and complementary subservice organization controls are required to meet the control objectives.*]

XYZ Service Organization uses a subservice organization to **[identify the function or service provided by the subservice organization].** ***The description includes only the control objectives and related controls of XYZ Service Organization and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.***

[*A statement such as the following is added to the service auditor's report when complementary user entity controls are required to meet the control objectives.*]

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the [*type or name of*] system made available to user entities of the system during some or all of the period [*date*] to [*date*] for processing their transactions [*or identification of the function performed by the system*] as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,

   (1) the types of services provided, including, as appropriate, the classes of transactions processed;

   (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system;

   (3) the information used in the performance of the procedures including, if applicable, related accounting records (whether electronic or manual) and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

   (4) how the system captures and addresses significant events and conditions other than transactions;

   (5) the process used to prepare reports and other information for user entities;

   (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;

   (7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and CSOCs assumed in the design of the service organization's controls; and

   (8) other aspects of our control environment, risk assessment process, information

and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to the service organization’s system during the period covered by the description; and

iii. does not omit or distort information relevant to the service organization’s system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and therefore may not include every aspect of the [type or name of] system that each individual user entity of the system and its auditor may consider important in its own particular environment; and

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period [*date*] to [*date*] to achieve those control objectives ***if subservice organizations and user entities applied the complementary controls assumed in the design of XYZ Service Organization’s controls throughout the period* [date] *to* [date]**. The criteria we used in making this assertion were that

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization;

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

156

Appendix C: Types of Financial Statement Assertions in User Entities' Financial Statements and Risks That Threaten the Achievement of the Service Organization's Control Objectives

The control objectives stated in management's description of the service organization's system should be reasonable in the circumstances. Control objectives are reasonable in the circumstances when they "relate to the types of assertions commonly embodied in the broad range of user entities' financial statements to which controls at the service organization could reasonably be expected to relate."

The following tables present the types of assertions that may exist in a user entity's financial statements, illustrative service organization control objectives that relate to those types of assertions, and the risks that threaten the achievement of those control objectives. There are separate tables for transactions and events during the period (table 1) and for account balances as of the end of the period (table 2). Because the control objectives in the tables are illustrative, they would need to be tailored to the specific facts and circumstances of the service organization.

Table 1 presents the categories of assertions that may exist in a user entity's financial statements and that may be affected when the service provided by the service organization involves processing transactions and recording events for user entities.[10]

[10] If the services provided by the service organization include preparation of user entity financial statements, the following user entity assertions about presentation and disclosure may also be relevant:

- *Occurrence and rights and obligations*. Disclosed events, transactions, and other matters have occurred and pertain to the entity.
- *Completeness*. All disclosures that should have been included in the financial statements have been included.
- *Classification and understandability*. Financial information is appropriately presented and described, and disclosures are clearly expressed.
- *Accuracy and valuation*. Financial and other information is disclosed fairly and at appropriate amounts.

Table 1. Types of Financial Statement Assertions[11] About Classes of Transactions and Events During a Period, Related Service Organization Control Objectives, and Risks That Threaten the Achievement of the Control Objectives

User Entity Financial Statement Assertions	**Illustrative Service Organization Control Objectives** Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks[12] That Threaten the Achievement of the Control Objectives As They Relate to the User Entities' Financial Statements**
Occurrence. Transactions and events that have been recorded have occurred and pertain to the entity.	• Transactions are authorized and received only from authorized sources.[13] • Transactions are validated[14] in a complete, accurate, and timely manner.[15]	Unauthorized transactions are entered and not detected. For example, manual transactions are not reviewed and approved by authorized individuals, or transactions are entered by unauthorized individuals. Invalid transactions are entered and not detected. For example, duplicate transactions are entered. Entered transactions are not validated against master data and other management authorization criteria. For example, automated transactions are not validated against master data, or transactions that do not correspond with master data are not rejected. Transactions are incorrectly attributed to the entity. Transactions are incorrectly processed so that invalid transactions are recorded (for example, recorded as a result of a logic error in the application). Transaction reports provided to user entities inappropriately accumulate transactions. For example, transaction reports include invalid transactions or information that is inconsistent with the transaction detail maintained by the service organization.

[11] Paragraph .A114 of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement,* in AICPA *Professional Standards*.

[12] The risks that threaten the achievement of the service organization's control objectives are dependent on the unique facts and circumstances of the service organization.

[13] Transaction data may be received in paper or electronic form or by telephone (for example, by a call center). The service organization may have separate control objectives for each method of receipt.

[14] Validation includes determining that the recorded transaction has occurred and pertains to the user entity. It also includes correcting invalid data and properly reentering corrected data.

[15] A timely manner also includes recording the transaction in the correct period.

User Entity Financial Statement Assertions	**Illustrative Service Organization Control Objectives** Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks[12] That Threaten the Achievement of the Control Objectives As They Relate to the User Entities' Financial Statements**
		Master data are inaccurate or incomplete. Unauthorized or invalid transactions are entered as a result of compromises in IT general controls. Physical media needed to process a transaction are not properly controlled. For example, blank checks are stolen; and improper, unauthorized checks are issued.
Completeness. All transactions and events that should have been recorded have been recorded.	• Transactions are entered, processed, recorded, and reported in a complete manner.	All authorized and valid transactions are not recorded. For example, transactions are incorrectly rejected, are not properly reentered, are not entered on a timely basis, or are recorded in the accounts of the wrong entity. Applications incorrectly process transactions so that all authorized and valid transactions are not recorded. For example, all transactions are not processed, processing is incomplete, or programming logic is incorrect. Transaction reports provided to user entities inappropriately accumulate valid and authorized transactions. For example, valid transactions are excluded, or reported information is inconsistent with transaction detail maintained by the service organization. Authorized and valid transactions are not recorded or reported as a result of compromises in IT general controls.
Accuracy. Amounts and other data relating to recorded transactions and events have been recorded appropriately.	• Transactions are entered, processed, recorded, and reported in an accurate manner.	Inaccurate or incomplete amounts or other relevant transaction data are entered and not detected. For example, expected transaction data are missing, do not match expected field values, or do not fall within predetermined limits. Master data are inaccurate or incomplete. Applications process transactions incorrectly, so that transactions contain

User Entity Financial Statement Assertions	**Illustrative Service Organization Control Objectives** Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks[12] That Threaten the Achievement of the Control Objectives As They Relate to the User Entities' Financial Statements**
		inaccurate amounts or inaccuracies in other relevant transaction data. For example, a logic error in the application results in incorrect programmed calculations. Transaction reports provided to user entities inappropriately accumulate transactions. For example, reports include transactions containing inaccurate amounts or inaccuracies in other relevant data. Inaccurate or incomplete amounts or other relevant data are recorded or reported as a result of compromises in IT general controls.
Cutoff. Transactions and events have been recorded in the correct accounting period.	- Transactions are entered, processed, recorded, and reported in a timely manner.[16]	The incorrect period is entered for the transaction or the period is omitted and is not detected. Applications process transactions incorrectly so that transactions are recorded or reported in an incorrect period, for example, as a result of a logic error in the application. Transactions are recorded or reported in the wrong period as a result of compromises in IT general controls. Entered transactions are not validated in a timely manner.
Classification. Transactions and events have been recorded in the proper accounts.	- Transactions are recorded and reported in the proper accounts. *Note*: Entering, processing, recording, and reporting transactions in a complete, accurate, and timely manner includes appropriate classification to facilitate proper reporting by the user entity.	An incorrect account is entered for a transaction and is not detected. Applications process transactions incorrectly, so that transactions are recorded in the wrong account (for example, as a result of a logic error in the application). Transaction reports provided to user entities inappropriately accumulate transactions,

[16] Ibid.

User Entity Financial Statement Assertions	**Illustrative Service Organization Control Objectives** Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks[12] That Threaten the Achievement of the Control Objectives As They Relate to the User Entities' Financial Statements**
		resulting in transactions being reported in the wrong accounts. Transactions are classified in the wrong accounts as a result of compromises in IT general controls.

Table 2. Types of Financial Statement Assertions About Account Balances at the Period End, Related Service Organization Control Objectives, and Risks That Threaten the Achievement of the Control Objectives

User Entity Financial Statement Assertions	**Illustrative Service Organization Control Objectives** Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks That Threaten the Achievement of the Control Objectives As They Relate to the User Entities' Financial Statements**
Existence. Assets, liabilities, and equity interests exist.	• Balances represent valid asset, liability, and equity interest balances and are classified properly.	Invalid transactions are recorded or reported in the account balance. Recorded or reported balances include valid transactions that should be recorded in another account. Balances do not reconcile to subsidiary detail (for example, because reconciliations are not performed or are not properly performed). Proper adjustments for reconciling items are not recorded or are not recorded in a timely manner. Recorded adjustments to account balances are not authorized and approved. Master data are inaccurate or incomplete. Unauthorized or invalid transactions are recorded in account balances as a result of compromises in IT general controls.
Rights and obligations. The entity holds or controls the rights to assets, and liabilities are the obligations of the entity.	• Asset and liability balances relate to rights or obligations of the user entity.	User entity asset or liability balances include balances that are not rights and

User Entity Financial Statement Assertions	**Illustrative Service Organization Control Objectives** Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks That Threaten the Achievement of the Control Objectives As They Relate to the User Entities' Financial Statements**
		obligations of the user entity (for example, the balances pertain to another entity). Master data are inaccurate or incomplete. User entity assets or liabilities are improperly recorded as a result of compromises in IT general controls.
Completeness. All assets, liabilities, and equity interests that should have been recorded have been recorded.	• Balances represent all asset, liability, and equity interest balances that should have been recorded.	Recorded or reported balances do not include all valid transactions (for example, account numbers are invalid, or transactions are incorrectly recorded in another account). Balances do not reconcile to subsidiary detail (for example, because reconciliations are not performed or are not properly performed). Proper adjustments for reconciling items are not recorded or are not recorded in a timely manner. Not all authorized or approved adjustments to account balances are recorded. Master data are inaccurate or incomplete. Not all valid transactions are recorded or reported in account balances as a result of compromises in IT general controls.
Valuation and allocation. Assets, liabilities, and equity interests are included in the financial statements at appropriate amounts, and any resulting valuation or allocation adjustments are appropriately recorded.	• Asset, liability, and equity interest balances are reported at accurate amounts.	Balances are recorded or reported at inaccurate amounts. Amounts for valid transactions are not properly or completely summarized in the recorded or reported account balance. Valuation or allocation calculations are not properly performed. Valuation or allocation adjustments are not recorded or reported accurately and in a timely manner. Balances do not reconcile to subsidiary detail (for example, because reconciliations

User Entity Financial Statement Assertions	Illustrative Service Organization Control Objectives Controls provide reasonable assurance that the following control objectives are achieved:	Illustrative Risks That Threaten the Achievement of the Control Objectives As They Relate to the User Entities' Financial Statements
		are not performed or are not properly performed). Proper adjustments for reconciling items are not recorded or are not recorded in a timely manner. Adjustments to recorded account balances are not authorized or approved. Authorized and approved adjustments to account balances are not recorded. Master data are inaccurate or incomplete. Balances and underlying transactions are not properly valued or allocated as a result of compromises in IT general controls.

157.

Appendix D: Illustrative Control Objectives for Various Types of Service Organizations

This appendix illustrates typical control objectives related to the following:

- General business processes
- IT general controls
- Specific types of service organizations, including
  - — application service providers,
  - — claims processors,
  - — credit card payment processors,
  - — defined contribution plan recordkeepers,
  - — investment managers,
  - — payroll processors, and
  - — transfer agents.
- Custodians subject to SEC Rule 206(4)-2, "Custody of Funds or Securities of Clients by Investment Advisers"

The illustrative control objectives in this appendix are not meant to be all-encompassing. Rather, they represent typical control objectives included in descriptions of a service organization's system for service organizations that provide the services listed in the preceding paragraph; these control objectives should be tailored to the particular service organization's business. Additionally, the service organization should review the entire appendix before determining which control objectives best fit its needs. For example, control objectives for transaction processing are presented in a number of ways in this appendix.

To assist the service organization in identifying applicable control objectives the appendix contains footnotes designed to further explain and clarify the control objectives as written.

Illustrative General Business Process Control Objectives

The illustrative control objectives in this section generally are applicable to many types of service organizations. These control objectives are discussed in Table 2 of this guide along with the related user entity financial statement assertions and illustrative risks that threaten the achievement of the control objectives as they relate to the user entities' financial statements. The control objectives would be tailored to the facts and circumstances of the service organization and the particular business process service being provided to user entities.

Application Control Objectives Related to Transactions and Events During a Period

Controls provide reasonable assurance that the following control objectives are achieved:

- Transactions are authorized and received only from authorized sources.[17]
- Transactions are validated[18] in a complete, accurate, and timely manner.[19]
- Transactions are entered, processed, recorded, and reported in a complete manner.
- Transactions are entered, processed, recorded, and reported in an accurate manner.
- Transactions are entered, processed, recorded, and reported in a timely manner.[20]
- Transactions are recorded and reported in the proper accounts.

Application Control Objectives Related to Account Balances at the Period End

Controls provide reasonable assurance that the following control objectives are achieved:

- Balances represent valid asset, liability, and equity interest balances and are classified properly.
- Asset and liability balances relate to rights or obligations of the user entity.
- Balances represent all asset, liability, and equity interest balances that should have been recorded.
- Asset, liability, and equity interest balances are reported at accurate amounts.

Control Objectives Related to IT General Controls

The illustrative control objectives in this section are applicable to IT general controls and are discussed in appendix E of this guide, along with the related illustrative risks that threaten the achievement of the IT general control objectives. IT general control objectives can be used alone or in combination with the business process control objectives, depending on the nature of the outsourced service. The service organization tailors these control objectives to the services provided, selecting control objectives that are likely to be relevant to controls over financial reporting at user entities.

Illustrative Control Objectives

Information Security

Controls provide reasonable assurance that the following control objectives are achieved:

[17] Transaction data may be received in paper or electronic form or by telephone, for example, by a call center. The service organization may have separate control objectives for each method of receipt.

[18] Validation includes determining that the recorded transaction has occurred and pertains to the user entity. It also includes correcting invalid data and properly reentering corrected data.

[19] A timely manner also includes recording the transaction in the correct period.

[20] See footnote 3.

- Logical access[21] to programs, data, and computer resources[22] relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.[23]
- Physical access to computer and other resources[24] relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate personnel.

Change Management

Controls provide reasonable assurance that the following control objectives are achieved:

- Changes to application programs and related data management systems[25] are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely[26] processing and reporting of transactions and balances relevant to user entities' internal control over financial reporting.[27]
- Network infrastructure[28] is configured as authorized to
  - support the effective functioning of application controls to result in valid, complete,

[21] In assessing the logical access controls over programs, data, and computer resources, the service organization considers

- logical access controls that may affect the user entities' financial statements. Generally, this would begin with the access controls directly over the application. If the effectiveness of application level security is dependent on the effectiveness of network and operating system controls, these are also considered. Controls over direct access to the databases or data files and tables are considered as well.
- the configuration and administration of security tools and techniques and monitoring controls designed to identify and respond to security violations in a timely manner.

[22] Computer resources include, but are not limited to, computer equipment, network equipment, storage media, and other hardware supporting the services provided by the service organization.

[23] Many service organizations have features enabling customers to directly access programs and data. In assessing the logical access controls over programs and data, the service organization considers the controls over security related to service organization personnel, the service organization's customers, and the customers' clients, as applicable, as well as the likely effect of these controls on user entities' financial statements.

[24] Computer resources include, but are not limited to, computer equipment, network equipment, storage media, and other hardware supporting the services provided by the service organization. Other resources include, but are not limited to, buildings, vaults, and negotiable instruments.

[25] Data management systems include database management systems, specialized data transport or communications software (often called middleware), data warehouse software, and data extraction or reporting software. Controls over data management systems may enhance user authentication or authorization, the availability of system privileges, data access privileges, application processing hosted within the data management systems, and segregation of duties.

[26] Timeliness may be relevant in particular situations, for example, when emergency changes are needed or when changes that would likely affect the user entities' information system are being implemented to meet contractual requirements. Controls for emergency changes typically will be different from those for planned changes.

[27] This control objective is quite broad and should be tailored to the service organization's environment. For example, if the service organization has different controls for developing new applications or for making changes to applications or databases, it might be clearer to have separate control objectives for each of these.

[28] Network infrastructure includes all the hardware, software, operating systems, and communication components within which the applications and related data management systems operate.

accurate, and timely[29] processing and reporting of transactions and balances relevant to user entities' internal control over financial reporting;

- protect data relevant to user entities' internal control over financial reporting from unauthorized changes; and
- support user entities' internal control over financial reporting.[30]

Computer Operations

Controls provide reasonable assurance that the following control objectives are achieved:

- Application and system processing[31] relevant to user entities' internal control over financial reporting are authorized and executed in a complete, accurate, and timely manner and deviations, problems, and errors that may affect user entities' internal control over financial reporting are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.
- Data transmissions between the service organization and its user entities and other outside entities that affect user entities' internal control over financial reporting are from authorized sources and are complete, accurate, secure, and timely.[32]
- Data relevant to user entities' internal control over financial reporting is backed up regularly and is available for restoration in the event of processing errors or unexpected processing interruptions.

Illustrative Control Objectives for an Application Service Provider

In addition to the illustrative control objectives in this section, the control objectives in the preceding section, "Control Objectives Related to IT General Controls," may be appropriate for an ASP.[33] An ASP may perform some or all of the following services for user entities:

[29] Timeliness may be relevant in particular situations, for example, when emergency changes are needed or when changes are being implemented to meet contractual requirements.

[30] Program change controls over network infrastructure include, as appropriate, the authorization, testing, documentation, approval, and implementation of changes to network infrastructure. In assessing change management, the service organization considers the configuration and administration of the security tools and techniques, and monitoring controls designed to identify exceptions to authorized network infrastructure applications and data management systems (for example, database structures) and act upon them in a timely manner. If the service organization has different controls for new implementations or for making changes to either the infrastructure, applications, or data management systems, it might be clearer to have separate control objectives that address the controls over each type of infrastructure. There also may be separate control objectives for controls over new implementations and controls over changes to existing resources.

[31] The processing in this control objective refers to the batch processing of data. It typically does not include scheduling of file backups. Should the service organization have significant online, real-time processing, it may tailor this control objective or add a new control objective to address controls over the identification, tracking, recording, and resolution of problems and errors in a complete, accurate, and timely manner.

[32] This control objective may also be presented as part of logical access security or as part of the business operations related to data input or reporting.

[33] An application service provider (ASP) may provide software for functions, such as credit card payment processing or timesheet services, or may provide a particular financial application or solution package for a specific type of customer, such as a dental practice.

- Providing a commonly used application that is accessed using an internet protocol such as HTTPS or a web browser
- Maintaining and operating the application software on behalf of its clients
- Owning, operating, and maintaining the servers that support the software
- Billing the ASP's clients on a "per use" basis

Illustrative Control Objectives

New Customer Setup and Maintenance

Controls provide reasonable assurance that the following control objectives are achieved:

- New customers are established on the system in accordance with the applicable contracts and requirements.[34]
- Maintenance instructions[35] are properly authorized, recorded completely and accurately, and processed timely.

Transaction Processing

Controls provide reasonable assurance that the following control objectives are achieved:

- Client transactions are initially recorded completely, accurately, and in a timely manner.
- Invalid transactions and errors are identified, rejected, and correctly reentered into the system in a timely manner.
- Client transactions are processed in a timely manner and reported in accordance with client-specific business rules.
- The contents of data files remain complete and accurate, and the correct versions of all data files are used in processing.[36]

Customer Support

Controls provide reasonable assurance that the following control objectives are achieved:

- Production and business problems[37] are identified, recorded, analyzed, and resolved completely and in a timely manner.

[34] Because most ASPs provide a service that is flexible and can be tailored to a particular customer, it is important that a new customer's business rules be properly established on the system to ensure that processing of its data are in accordance with expectations and requirements.

[35] Maintenance instructions are required to make changes to customer information.

[36] This control objective includes controls in place to ensure that the correct versions of the files are used to validate and update transactions entered for processing. This control objective can be used as a control objective related to any transaction processing. The service organization determines the nature and extent of the control objective and whether the control objective belongs with the business process controls or with the IT general controls, based on the services provided and the relevance of these controls to the preparation of financial statements.

[37] *Production and business problems* refer to the issues encountered by user entities, the computer systems that support the services, or the general business questions user entities may have regarding the services rendered.

- System availability is monitored, and issues are identified and resolved on a timely basis.

Illustrative Control Objectives for a Claims Processor

The illustrative control objectives in this section may be appropriate for a service organization that processes claims for user entities such as health insurers. The claims processor may perform some or all the following services for user entities:

- Maintaining eligibility and enrollment information for customers
- Processing claims, such as insurance or medical benefit claims, on behalf of customers of the user entities based on contractual arrangements
- Adjudicating claims on behalf of their customers
- Processing bills to customers

Illustrative Control Objectives

Groups or Customers[38]

Controls provide reasonable assurance that group and benefits contracts[39] are authorized and that contract terms are established[40] and maintained in a complete, accurate, and timely manner.

Providers

Controls provide reasonable assurance that provider contracts are authorized, and provider data are established[41] and maintained in a complete, accurate, and timely manner.

Enrollments[42]

Controls provide reasonable assurance that enrollment and eligibility information received from customers is authorized and processed in a complete, accurate, and timely manner.

Claims Receipts and Adjudication[43]

[38] Group or customer information would include information such as member benefits, global pricing, and reimbursement schedules.

[39] Group and benefits contracts may refer to physician, dental, and other health care provider agreements.

[40] Establishing this information in the application software may also be referred to as installation of the group and customer information.

[41] Establishing this information in the application software may also be referred to as installation of the provider information.

[42] Enrollment information may be received through various channels either electronically via fax, Internet, or specific feeds or as a hard copy. If the controls for each channel are different, the service organization should consider establishing individual control objectives for each channel.

[43] Claims may be received in paper or electronic format. The service organization may establish separate control objectives for each method of receipt, depending on the control activities and the needs of the user entities.

Controls provide reasonable assurance that the following control objectives are achieved:

- Claims are received only from authorized sources.
- Claims received are entered in a complete, accurate, and timely manner.
- Claims are validated and adjudicated in a complete, accurate, and timely manner.
- Claim adjustments are authorized and processed in a complete, accurate, and timely manner.
- Claim actions for subrogation, coordination of benefits, and other recoveries for submitted claims are processed in a complete, accurate, and timely manner.[44]

Claim Payments and Billing Operations

Controls provide reasonable assurance that the following control objectives are achieved:

- Adjudicated claims are paid in a complete, accurate, and timely manner.
- Customer invoices and funding requests are authorized and processed in a complete, accurate, and timely manner.
- Reports provided to customers are complete, accurate, and timely.

Illustrative Control Objectives for a Credit Card Payment Processor

The illustrative control objectives in this section may be appropriate for a service organization that processes credit card payments. The credit card payment processor may perform some or all of the following services for user entities:

- Processing transactions initiated by credit card holders at authorized merchants
- Paying merchants for authorized credit card transactions
- Preparing and managing cardholder invoices and payments
- Managing and reporting potential fraudulent transactions
- Managing blank cards and personal identification numbers
- Reporting to the merchants and credit bureaus
- Managing rewards programs

Illustrative Control Objectives

Merchant and Sales Partner Setup

Controls provide reasonable assurance that the following control objectives are achieved:

- New merchant accounts are authorized and set up completely and accurately, according to the contractual agreement.
- New sales partners are authorized and set up completely and accurately, according to the contracted agreement.

[44] This control objective should include controls over the collection and payment to the appropriate parties of any funds recovered. In such cases, the service organization may consider a separate control objective for these controls.

- Changes to merchant and sales partner data are authorized and processed completely and accurately and in a timely manner.

Authorization Processing

Controls provide reasonable assurance that authorization requests are received, transmitted to the processing system, properly evaluated based on the cardholder's available credit and current account status, and that the authorization or denial message received from the processor is transmitted back to the originating merchant.

Transaction Processing

Controls provide reasonable assurance that the following control objectives are achieved:

- All and only authorized transactions are processed and settled completely, accurately, timely, and only once.
- All data are validated, and errors are rejected and reported for user entity follow-up and correction.
- Transmissions to and from clearinghouses are accurate, complete, and valid.
- The contents of data files remain complete and accurate, and the correct versions of all data files are used in processing.[45]

Chargebacks and Refunds

Controls provide reasonable assurance that all and only authorized chargeback or refund data received is processed and settled completely, accurately, and in a timely manner.

Merchant Payments

Controls provide reasonable assurance that the following control objectives are achieved:

- Amounts payable to merchants are computed completely and accurately and amounts due are transferred to the merchant using the appropriate remittance option.
- Sales partner residual amounts are calculated completely, accurately, and in a timely manner.

Client Settlement

Controls provide reasonable assurance that the following control objectives are achieved:

- The system is in balance prior to settlement with the interchange clearinghouses and the

[45] This control objective includes controls in place to ensure that the correct versions of the files are used to validate and update transactions entered for processing. This can be used as a control objective related to any transaction processing. The service organization determines the nature and extent of the control objective and whether the control objective belongs with the business process controls or the IT general controls, based on the services provided and the relevance of these controls to the preparation of financial statements.

client’s processing, and net settlement amounts are properly computed.

- All outgoing wire transfers are properly authorized and all incoming wire transfers are received accurately and on a timely basis.

Cardholder Accounting

Controls provide reasonable assurance that the following control objectives are achieved:

- Transactions are processed in accordance with system descriptions and posted completely and accurately to the correct cardholder accounts in a timely manner.
- Problem accounts (for example, accounts that exceed limits or are delinquent) are identified by the system and reported to the client for follow-up.

Cardholder Inquiry Management

Controls provide reasonable assurance that cardholder inquiries are logged and processed to permit a timely response to the inquiry or resolution of the problem.

Cardholder Statements and Communication

Controls provide reasonable assurance that cardholder statements are generated on a timely basis and distributed no more than 10 days after statement generation.

Risk Management

Controls provide reasonable assurance that periodic credit reviews, fraud investigations, and collections are routinely performed, monitored, and reported for follow-up on a timely basis.

Rewards

Controls provide reasonable assurance that cardholder rewards processing functions and calculations are performed in accordance with system descriptions and all and only authorized transactions are posted to the correct cardholder account in the proper accounting period.

Blank Cards

Controls provide reasonable assurance that the following control objectives are achieved:

- Blank cards are safeguarded and protected from unauthorized use.
- Blank cards are not lost or duplicated during the personalization process.
- Adjustments to inventory levels are authorized by appropriate individuals.

Personal Identification Numbers

Controls provide reasonable assurance that the following control objectives are achieved:

- Personal identification numbers (PINs) used to authenticate cash advance transactions are protected from unauthorized disclosure.
- Cardholder PINs generated and mailed during the card-issuance process are protected from unauthorized disclosure.
- Access to the information used to produce the PIN mailer, as well as the printed mailers, is restricted to authorized and appropriate individuals.
- Client-defined encryption keys are protected from unauthorized disclosure.

Report Statement Generation and Distribution

Controls provide reasonable assurance that client reports are complete, accurate, and distributed on a timely basis.

Credit Bureau Reporting

Controls provide reasonable assurance that month-end credit bureau reporting files are complete, accurate, and transmitted to the appropriate credit bureaus in the agreed-upon timeframes and in accordance with client specifications.

Illustrative Control Objectives for a Defined Contribution Plan Recordkeeper

The illustrative control objectives in this section may be relevant to a service organization that is a defined contribution plan recordkeeper. Selected control objectives may also be relevant to a defined benefit plan recordkeeper.

Illustrative Control Objectives

New Plan Setup and Maintenance

Controls provide reasonable assurance that the following control objectives are achieved:

- New plan setups, plan mergers, and plan conversions[46] are authorized and processed in a complete, accurate, and timely manner in accordance with instructions from the plan sponsor and specific plan provisions.
- Plan parameter changes are authorized and processed in a complete, accurate, and timely manner in accordance with instructions from the plan sponsor.

Enrollments and Changes

Controls provide reasonable assurance that the following control objectives are achieved:

- Enrollments are authorized and processed in a complete, accurate, and timely manner.
- Indicative data changes are authorized and processed in a complete, accurate, and timely manner.

Contributions

Controls provide reasonable assurance that contributions[47] are authorized and processed in a complete, accurate, and timely manner.

Distributions

Controls provide reasonable assurance that distributions[48] are authorized and processed in a complete, accurate, and timely manner.

[46] Depending on the similarities in the controls, these three areas may be included as one, two, or three control objectives. To the extent controls related to new plans, mergers, and conversions are different, the service organization may want to have separate control objectives for ease of understanding.

[47] Contributions, including the recordkeeping and money movement, commonly include, but may not be limited to, payroll deductions, loan repayments, loan payoffs, rollovers-in and adjustments.

[48] Distributions, including recordkeeping and money movement, commonly include, but may not be limited to, forfeitures, loans, qualified domestic relations orders (QDROs), pension payments (lump sum and periodic), and adjustments.

Investments and Related Transactions

Controls provide reasonable assurance that the following control objectives are achieved:

- Investment transactions are processed in a complete, accurate, and timely manner.
- Fund transfers are authorized and processed in a complete, accurate, and timely manner.

Pricing

Controls provide reasonable assurance that prices and net asset values are received daily from an authorized source and are recorded in a complete, accurate, and timely manner.

Investment Income

Controls provide reasonable assurance that investment income (for example, dividends and interest income) is processed and allocated to participant accounts in a complete, accurate, and timely manner.

Corporate Actions

Controls provide reasonable assurance that corporate actions are authorized and processed in a complete, accurate, and timely manner.

Reconciliations

Controls provide reasonable assurance that reconciliations between plan and participant records are performed in a complete, accurate, and timely manner.

Statements

Controls provide reasonable assurance that statements are provided to participants and plan sponsors in a complete, accurate, and timely manner.

Illustrative Control Objectives for an Investment Manager

The illustrative control objectives in this section may be relevant to asset management service organizations. They also can be adapted and used, as appropriate, for investment management organizations, trust organizations, hedge fund advisers, or hedge fund of fund advisers.

The control objectives included in this section would be appropriate for an investment manager that performs some or all the following functions:

- Initiating and executing purchase and sale transactions, either by specific direction from the client or under discretionary authority granted by the client
- Determining whether transactions comply with guidelines and restrictions
- Reconciling records of security transactions and portfolio holdings, for each client, to statements received from the custodian
- Reporting to the customer on portfolio performance and activities

Illustrative Control Objectives

New Account Setup and Administration

Controls provide reasonable assurance that the following control objectives are achieved:

- New accounts are authorized and set up in accordance with client instructions and guidelines in a complete, accurate, and timely manner.
- Account modifications are authorized and implemented in a complete, accurate, and timely manner.
- New account holdings and cash are reconciled to custodian bank statements in a complete, accurate, and timely manner.[49]

Security Setup

Controls provide reasonable assurance that new securities and changes to existing securities are authorized and entered in the security master file in a complete, accurate, and timely manner.

Investment Transaction Processing

Controls provide reasonable assurance that the following control objectives are achieved:

- Investment transaction instructions are authorized and entered into the system in a complete, accurate, and timely manner.
- Portfolio guidelines are monitored, and exceptions are identified and resolved in a complete, accurate, and timely manner.[50]
- Allocations are approved by a portfolio manager.
- Block orders are allocated to clients on a pro rata basis for equity trades and a predetermined allocation for fixed-income trades.

Confirmation, Affirmation, or Settlement

Controls provide reasonable assurance that the following control objectives are achieved:

- Investments are settled in a complete, accurate, and timely manner.
- Custodians are informed of transactions in a complete, accurate, and timely manner.

Loans

[49] The service organization may consider establishing a separate control objective that covers the applicable controls related to account conversions or new account set up or including these controls as part of the reconciliation control objective listed subsequently.

[50] This control objective may also be combined with the first control objective in this section by including the additional wording "investment transactions are authorized and executed in accordance with the portfolio policies."

Controls provide reasonable assurance that the following control objectives are achieved:

- Loans and collateral are authorized and processed and recorded in a complete, accurate, and timely manner.
- Collateral on loans is invested in accordance with the lender agreement and recorded and monitored in a complete, accurate, and timely manner.
- Loan repayments are processed and recorded completely, accurately, and in a timely manner.

Pricing

Controls provide reasonable assurance that the following control objectives are achieved:

- Security prices are received from an authorized source and updated in a complete, accurate, and timely manner.
- Price overrides are authorized and processed in a complete, accurate, and timely manner.

Corporate Actions

Controls provide reasonable assurance that corporate action notices are identified and received from an authorized source and are updated in the system in a complete, accurate, and timely manner.

Investment Income

Controls provide reasonable assurance that the following control objectives are achieved:

- Interest, dividend, and other income information is received from an authorized source and recorded in a complete, accurate, and timely manner.
- Cash received for interest and dividends is processed in a complete, accurate, and timely manner.

Money Movement

Controls provide reasonable assurance that money movement (receipts and disbursements) is authorized and processed in a complete, accurate, and timely manner.[51]

Custodian Reconciliation

Controls provide reasonable assurance that security positions and cash balances reflected in the portfolio accounting system are reconciled in a complete, accurate, and timely manner to actual positions and balances held by custodians.[52]

Fees

Controls provide reasonable assurance that investment management fees and other expenses are authorized, calculated, and recorded in a complete, accurate, and timely manner.[53]

Net Asset Valuation

Controls provide reasonable assurance that net asset values are authorized and calculated in a complete, accurate, and timely manner.

[51] The service organization may consider establishing separate control objectives for receipts and disbursements.

[52] The service organization may consider establishing separate control objectives for security positions and cash balances.

[53] A service organization may establish separate control objectives for the accrual of the expense and the payment of the expense.

Account Statements and Client Reports

Controls provide reasonable assurance that account statements and client reports detailing client account holdings and market values are complete, accurate, and provided to clients in a timely manner.

Illustrative Control Objectives for a Payroll Processor

The illustrative control objectives included in this section may be appropriate for a service organization that performs some or all the following functions:

- Processing various types of payroll
- Calculating payroll tax liabilities for federal, state, and local jurisdictions
- Preparing and submitting payroll tax returns and compliance reports
- Printing and distributing payroll checks
- Calculating workers' compensation, state unemployment, and other benefit costs
- Making payments to appropriate agencies and other third parties

Illustrative Control Objectives

Payroll Processing Setup

Controls provide reasonable assurance that the following control objectives are achieved:

- Client requirements are properly authorized and set up in the system completely, accurately, and timely.
- Payroll taxes and other deductions are authorized and set up completely, accurately, and timely.
- Payroll tax and other deductions tables are updated completely, accurately, and timely, as required.
- Changes to client requirements, payroll taxes, and other deductions are updated completely, accurately, and timely.

Payroll Data Authorization and Recording

Controls provide reasonable assurance that the following control objectives are achieved:

- Payroll data are received from authorized sources.
- Payroll data are recorded completely, accurately, and timely.
- Rejected transactions and errors are identified, reported to user entities for follow-up, and properly reentered into the system on a timely basis.
- Payroll transactions are processed completely, accurately, and timely.
- Payroll adjustments are received from authorized sources and processed completely, accurately, and timely.
- Data transmissions to or from clients are authorized, complete, accurate, secure, and processed timely.

Payroll Processing

Controls provide reasonable assurance that the following control objectives are achieved:

- Processing is scheduled and performed appropriately in accordance with client specifications; deviations from the schedule are identified and resolved timely.54
- Payroll deductions and tax withholdings are calculated by the system in accordance with statutory and client specifications.

Reporting

Controls provide reasonable assurance that the following control objectives are achieved:

- Payroll checks, pay statements, and reports are produced completely, accurately, and timely in accordance with client specifications.
- Disbursements of direct deposits are authorized, complete, accurate, and processed timely.
- Data transmissions of money movement and files from the system to outside parties and to the clients' banks are authorized, complete, accurate, secure, and processed in a timely manner.

Illustrative Control Objectives for a Transfer Agent

The illustrative control objectives in this section may be appropriate for a transfer agent that performs transfer or registrar functions. Transfer agents may also perform securities custodial services or execute trades based on authorized instructions. If this is the case, refer to the control objectives under the heading "Illustrative Control Objectives for an Investment Manager," for control objectives that may apply to these functions.

The transfer function may include any of the following tasks:

- Processing old certificates that are properly presented and endorsed in good deliverable form
- Reviewing legal documents to ensure that they are complete and appropriate, before transferring the securities
- Notifying the presenter if the documents are incomplete, or returning rejected documents that are incorrect, insufficient, or otherwise unexecutable
- Issuing new certificates in the name of the new owner
- Making appropriate adjustments to the issuer's shareholder records

The registrar function may include any of the following tasks:

[54] This control objective includes controls in place to ensure that the correct versions of the files are used to validate and update transactions entered for processing. This can be used as a control objective related to any transaction processing. The service organization determines the nature and extent of the control objective and whether the control objective belongs with the business process controls or the IT general controls, based on the services provided and the relevance of these controls to the preparation of financial statements.

- Monitoring the issuance of authorized securities
- Ensuring that the issuance of the new securities will not cause the authorized number of shares in an issue to exceed the total permitted to be issued
- Ensuring that the number of shares transferred corresponds to the number of shares canceled

As part of the transfer and registrar functions previously noted, a transfer agent's functions may also include reasonable assurance that the following control objectives are achieved:

- Maintaining records of the name and address of each security holder, the number of securities owned by each security holder, the certificate numbers corresponding to a security holder's position, the issue date of the security certificate, and the cancelation date of the security certificate, if applicable
- Logging and tracking shareholder and issuer correspondence and resolving inquiries in the correspondence in a timely manner
- Acting as paying agent for cash dividends, dividend reinvestments, and distributions of stock dividends and stock splits
- Monitoring and controlling the proxy voting process

Illustrative Control Objectives

Issuer and Shareholder Setup and Maintenance

Controls provide reasonable assurance that the following control objectives are achieved:

- New clients are authorized and established in the system in a complete, accurate, and timely manner, in accordance with client instructions.
- Changes to client data are authorized and updated in the system in a complete, accurate, and timely manner.
- Shareholder account information and maintenance instructions are authorized and recorded in a complete, accurate, and timely manner.

Securities Transfers

Controls provide reasonable assurance that the following control objectives are achieved:

- Only eligible securities can be transferred, and stock transfers are processed completely and accurately and on a timely basis.
- Subscriptions are authorized and processed in a complete, accurate, and timely manner.
- Exchanges are authorized and processed in a complete, accurate, and timely manner.
- Redemptions are authorized and processed in a complete, accurate, and timely manner.
- Total outstanding share balances are accurately maintained and reconciled in a timely manner.

Dividends

Controls provide reasonable assurance that the following control objectives are achieved:

- Dividend rates are authorized, and payments are calculated and distributed to shareholders of record in a complete, accurate, and timely manner.
- Dividend reinvestments are processed only for authorized individuals and the processing is complete, accurate, and timely.
- Dividend check replacement requests are processed completely, accurately, and in a timely manner.

Safeguarding Assets

Controls provide reasonable assurance that securities and checks in the custody or possession of the transfer agent are protected from loss, misappropriation, or other unauthorized use.

Certificate Replacements

Controls provide reasonable assurance that the following control objectives are achieved:

- Notifications of lost or stolen certificates are authorized and recorded in a complete, accurate, and timely manner.
- Certificate replacement requests are authorized and processed completely, accurately, and in a timely manner.

Illustrative Control Objectives for Custodians Subject to SEC Rule 206(4)-2, "Custody of Funds or Securities of Clients by Investment Advisers"[55]

The illustrative control objectives in this section are relevant when performing an engagement under AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, to meet the reporting requirements of SEC Rule 206(4)-2, which amends the custody rule under the Investment Advisers Act of 1940 by requiring advisers that have custody of client funds or securities to maintain those assets with broker-dealers, banks, or other qualified custodians. Paragraph (a)(6) of Rule 206(4)-2 indicates that an investment adviser that maintains (or has custody because a related person maintains) client funds or securities pursuant to Rule 206(4)-2 as a qualified custodian in connection with advisory services provided to clients must obtain or receive from its related person, no less frequently than once each calendar year, a written internal control report prepared by an independent public accountant. The internal control report must include an opinion of an independent public accountant about whether controls have been placed in operation as of a specified date and are suitably designed and operating effectively to meet control objectives related to custodial services, including the safeguarding of funds and securities held by either the adviser or a related person on behalf of the advisory clients, during the year. In addition to meeting the reporting requirements of SEC Rule 206(4)-2, the illustrative control objectives in this section may also be appropriate for a custodian that is not subject to SEC Rule 206(4)-2 but wishes to undergo an attestation engagement that addresses controls over custody.

[55] Code of Federal Regulations (CFR), Title 17, Section 275.206(4)-2

Controls provide reasonable assurance that the following control objectives are achieved:

- Documentation for the opening and modification of client accounts is received, authenticated, and established completely, accurately, and timely on the applicable systems
- Client transactions, including contributions and withdrawals, are authorized and processed in a complete, accurate, and timely manner
- Trades are properly authorized, settled, and recorded completely, accurately, and timely in the client account(s)
- New securities and changes to securities are authorized and established on the relevant system(s) in a complete, accurate, and timely manner
- Securities income and corporate action transactions are processed to client accounts in a complete, accurate, and timely manner
- Physical securities are safeguarded from loss or misappropriation
- Cash and security positions are reconciled completely, accurately, and on a timely basis between the custodian and depositories
- Account statements reflecting cash and security positions are provided to clients in a complete, accurate, and timely manner

158.

Appendix E: IT General Control Objectives and Risks That Threaten the Achievement of the Control Objectives

	Illustrative Service Organization IT General Control Objectives Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks That Threaten the Achievement of the IT General Control Objectives**
Information Security	• Logical access[56] to programs, data, and computer resources[57] relevant to user entities' internal control over financial reporting (ICFR) is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.[58]	Unauthorized users gain access to and modify data or applications. Authorized users make unauthorized or inappropriate use of or modification to applications or application data. Segregation of duties is not effective or is not enforced by logical access security measures. Logical access security measures are bypassed through physical access to sensitive system resources, resulting in unauthorized access and changes to data or applications.
	• Physical access to computer and other resources[59] relevant to user entities' ICFR is restricted to authorized and appropriate personnel.	Physical media are taken or copied. Unauthorized use is made of system resources.

[56] In assessing the logical access controls over programs, data, and computer resources, the service organization considers the following:

- Logical access controls that may affect the user entities' financial statements – Generally, this would begin with the access controls directly over the application. If the effectiveness of application-level security is dependent on the effectiveness of network and operating system controls, these are also considered. Controls over direct access to the databases or data files and tables are considered as well.
- The configuration and administration of security tools and techniques, and monitoring controls designed to identify and respond to security violations in a timely manner

[57] Computer resources include computer equipment, network equipment, storage media, and other hardware supporting the services provided by the service organization.

[58] Many service organizations have features enabling customers to directly access programs and data. In assessing the logical access controls over programs and data, the service organization considers controls over security related to service organization personnel, the service organization's customers, and the customers' clients, as applicable, as well as the likely effect of these controls on user entities' financial statements.

[59] Other resources include buildings, vaults, and negotiable instruments.

	Illustrative Service Organization IT General Control Objectives Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks That Threaten the Achievement of the IT General Control Objectives**
		Unauthorized physical access is not detected.
Change Management	• Changes to application programs and related data management systems[60] are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely[61] processing and reporting of transactions and balances relevant to user entities' ICFR.[62]	Authorized changes are not entered or are not entered accurately. Application specifications are inconsistent with management needs, intent, or requirements. Application change process is not initiated when business rules, calculations, or processes change. Application logic does not function properly or as specified. Unauthorized changes are made to production applications. Application changes are not approved. Application configuration changes made to the system are not authorized, or authorized changes are not made. Authorized application configuration changes are not entered accurately in the system.

[60] Data management systems include database management systems, specialized data transport, or communications software (often called middleware), data warehouse software, and data extraction or reporting software. Controls over data management systems may enhance user authentication or authorization, the availability of system privileges, data access privileges, application processing hosted within the data management systems, and segregation of duties.

[61] Timeliness may be relevant in particular situations, for example, when emergency changes are needed or when changes that would likely affect the user entities' information systems are being implemented to meet contractual requirements. Controls for emergency changes typically will be different from those for planned changes.

[62] This control objective is quite broad and should be tailored to the service organization's environment. For example, if the service organization has different controls for developing new applications or for making changes to applications or databases, it might be clearer to have separate control objectives for each of these.

	Illustrative Service Organization IT General Control Objectives Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks That Threaten the Achievement of the IT General Control Objectives**
		Application configuration changes are implemented before or after the appropriate time.
	- Network infrastructure[63] is configured as authorized to (1) support the effective functioning of application controls to result in valid, complete, accurate, and timely[64] processing and reporting of transactions and balances relevant to user entities' financial reporting; (2) protect data relevant to user entities' financial reporting from unauthorized changes;[65] and (3) support user entities' ICFR.	Unauthorized changes are made to application configurations. Unauthorized changes are made to infrastructure and infrastructure configurations. Infrastructure and infrastructure configurations do not support the proper functioning of application processing, logical security, or availability of data and files, resulting in unauthorized access to applications or data. Network infrastructure is not updated on a timely basis to protect against known vulnerabilities. Emergency configuration changes are not authorized or appropriate. Unauthorized changes to infrastructure are not detected.

[63] Network infrastructure includes all the hardware, software, operating systems, and communication components within which the applications and related data management systems operate.

[64] Timeliness may be relevant in particular situations (for example, when emergency changes are needed or when changes are being implemented to meet contractual requirements).

[65] Program change controls over network infrastructure include, as appropriate, the authorization, testing, documentation, approval, and implementation of changes to network infrastructure. In assessing change management, the service organization considers the configuration and administration of the security tools and techniques, and monitoring controls designed to identify exceptions to authorized network infrastructure, applications, and data management systems (for example, database structures) and act upon them in a timely manner. If the service organization has different controls for new implementations or making changes to the infrastructure, applications, or data management systems, it might be clearer to have separate control objectives that address the controls over each type of infrastructure. There may also be separate control objectives for controls over new implementations and controls over changes to existing resources.

	Illustrative Service Organization IT General Control Objectives Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks That Threaten the Achievement of the IT General Control Objectives**
Computer Operations	• Application and system processing[66] relevant to user entities' ICFR are authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors that may affect user entities' ICFR are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.	Programs are not executed in the correct order. Programs are not executed within scheduled timeframes. Programs do not execute completely. Abnormally ended programs corrupt the data they were processing. Restarted programs result in incomplete processing or duplicate processing of data. Processing problems and errors are not detected or are not detected in a timely manner. Processing problems are not appropriately resolved in a timely manner. Controls are overridden. Emergency access privileges are misused.
	• Data transmissions between the service organization and its user entities and other outside entities that affect user entities' ICFR are from authorized sources and are complete, accurate, secure, and timely.[67] • Data relevant to user entities' financial reporting is backed up regularly and	Data transmissions do not occur in a timely manner. Data transmissions are not received. Data transmissions are incomplete. Data transmissions are not accurate. Data are transmitted more than once. Data are corrupted or lost and are not recoverable.

[66] The processing in this control objective refers to the batch processing of data. It typically does not include the scheduling of file backups. Should the service organization have significant online, real-time processing, it may tailor this control objective or add a new control objective to address controls over the identification, tracking, recording, and resolution of problems and errors in a complete, accurate, and timely manner.

[67] This control objective may also be presented as part of logical access security or as part of the business operations related to data input or reporting.

	Illustrative Service Organization IT General Control Objectives Controls provide reasonable assurance that the following control objectives are achieved:	**Illustrative Risks That Threaten the Achievement of the IT General Control Objectives**
	available for restoration in the event of processing errors or unexpected processing interruptions.	

159.

Appendix F

Glossary

The following are definitions of some of the terms used in this guide.

carve-out method. A method of providing information about a subservice that management of a service organization may use in preparing its description of the service organization's system. When using this method, the description identifies the nature of the services performed by the subservice organization and excludes from the description the subservice organization's relevant control objectives and related controls.

complementary subservice organization controls. Controls that need to be implemented by a subservice organization for certain control objectives in management's description of the service organization's system to be achieved. When designing its controls, management of the service organization assumes that the subservice organization has implemented these controls and identifies them in its description of the service organization's system.

complementary user entity controls. Controls that need to be implemented by the user entities for certain control objectives in management's description of the service organization's system to be achieved. When designing its controls, management of the service organization assumes that the user entities have implemented these controls and identifies them in its description of the service organization's system.

control objectives. The aim or purpose of specified controls at the service organization. Control objectives address the risks that controls are intended to mitigate.

controls at a service organization. The policies and procedures at a service organization that are likely to affect user entities' internal control over financial reporting (for example, controls at the service organization that affect information processed by the service organization and incorporated in the user entities' financial statements.) The service organization designs, implements, and documents these controls to provide reasonable assurance that the relevant control objectives will be achieved.

inclusive method. A method of providing information about a subservice organization that management of a service organization may use in preparing its description of the service organization's system. When using this method, the description includes a description of the nature of the services provided by the subservice organization as well as the subservice organization's relevant control objectives and related controls.

management's description of the service organization's system. A written description prepared by management of the service organization that identifies the service provided to customers (user entities) that is, the period to which the description relates (or in the case of a type 1 report, the date to which the description relates), the control objectives specified by management or an outside party, the party specifying the control objectives (if not specified by management), and the related controls.

service organization's assertion. For a type 1 SOC 1® report, a written statement by management of the service organization about the matters referred to in part (*b*) of the definition of *type 1 SOC 1® report*, and for a type 2 report, the matters referred to in part (*b*) of the definition of *type 2 SOC 1® report.*

service organization's system. The policies and procedures designed, implemented, and documented by management of the service organization to provide user entities with the services covered by management's description of the service organization's system.

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

test of controls. A procedure designed to evaluate whether controls included in management's description of the service organization's system were operating effectively to achieve the related control objectives, also included in the description. A type 2 SOC 1® report includes a description of the service auditor's tests of the controls and the results of those tests.

type 1 SOC® 1 report: A service auditor's report that comprises the following:

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

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

  i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented as of a specified date

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

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

type 2 SOC 1® report: A service auditor's report that comprises the following:

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

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

  i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented as of a specified date

ii. the controls related to the control objectives stated in management’s description of the service organization’s system were suitably designed to achieve those control objectives as of the specified date

c. A report that expresses an opinion on the matters in *b*i–iii

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

user entity. An entity that uses a service organization for which controls at the service organization are likely to affect that entity’s internal control over financial reporting.

AICPA®

aicpa.org