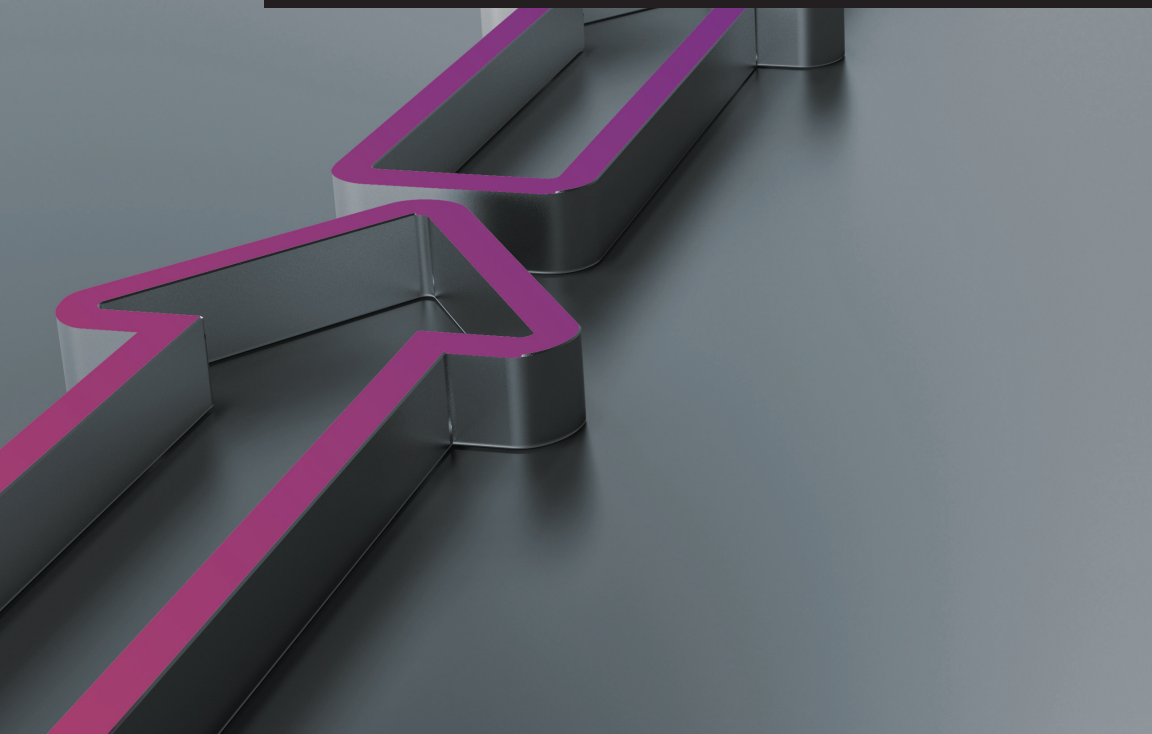
AICPA®

Guide

Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy

SOC 2®

October 15, 2022



AICPA®

Guide

Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy

SOC 2®

October 15, 2022

2202-61712

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

ISBN 978-1-95515-910-4

Preface

(Updated as of October 15, 2022)

About AICPA Guides

This AICPA Guide, *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, has been developed by members of the AICPA Assurance Services Executive Committee's (ASEC's) SOC 2 Working Group, in conjunction with members of the Auditing Standards Board (ASB), to assist practitioners engaged to examine and report on a service organization's controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy.

This AICPA Guide includes certain content presented as an "appendix." Appendixes are included for informational purposes and have no authoritative status.

An AICPA Guide containing attestation guidance is recognized as an interpretive publication as described in AT-C section 105, *Concepts Common to All Attestation Engagements*.[1] Interpretative publications are recommendations on the application of Statements on Standards for Attestation Engagements (SSAEs) in specific circumstances, including engagements for entities in specialized industries. Interpretive publications are issued under the authority of the ASB. The members of the ASB have found the attestation guidance in this guide to be consistent with existing SSAEs.

A practitioner should consider the guidance in this guide in planning and performing an attestation engagement.

Any attestation guidance in a guide appendix, although not authoritative, is considered an "other attestation publication." In applying such guidance, the practitioner should, exercising professional judgment, assess the relevance and appropriateness of such guidance to the circumstances of the engagement. Although the practitioner determines the relevance of other attestation guidance, such guidance in a guide appendix has been reviewed by the AICPA Audit and Attest Standards staff and the practitioner may presume that it is appropriate.

The ASB is the designated senior committee of the AICPA authorized to speak for the AICPA on all matters related to attestation. Conforming changes made to the attestation guidance contained in this guide are approved by the ASB Chair (or a designee) and the director of the AICPA Audit and Attest Standards staff. Updates made to the attestation guidance in this guide exceeding that of conforming changes are issued after all ASB members have been provided an opportunity to consider and comment on whether the guide is consistent with the SSAEs.

---

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

Recently Issued Attestation Standards

SSAE No. 20, *Amendments to the Description of the Concept of Materiality*

In December 2019, the ASB issued SSAE No. 20, *Amendments to the Description of the Concept of Materiality*, which amends various AT-C sections to reflect a revised description of the concept of materiality. The ASB's current description of the concept of materiality is consistent with the definition of materiality used by the International Accounting Standards Board (IASB) and the International Auditing and Assurance Standards Board (IAASB). SSAE No. 20 aligns the materiality concepts discussed in the attestation standards with the description of materiality used by the U.S. judicial system, the auditing standards of the PCAOB, the SEC, and FASB. The ASB believes it is in the public interest to eliminate inconsistencies between the description of materiality in the attestation standards and the description of materiality used by the U.S. judicial system and other U.S. standard setters and regulators. The ASB believes that, because the revised definition is aligned with FASB's definition, the revised description is substantially consistent with current U.S. firm practices with respect to determining and applying materiality in an attest engagement; accordingly, the amendments are neither expected nor intended to change U.S. practice. The revised description of materiality is as follows: Misstatements, including omissions, are considered to be material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

The SSAE is effective for periods ending, or for practitioners' examination or review reports dated, on or after December 15, 2020.

SSAE No. 21, *Direct Examination Engagements*

In October 2020, the ASB issued SSAE No. 21, *Direct Examination Engagements*, which among other things, adds a new AT-C section to the attestation standards, designated as AT-C section 206, *Direct Examination Engagements*. AT-C section 206 enables a practitioner to perform an examination engagement in which the practitioner obtains reasonable assurance by (1) measuring or evaluating underlying subject matter against criteria and (2) expressing an opinion that conveys the results of that measurement or evaluation.

SSAE No. 21 also amends AT-C section 105 of SSAE No. 18 and supersedes AT-C section 205, *Examination Engagements*, of SSAE No. 18. Revisions to those standards were necessary to address both assertion-based and direct examination engagements. Where applicable, those changes are reflected in this guide.

SSAE No. 21 is effective for reports dated on or after June 15, 2022.

As discussed in paragraph 1.17 of this guide, the SOC 2 examination discussed herein is an assertion-based examination. Accordingly, the service auditor performs the examination under AT-C section 205, which supplements the requirements and guidance in AT-C section 105. Therefore, this guide does not address the requirements and guidance in AT-C section 206.

Purpose and Applicability

This guide, *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, provides guidance to practitioners engaged to examine and report on a service organization's controls over one or more of the following:

- The security of a service organization's system
- The availability of a service organization's system
- The processing integrity of a service organization's system
- The confidentiality of the information that the service organization's system processes or maintains for user entities
- The privacy of personal information that the service organization collects, uses, retains, discloses, and disposes of for user entities

AT-C sections 105 and 205 establish the requirements and application guidance for reporting on a service organization's controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy. Because certain underlying circumstances of the subject matter addressed in this guide are analogous to circumstances addressed in AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, requirements and application guidance in that standard may be relevant when reporting on an entity's controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy.

The attestation standards enable a practitioner to report on subject matter other than historical financial statements. A practitioner may be engaged to examine and report on controls at a service organization related to various types of subject matter (for example, controls that affect user entities' financial reporting or the privacy of information processed for user entities' customers).

Terms Used to Define Professional Responsibilities in This AICPA Guide

Any requirements described in this guide are normally referenced to the applicable standards or regulations from which they are derived. Generally, the terms used in this guide to describe the professional requirements of the referenced standard setter (for example, the ASB) are the same as those used in the applicable standards or regulations (for example, "must" or "should").

Readers should refer to the applicable standards and regulations for more information on the requirements imposed by the use of the various terms used to define professional requirements in the context of the standards and regulations in which they appear.

References to Professional Standards

In citing attestation standards and their related interpretations, references to standards that have been codified use section numbers within the codification of currently effective SSAEs and not the original statement number.

Examinations of System and Organization Controls: SOC Suite of Services

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 or 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. This guide, *SOC 2® Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, is an interpretation of AT-C sections 105 and 205 that assists CPAs in reporting on the security, availability, or processing integrity of a system or the confidentiality or privacy of the information processed by the system. This engagement is referred to as SOC 2 — SOC for Service Organizations: Trust Services Criteria. Other SOC engagements include the following:

- *SOC 1 — SOC for Service Organizations: ICFR*. Service organizations may provide services that are relevant to their user entities' internal control over financial reporting and, therefore, to the audit of financial statements. These examinations are performed under AT-C section 320. The requirements and guidance for performing and reporting on such controls are provided in AT-C sections 105, 205, and 320. AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)* provides relevant interpretive guidance to assist practitioners in performing these engagements.
- *SOC 3 — SOC for Service Organizations: Trust Services Criteria for General Use Report*. Although the requirements and guidance for performing a SOC 3 examination are similar to those for a SOC 2 examination, the reporting requirements are different. Because of the different reporting requirements, a SOC 2 report is appropriate only for specified parties with sufficient knowledge and understanding of the service organization and the system, whereas a SOC 3 report is ordinarily appropriate for general use.
- *SOC for Cybersecurity*. As part of an entity's cybersecurity risk management program, an entity designs, implements, and operates cybersecurity controls. An engagement to examine and report on a description of the entity's cybersecurity risk management program and the effectiveness of controls within that program is a *cybersecurity risk management examination*. The requirements and guidance for performing and reporting in a cybersecurity risk management examination are provided in AT-C sections 105 and 205. Because certain underlying circumstances of the subject matter addressed in a SOC for Cybersecurity engagement are analogous to circumstances addressed in AT-C section 320, certain requirements and application guidance in that standard may be relevant when reporting on an entity's controls over its cybersecurity risk management program and the effectiveness

of controls within that program. AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* provides interpretive guidance for the relevant attestation standards to assist practitioners engaged to examine and report on the description of an entity's cybersecurity risk management program and the effectiveness of controls within that program.

- *SOC for Supply Chain*. Internal and external forces such as globalization, global interconnectivity, automation, and other technological advancements are making today's supply chains highly sophisticated and complex. For entities that produce, manufacture, or distribute products, there's often a high level of interdependence and connectivity between them and their suppliers and their customers and business partners. A SOC for Supply Chain examination helps these organizations, and their customers and business partners, identify, assess, and address supply chain risks. The performance and reporting requirements for an examination of an entity's controls over a system that produces, manufactures, or distributes products are found in AT-C sections 105 and 205. Because certain underlying circumstances of the subject matter addressed in a SOC for Supply Chain engagement are analogous to circumstances addressed in AT-C section 320, certain requirements and application guidance in that standard may be relevant when reporting on an entity's controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy. AICPA Guide *Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System (SOC for Supply Chain)* contains application guidance for practitioners.

This guide focuses on SOC 2 engagements. To make practitioners aware of the various professional standards and guides available to them for examining and reporting on system-level controls at a service organization and entity-level controls at other organizations, and to help practitioners select the appropriate standard or guide for a particular engagement, appendix A, "Comparison of SOC 1, SOC 2, and SOC 3 Examinations and Related Reports," includes a table that compares the features of the three engagements. Additionally, appendix B, "Comparison of SOC 2, SOC for Supply Chain, and SOC for Cybersecurity Examinations and Related Reports," compares the features of a SOC 2 examination and a cybersecurity risk management examination.

Description Criteria for a Description of a Service Organization's System in a SOC 2 Report

In February 2018, ASEC issued revised description criteria for a description of a service organization's system in a SOC 2 report, which are codified in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)*, (2018 description criteria).[2] The 2018 description criteria were established by

[2] All DC sections can be found in AICPA *Description Criteria*.

ASEC for use by service organization management when preparing the description of the service organization's system and by service auditors when evaluating whether the description is presented in accordance with the description criteria in a SOC 2 examination.

The current version of the 2018 description criteria has been modified to reflect revisions to the implementation guidance relevant to certain of the description criteria. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. As such, it may assist management when developing disclosures. In addition, the points of focus may assist the practitioner when evaluating whether the description is fairly presented.

The revisions to the implementation guidance do not in any way alter the criteria in the 2018 description criteria. Such criteria continue to be suitable criteria for use when evaluating the description of a system in a SOC 2 engagement.

Revisions to the implementation guidance were developed by ASEC's SOC 2 Working Group; all revisions were reviewed by the ASEC chair. The revised implementation guidance is intended to provide users of the criteria with

- additional clarity regarding certain disclosure requirements.
- guidance on disclosure of how controls meet the requirements of a process or control framework.
- guidance on disclosure of information about the risk assessment process and specific risks.

In establishing and developing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees*,[3] designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA Council or the board of directors. Paragraph .A46 of AT-C section 105 indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable. Accordingly, these criteria are suitable criteria for preparing and evaluating a description of a system in a SOC 2 examination. ASEC has also published the description criteria and made them available to users. Therefore, the description criteria meet the requirements in paragraph .27*b*ii of AT-C section 105 for criteria that are both suitable and available for use in an attestation engagement.

Trust Services Criteria

Codified as TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* (2017 trust services criteria),[4] the trust services criteria were established by ASEC for use by practitioners when providing attestation or consulting services to evaluate controls relevant to the security, availability, or processing integrity of one or more systems, or the confidentiality or privacy of

[3] All BL sections can be found in AICPA *Professional Standards*.

[4] All TSP sections can be found in AICPA *Trust Services Criteria*.

information processed by one or more systems, used by an entity. Entity management may also use the trust services criteria to evaluate the suitability of design and operating effectiveness of such controls.

The current version of the 2017 trust services criteria has been modified to reflect new points of focus and edits to extant points of focus (collectively referred to as "revisions") relevant to certain of the trust services criteria. Points of focus represent important characteristics of the criteria. As such, they may assist management when designing, implementing, and operating controls over security, availability, processing integrity, confidentiality, or privacy. In addition, the points of focus may assist both management and the practitioner when they are evaluating whether controls were suitably designed and operated effectively to achieve the entity's objectives based on the trust services criteria.

The revisions to the points of focus do not in any way alter the criteria in the 2017 trust services criteria. Such criteria continue to be suitable criteria for use when evaluating controls in any trust services engagement.

Revisions to the points of focus were developed by ASEC's SOC 2 Working Group and ASEC's Data Privacy Working Group; all revisions were reviewed by the ASEC chair. The revised points of focus in this version are intended to better support application of the criteria in

- an environment of ever-changing technologies, threats and vulnerabilities, and other matters that may create additional security risks to organizations.
- addressing changing legal and regulatory requirements and related cultural expectations regarding privacy.
- addressing data management requirements (for example, data storage, backup, and retention), particularly when related to confidentiality.
- differentiating which points of focus related to privacy may apply only to an organization that is a data controller and which may apply only to an organization that is a data processor, as defined in the glossary. (Although this distinction is intended to assist management and the service auditor in identifying situations in which certain points of focus may be particularly relevant, the specific facts and circumstances of the organization's operations are relevant when identifying and applying points of focus in a trust services engagement.)

In establishing and developing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. BL section 360R designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA Council or the board of directors. Paragraph .A46 of AT-C section 105 indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable. Accordingly, these criteria are suitable criteria for evaluating controls in a SOC 2 examination. ASEC has also published the trust services criteria and made them available to users. Therefore, the trust services criteria meet the requirements in paragraph .27*b*ii of AT-C section 105 for criteria that are both suitable and available for use in an attestation engagement.

Applicability of Quality Control Standards

QM section 10A, *A Firm's System of Quality Control*,[5] addresses a CPA firm's responsibilities for its system of quality control for its accounting and auditing practice. A system of quality control consists of policies that a firm establishes and maintains to provide it with reasonable assurance that the firm and its personnel comply with professional standards, as well as applicable legal and regulatory requirements. The policies also provide the firm with reasonable assurance that reports issued by the firm are appropriate in the circumstances.

QM section 10A applies to all CPA firms with respect to engagements in their accounting and auditing practice. In paragraph .13 of QM section 10A, an *accounting and auditing practice* is defined as

> [a] practice that performs engagements covered by this section, which are audit, attestation, compilation, review, and any other services for which standards have been promulgated by the AICPA Auditing Standards Board (ASB) or the AICPA Accounting and Review Services Committee (ARSC) under the "General Standards Rule" (ET sec. 1.300.001)[6] or the "Compliance With Standards Rule" (ET sec. 1.310.001) of the AICPA Code of Professional Conduct. Although standards for other engagements may be promulgated by other AICPA technical committees, engagements performed in accordance with those standards are not encompassed in the definition of an *accounting and auditing practice*.

In addition to the provisions of QM section 10A, readers should be aware of other sections within AICPA *Professional Standards* that address quality control considerations, including the following provisions that address engagement-level quality control matters for various types of engagements that an accounting and auditing practice might perform:

- AU-C section 220A, *Quality Control for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards*[7]
- AT-C section 105, *Concepts Common to All Attestation Engagements*
- AR-C section 60A, *General Principles for Engagements Performed in Accordance With Statements on Standards for Accounting and Review Services*[8]

See the AICPA practice aid *Establishing and Maintaining a System of Quality Control for a CPA Firm's Accounting and Auditing Practice*, available at https://us.aicpa.org/interestareas/frc/enhancingauditqualitypracticeaid.html for guidance about the key aspects of the quality control standards currently in effect.

---

[5] All QM sections can be found in AICPA *Professional Standards*.

[6] All ET sections can be found in AICPA *Professional Standards*.

[7] All AU-C sections can be found in AICPA *Professional Standards*.

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

Recent Developments in the Quality Management Standards

On June 2, 2022, the ASB issued Statement on Quality Management Standards (SQMS) No. 1, *A Firm's System of Quality Management*, codified as QM section 10. Systems of quality management in compliance with SQMS No. 1 are required to be designed and implemented by December 15, 2025, and the evaluation of the system of quality management required by SQMS No. 1 is required to be performed within one year following December 15, 2025.

QM section 10 addresses a CPA firm's responsibilities for its system of quality management for its accounting and auditing practice. The objective of a system of quality management is to provide the firm with reasonable assurance that the firm and its personnel comply with professional standards, as well as applicable legal and regulatory requirements. The system also provides the firm with reasonable assurance that reports issued by the firm are appropriate in the circumstances. The firm designs, implements, and operates the system by establishing quality objectives, identifying and assessing risks to the achievement of the quality objectives, and designing and implementing responses, consisting of policies or procedures, to address the quality risks.

QM section 10 applies to all CPA firms with respect to engagements in their accounting and auditing practice. In paragraph .17 of QM section 10, an *accounting and auditing practice* is defined as a

> practice that performs engagements covered by this section, which are audit, attestation, review, compilation, and any other services for which standards have been promulgated by the AICPA Auditing Standards Board (ASB) or the AICPA Accounting and Review Services Committee (ARSC) under the "General Standards Rule" (ET sec. 1.300.001) or the "Compliance With Standards Rule" (ET sec. 1.310.001) of the AICPA code.

A firm's accounting and auditing practice comprises engagements performed under the following standards promulgated by the ASB and ARSC:

- Statements on Auditing Standards (SASs)
- Statements on Standards for Attestation Engagements (SSAEs)
- Statements on Standards for Accounting and Review Services (SSARSs)

Although standards for other engagements may be promulgated by other AICPA technical committees, engagements performed in accordance with those other standards are not encompassed in the definition of an *accounting and auditing practice.*

Readers should be aware of other sections within AICPA *Professional Standards* that address quality management considerations, including the following:

- QM section 20, *Engagement Quality Reviews*
- AU-C section 220, *Quality Management for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards*

- AT-C section 105, *Concepts Common to All Attestation Engagements*
- AR-C section 60, *General Principles for Engagements Performed in Accordance With Statements on Standards for Accounting and Review Services*

Because of the importance of engagement quality, this guide includes appendix I, "Overview of Statements on Quality Management Standards," which summarizes key aspects of the quality management standards. This summarization should be read in conjunction with QM section 10, QM section 20, AU-C section 220, AT-C section 105, and AR-C section 60, as applicable.

Recognition

Auditing Standards Board (2021–2022)

Tracy W. Harding, *Chair*
Brad C. Ames
Maxene Bardwell
Samantha Bowling
Patricia Bottomly
Sherry Chesser
Harry Cohen
Jeanne Dee
Horace Emery
Diane Hardesty
Robert Harris
Kathleen K. Healy
Jon Heath
Clay Huffman
Greg Jenkins
Sara Lord
Maria C. Manasses
Andrew Prather
Chris Rogers
Tania Desilva Sergott

Assurance Services Executive Committee (2021–2022)

Jim Burton, *Chair*
Damon T. Busse
Daniel Richard Balla
Mary Grace Davenport
Jim Dalkin
Chris Halterman
Dyan Rohol
Catherine M. Schweigel
Amy Steele
Kimberly Ellison-Taylor
Steve Ursillo
Miklos Vasarhelyi

ASEC SOC 2 Working Group

Chris Halterman, *Chair*
Angela Appleby
David Barnes
Efrim Boritz
Brandon Brown
Jeff Cook
Charles Curran
Joel Eshleman
Meghan Hester
Peter F. Heuzey
Audrey Katcher
Kevin Knight
Christopher W. Kradjan
Brandon Miller (Observer)
Thomas Patterson
Binita Pradhan
John Richardson
Don Sheehy
Soma Sinha
Rod Smith
Steve Ursillo (Observer)
David Wood

AICPA Staff

Jennifer Burns
Chief Auditor
Professional Standards and Services

Amy Pawlicki
Vice President
Assurance and Advisory Innovation

Mimi Blanco-Best
Associate Director
Attestation Methodology and Guidance

Carrie Kostelec
Lead Manager
SOC & Related Services

Anna Miller
Technical Publishing Manager
Publishing

Chapter 1

Introduction and Background

This chapter explains the relationship between a service organization and its user entities; provides examples of service organizations and the services they may provide; explains the relationship between those services and the system used to provide them; describes the components of a system and its boundaries; identifies the criteria used to evaluate a description of a service organization's system (description criteria) and the criteria used to evaluate whether controls were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved (applicable trust services criteria); and explains the difference between a type 1 SOC 2 report and type 2 SOC 2 report.[1] It also describes the relationship between a service organization and its business partners and the effect of a service organization's system on those business partners. In addition, this chapter provides an overview of a SOC 3® examination and other SOC services.

Introduction

1.01 Entities often use business relationships with other entities to further their objectives. Network-based information technology has enabled, and telecommunications systems have substantially increased, the economic benefits derived from these relationships. For example, some entities (user entities) are able to function more efficiently and effectively by outsourcing tasks or entire functions to another organization (service organization). A service organization is organized and operated to provide user entities with the benefits of the services of its personnel, expertise, equipment, and technology to help accomplish these tasks or functions. Other entities (business partners) enter into agreements with a service organization that enable the service organization to offer the business partners' services or assets (for example, intellectual property) to the service organization's customers. In such instances, business partners may want to understand the effectiveness of controls implemented by the service organization to protect the business partners' intellectual property.

1.02 Examples of the types of services provided by service organizations include the following:

- *Customer support*. Providing user entities with online or telephonic post-sales support and service management for their customers. Examples of these services are warranty inquiries and investigating and responding to customer complaints.
- *Health care claims management and processing*. Providing medical providers, employers, third-party administrators, and insured parties of employers with systems that enable medical records and related health insurance claims to be processed accurately, securely, and confidentially.

[1] Throughout this guide, these SOC 2 reports and the related examinations are referred to simply as type 1 and type 2 reports and examinations.

- *Enterprise information technology (IT) outsourcing services*. Managing, operating, and maintaining user entities' IT data centers, infrastructure, and application systems and related functions that support IT activities, such as network, production, security, change management, hardware, and environmental control activities.
- *eCommerce software-as-a-service (SaaS) application*. Providing user entities with shopping cart software, allowing businesses to create an online shop within minutes without coding, hosting, or software.
- *Managed security*. Managing access to networks and computing systems for user entities (for example, granting access to a system and preventing, or detecting and mitigating, system intrusion).
- *Financial technology services*. Providing financial services companies with IT-based transaction processing services. Examples of such transactions are loan processing, peer-to-peer lending, payment processing, retirement recordkeeping, crowdfunding, big data analytics, and investment management.
- *Environmental, social, and governance (ESG) metric services*. Measuring, calculating, and otherwise assisting companies with gathering and reporting their ESG metrics.

1.03 Although these relationships may increase revenue, expand market opportunities, reduce costs for the user entities and business partners, and mitigate certain business risks, they also result in new risks arising from interactions with the service organization and its system. Accordingly, the management of user entities and business partners are responsible for identifying, evaluating, and addressing those additional risks as part of their risk assessment. In addition, although management can delegate responsibility for specific tasks or functions to a service organization, management remains accountable for those tasks to boards of directors, shareholders, regulators, customers, and other affected parties. As a result, management is responsible for establishing effective internal control over interactions between the service organizations and their systems.

1.04 To identify, assess and address the risks associated with a service organization, its services, and the system used to provide the services, user entities and business partners usually need information about the design, operation, and effectiveness of controls[2] within the system. To support their risk assessments, user entities and business partners may request a SOC 2 report from the service organization. A SOC 2 service auditor's report is the culmination of an independent service auditor's[3] examination of whether (*a*) the description of the service organization's system presents the system that was

---

[2] In this guide, *controls* are policies and procedures that are part of the service organization's system of internal control. Controls exist within each of the five internal control components of the Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control — Integrated Framework*: control environment, risk assessment, control activities, information and communication, and monitoring. The objective of a service organization's system of internal control is to provide reasonable assurance that its service commitments and system requirements are achieved. When this guide refers to "controls that provide reasonable assurance," it means the controls that make up the system of internal control.

[3] The attestation standards refer to a CPA who performs an attestation engagement as a *practitioner*. However, this guide uses the term *service auditor* to refer to the practitioner in a SOC 2 examination.

designed and implemented in accordance with the description criteria; (*b*) the controls stated in the description were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the criteria, if those controls operated effectively; and (*c*) in a type 2 examination, the controls stated in the description operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the criteria relevant to the security, availability, or processing integrity of the service organization's system (security, availability, processing integrity) or based on the criteria relevant to the system's ability to maintain the confidentiality or privacy of the information processed for user entities (confidentiality or privacy).[4,5] This examination, which is referred to as a *SOC 2 examination*, is the subject of this guide.

1.05 As illustrated in table 1-1, there are two types of SOC 2 examinations that address the informational needs of users:

a. A type 1 examination is an examination of whether

i. a service organization's description presents the system that was designed and implemented as of a point in time in accordance with the description criteria and

ii. controls were suitably designed as of a point in time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, if controls operated effectively.

A report on such an examination is referred to as a *type 1 report*.

b. A type 2 examination also addresses the description of the system and the suitability of design of controls, but it includes an additional subject matter: whether controls operated effectively throughout the period of time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. A report on such an examination is referred to as a *type 2 report*. A type 2 report also includes a detailed description of the service auditor's tests of controls and the results of those tests.

1.06 A service auditor may be engaged to perform either a type 1 or a type 2 examination. A service auditor may not be engaged to examine and express an opinion on only the suitability of design of some controls and both the design and operating effectiveness of other controls in a SOC 2 examination.

Intended Users of a SOC 2 Report

1.07 A SOC 2 report, whether a type 1 or a type 2 report, is intended to provide report users with information about the service organization's system

---

[4] As discussed in footnote 1, controls can only provide reasonable assurance that an organization's objectives are achieved. In a SOC 2 examination, the service organization designs, implements, and operates controls to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria.

[5] A SOC 2 examination may be performed on any of the trust services categories (security, availability, processing integrity, confidentiality, and privacy). Use of the trust services criteria in a SOC 2 examination is discussed beginning in paragraph 1.44.

relevant to security, availability, processing integrity, confidentiality, or privacy to enable such users to assess and address the risks that arise from their relationships with the service organization. The report is also intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with the service organization's system, particularly system controls that the service organization has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria. For example, disclosures about the types of services provided, the environment in which the entity operates, and the components of the system used to provide such services allow report users to better understand the context in which the system controls operate.

1.08 A SOC 2 report is intended for use by those who have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide those services, among other matters. The expected knowledge of specified parties ordinarily includes the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations,[6] and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entities' ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks

1.09 Without such knowledge, users are likely to misunderstand the content of the SOC 2 report, the assertions made by management, and the service auditor's opinion, all of which are included in the report. For that reason, a SOC 2 report, as discussed in this guide, is restricted to use by users with that knowledge. Restricting the use of a service auditor's report in a SOC 2 examination is discussed beginning in paragraph 4.36.

1.10 In a SOC 2 report, the following intended users are presumed to have the knowledge identified in paragraph 1.08:

a. User entities of the system throughout some or all of the period. User entities need information about the service organization's system, including the nature and effectiveness of controls within that system, to understand the service organization's controls and to determine whether those controls, in addition to their own controls, are sufficient to mitigate their business risks.

---

[6] If a service organization uses a subservice organization, the description of the service organization's system may either (*a*) include the subservice organization's functions or services and related controls (inclusive method) or (*b*) exclude the subservice organization's functions or services and related controls (carve-out method). Chapter 2, "Accepting and Planning a SOC 2 Examination," discusses the two methods for treating subservice organizations.

b. *Business partners subject to risks arising from interactions with the system*. Business partners may include affiliated organizations that are user entities, vendors, or subservice organizations of the service organization. Business partners need information about the service organization's system and the controls within that system to manage and assess the risks associated with doing business with the service organization.

1.11 In some situations, federal or state governmental agencies, industry consortiums, or groups of subject matter experts who need information about a specific subject matter (for example, security controls over sensitive information) from their members or other entities with whom they do business may also be intended users.

1.12 Intended users may also include service organization personnel, practitioners providing services to the entity's customers and business partners, and regulators who have the knowledge and understanding discussed in paragraph 1.08.

1.13 Parties other than those identified in paragraphs 1.10–1.12 may also have the requisite knowledge and understanding identified in paragraph 1.08. For example, prospective user entities or business partners, who intend to use the information contained in the SOC 2 report as part of their vendor-selection process or to comply with regulatory requirements for vendor acceptance, may have gained such knowledge while performing due diligence. Additionally, a user entity of a service organization's subservice organization (an indirect or downstream user entity) may be included in the group to whom use of the service auditor's report is restricted. An organization that is considered an indirect user entity ordinarily would not have a contract with the subservice organization, but would have a contract with the primary service organization.

1.14 As previously discussed, the SOC 2 report has been designed to meet the common information needs of the broad range of intended users described in the preceding paragraphs. However, nothing precludes the service auditor from restricting the use of the service auditor's report to a smaller group of users.

1.15 In some situations, service organization management may wish to distribute a report on the service organization's controls relevant to security, availability, confidentiality, processing integrity, or privacy to users who lack the knowledge and understanding described in paragraph 1.08. In that case, management may engage a service auditor to examine and express an opinion on the effectiveness of controls within a service organization's system in a SOC 3 examination. As discussed beginning at paragraph 1.73, a SOC 3 report is ordinarily appropriate for general users. Chapter 4, "Forming the Opinion and Preparing the Service Auditor's Report," discusses the reporting elements of a SOC 3 report in further detail.

Overview of a SOC 2 Examination

1.16 As previously discussed, a SOC 2 examination is an examination of a service organization's description of its system, the suitability of the design of its controls, and in a type 2 examination, the operating effectiveness of controls relevant to security, availability, processing integrity, confidentiality, or privacy.

This guide provides performance and reporting guidance for both types of SOC 2 examinations.

1.17 The SOC 2 examination discussed in this guide is an assertion-based examination. Accordingly, the service auditor performs the examination under AT-C section 205, *Assertion-Based Examination Engagements*, which supplements the requirements and guidance in AT-C section 105, *Concepts Common to All Attestation Engagements*.[7] Therefore, this guide does not address the requirements and guidance in AT-C section 206, *Direct Examination Engagements*.

1.18 In a SOC 2 examination, service organization management is the responsible party. However, in certain situations there may be other responsible parties.[8] As the responsible party, service organization management prepares the description of the service organization's system that is included in the SOC 2 report.

1.19 The service auditor should request a written assertion from management.[9] Management's written assertion, which is also included in the SOC 2 report, addresses whether (*a*) the description of the service organization's system is presented in accordance with the description criteria, (*b*) the controls stated in the description were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and (*c*) in a type 2 examination, those controls were operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

1.20 The service auditor designs and performs procedures to obtain sufficient appropriate evidence about whether the description presents the system that was designed and implemented in accordance with the description criteria and whether (*a*) the controls stated in the description were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and, (*b*) in a type 2 examination, those controls were operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. In a type 2 examination, the service auditor also presents, in a separate section of the SOC 2 report, a description of the service auditor's tests of controls and the results thereof.

Contents of the SOC 2 Report

1.21 A SOC 2 examination results in the issuance of a *SOC 2 report*. As shown in table 1-1, the SOC 2 report includes three key components (four in a type 2 examination):

---

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

[8] If the service organization uses one or more subservice organizations and elects to use the inclusive method for preparing the description, subservice organization management is also a responsible party. Management's and the service auditor's responsibilities when the service organization uses one or more subservice organizations and elects to use the inclusive method are discussed further in chapter 2.

[9] See paragraph .10 of AT-C section 205, *Assertion-Based Examination Engagements*.

Table 1-1

Contents of a SOC 2 Report

Type 1 Report	*Type 2 Report*
1. Management's description of the system as of a point in time in accordance with the description criteria	1. Management's description of the system throughout a period of time in accordance with the description criteria
2. Management assertion that addresses whether *a.* the description of the service organization's system as of a point in time is presented in accordance with the description criteria and *b.* the controls stated in the description were suitably designed as of a point in time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria	2. Management assertion that addresses whether *a.* the description of the service organization's system throughout a period of time is presented in accordance with the description criteria, *b.* the controls stated in the description were suitably designed throughout a period of time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and *c.* the controls stated in the description operated effectively throughout a period of time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria
3. The service auditor's opinion about whether *a.* the description of the service organization's system as of a point in time is presented in accordance with the description criteria and	3. The service auditor's opinion about whether *a.* the description of the service organization's system throughout a period of time is presented in accordance with the description criteria,

(continued)

Contents of a SOC 2 Report — *continued*

Type 1 Report	*Type 2 Report*
b. the controls stated in the description were suitably designed as of a point in time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria	*b.* the controls stated in the description were suitably designed throughout a period of time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and *c.* the controls stated in the description operated effectively throughout a period of time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria
	4. Description of the service auditor's tests of controls and results thereof

Definition of a System

1.22 Service organization management is responsible for identifying the specific subject matter to be examined, including the components of the system used to provide the service and the boundaries of that system. Service organization management is also responsible for establishing its service commitments and system requirements and selecting the trust services category or categories to be addressed by the examination, as well as for selecting the period of time to be addressed. The following paragraphs provide a brief overview of each of these factors and how they might affect the subject matter of the engagement.

1.23 In the SOC 2 examination, a *system* includes the infrastructure, software, procedures, and data that are designed, implemented, and operated by people to achieve one or more of the organization's specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements.

1.24 System components can be classified into the following five categories:

- *Infrastructure*. The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal

networks and connected external telecommunications networks) that the service organization uses to provide the services

- *Software*. The application programs and IT system software that support application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications
- *People*. The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers)
- *Data*. The types of data used by the system, such as transaction streams, files, databases, tables, and other outputs used or processed by the system
- *Procedures*. The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information are prepared

Boundaries of the System

1.25 The boundaries of a system addressed by a SOC 2 examination need to be clearly understood, defined, and communicated to report users. For example, a financial reporting system is likely to be bounded by the components of the system related to financial transaction initiation, authorization, recording, processing, and reporting. The boundaries of a system related to processing integrity (system processing is complete, accurate, timely, and authorized), however, may extend to other operations (for example, risk management, internal audit, information technology, or customer call center processes).

1.26 If management has determined that functions or processes related to the system are outside of the boundaries of the system identified as the subject matter of the examination, there may be a risk that intended users think those functions or processes were examined as part of the SOC 2 examination. In that case, the description needs to clarify which processes or functions are within the scope of the examination and which are not.

1.27 In a SOC 2 examination that addresses the security, availability, or processing integrity criteria, the system boundaries would cover, at a minimum, all the system components as they relate to the transaction processing or service life cycle, including initiation, authorization, processing, recording, and reporting of the transactions processed for or services provided to user entities. The system boundaries would not include instances in which transaction-processing information is combined with other information for secondary purposes internal to the service organization, such as customer metrics tracking.

1.28 It is becoming increasingly common for service organizations to use information provided by third-party software applications or tools, whether installed on the premises or through software as a service, to perform certain internal control activities relevant to the system being examined. For example, tools may assist management in the identification or detection of threats and vulnerabilities (such as firewalls, intrusion-prevention systems [IPSs],

intrusion-detection systems [IDSs], and security information and event management systems [SIEMs]); monitoring the implementation of key software settings; or monitoring the effectiveness of automated controls. Such tools would be considered within the boundaries of the system when they support the service organization in achieving its service commitments and system requirements. The processing performed by these tools is designed to be consistent, but is highly dependent on other factors such as whether the ability to change configuration settings is appropriately restricted and whether changes are made in accordance with the change management process. It is important that the service auditor consider the information produced by such tools when evaluating the appropriateness of the boundaries of the system addressed by the engagement and related disclosures.

1.29 In a SOC 2 examination that addresses the confidentiality or privacy criteria, the system boundaries would cover, at a minimum, all the system components as they relate to the confidential or personal information life cycle, which consists of the collection, use, retention, disclosure, and disposal or anonymization of personal information by well-defined processes and informal ad hoc procedures, such as emailing personal information to an actuary for retirement benefit calculations. The system boundaries would also include instances in which that information is combined with other information (for example, in a database or system), a process that would not otherwise cause the other information to be included within the scope of the examination. For example, the scope of a SOC 2 examination that addresses the privacy of personal information may be limited to a business unit (online book sales) or geographical location (Canadian operations), as long as the personal information is not commingled with information from, or shared with, other business units or geographical locations.

The Service Organization's Objectives, Service Commitments, and System Requirements

1.30 A service organization adopts a mission and vision, sets strategies, and establishes objectives to help it achieve its mission and vision based on its strategies. Management designs and implements various systems to achieve specific objectives and designs and implements controls within the systems to mitigate the risks that would prevent the entity from achieving those objectives. As discussed in more detail in paragraph 1.56, the service organization's objectives for its services and the system used to deliver those services are embodied in the service commitments it makes to user entities and the requirements it establishes for the functioning of the system used to deliver those services (service commitments and system requirements).

1.31 In order to understand the service provided, the system, and the design and operation of the controls, SOC 2 report users usually require an understanding of the nature of the service organization's service commitments and system requirements. The service commitments and system requirements that are likely to be useful to support this understanding by a broad range of SOC 2 report users are referred to as *principal service commitments and system requirements*. These principal service commitments and system requirements are disclosed in the system description. Although management discloses only its principal service commitments and system requirements in the system description, management is responsible for designing and operating controls to

provide reasonable assurance that the entire population of its service commitments and system requirements are achieved. Likewise, the service auditor's opinion considers all of the service organization's service commitments and system requirements.

Selecting the Trust Services Category or Categories to Be Addressed by the Examination

1.32 In addition to identifying the components and boundaries of the system, it is also necessary to consider which trust services category or categories are to be addressed by the examination. As discussed in paragraph 1.44, the trust services criteria are used to measure the effectiveness of controls in a SOC 2 examination. The engaging party, who is also typically the responsible party, may choose to engage the service auditor to report on controls related to one or more of the trust services categories (security, availability, processing integrity, confidentiality, and privacy). Typically, the engaging party selects the category or categories that would best meet the information needs of intended users. Which category or categories are selected is often determined by considering the risks that use of the service organization presents to user entities and the principal service commitments made to them.

1.33 Because of increased dependence on technology and concerns about cybersecurity risks, security is likely to be addressed in most examinations performed using the trust services criteria. Often, customers and business partners of a service organization are also interested in the effectiveness of controls over availability because such controls may be integral to meeting their commitments.

1.34 In some cases, intended users may also be interested in the processing integrity of the system the service organization uses to process information. Processing integrity addresses system controls that mitigate the risk that the service organization's system objectives will not be achieved because of failures in the processing system.

1.35 When a service organization uses proprietary customer information or personal information in the system process, intended users may also be interested in controls over that information. In this case, an examination that also addresses confidentiality or privacy may best meet users' needs.

1.36 In some situations, the omission of a category that is likely to be important to report users may result in a misleading report. For example, the service auditor may become aware that report users are primarily concerned about cybersecurity risks arising from the interconnection of the service organization's system with users' systems. If service organization management wishes to engage a service auditor to perform an examination addressing only the availability category, such a report could be misunderstood by users, who would expect the examination to address controls designed, implemented, and operated by the service organization to mitigate its cybersecurity risks, not only those that threaten the achievement of the service organization's availability commitments. In this situation, the service auditor might conclude that an examination addressing only the availability category is likely to be misleading to report users and decide to decline the engagement.

Difference Between Privacy and Confidentiality

1.37 As used in this guide, the term "confidentiality" applies to various types of sensitive information,[10] whereas the term "privacy" applies only to personal information[11] and embodies the unique considerations in handling information related to people. Therefore, a SOC 2 examination that includes the trust services privacy category may encompass the service organization's specific processes that address the following, as applicable:

- Notice of the service organization's privacy commitments and practices
- Protection of personal information from unauthorized or inappropriate use and disclosure
- Data subjects' choices regarding the use and disclosure of their personal information
- Data subjects' rights to access their personal information for review and update
- An inquiry, complaint, and dispute resolution process

1.38 If the system that is the subject of the SOC 2 examination does not create, collect, transmit, use, or store personal information, or if the service organization does not make commitments to its system users related to one or more of the matters described in the preceding paragraph, a SOC 2 examination that addresses the privacy criteria may not be useful because many of the privacy criteria will not be applicable. Instead, a SOC 2 examination that addresses the confidentiality criteria is likely to provide report users with the information they need about how the service organization maintains the confidentiality of sensitive information used by the system.

Time Frame of Examination

1.39 Paragraph .A1 of AT-C section 105 states that the measurement or evaluation of conditions or events addressed by an attestation examination may be "as of a point in time" or "for a specified period of time." Service organization management is responsible for determining the time frame to be covered by the description of the service organization's system. Generally, in a type 1 examination, the time frame is as of a point in time; in a type 2 examination, it is for a specified period of time. Regardless of the time frame selected, the SOC 2 examination contemplates that the time frame is the same for both the description and management's assertion. Furthermore, the discussions in this guide about type 2 examinations contemplate that management has elected to have the examination performed for a specified period of time.

---

[10] Sensitive information varies from organization to organization but often includes nonpublic information such as the following: regulatory compliance information; financial information used for both internal and external reporting purposes; confidential sales information, including customer lists; confidential wholesale pricing information and order information; confidential product information including product specifications, new design ideas, and branding strategies; and proprietary information provided by business partners, including manufacturing data, sales and pricing information, and licensed designs. Sensitive information also includes personal information.

[11] Personal information is nonpublic information about or related to an identifiable individual, such as personal health information or personally identifiable information (such as personnel records, payment card information, and online retail customer profile information).

Criteria for a SOC 2 Examination

1.40 The following two types of criteria are applicable in a SOC 2 examination:

- *Description criteria*. DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)*,[12] includes the criteria used to prepare and evaluate the description of the service organization's system. The use of these criteria, referred to as the *description criteria,* in a SOC 2 examination is discussed further beginning in paragraph 1.41.
- *Trust services criteria*. TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*[13] (the 2017 trust services criteria), includes the criteria used to evaluate the suitability of the design and, in a type 2 examination, the operating effectiveness of the controls relevant to the trust services category or categories included within the scope of a particular examination. The use of these criteria, referred to as the *applicable trust services criteria*, in a SOC 2 examination is discussed further beginning in paragraph 1.44.

Description Criteria

1.41 The description criteria are used by management when preparing the description of the service organization's system and by the service auditor when evaluating the description. Applying the description criteria in actual situations requires judgment. Therefore, in addition to the description criteria, DC section 200 presents implementation guidance for each criterion. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. The implementation guidance does not address all possible situations; therefore, users are advised to carefully consider the facts and circumstances of the entity and its environment in actual situations when applying the description criteria.

1.42 The description criteria in DC section 200 were promulgated by the Assurance Services Executive Committee (ASEC). In establishing and developing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees*,[14] designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA Council or the board of directors. Paragraph .A46 of AT-C section 105 indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable. Accordingly, these criteria are suitable criteria for preparing and evaluating a description of a system in a SOC 2 examination. ASEC has also published the description criteria and made them available to users. Therefore, the description criteria meet the definition in paragraph .27*b*ii of AT-C section 105 for criteria that are both suitable and available for use in an attestation engagement.

---

[12] The DC sections can be found in AICPA *Description Criteria*.

[13] The TSP sections can be found in AICPA *Trust Services Criteria*.

[14] All BL sections can be found in AICPA *Professional Standards*.

1.43 Chapter 3, "Performing the SOC 2 Examination," discusses how the description criteria are used by the service auditor in a SOC 2 examination.

Trust Services Criteria

1.44 The trust services criteria are used to evaluate the suitability of design and operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. Because applying the trust services criteria requires judgment, TSP section 100 also presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control — Integrated Framework*[15] (COSO framework) states that points of focus represent important characteristics of the criteria in that framework. Consistent with the COSO framework, the points of focus in TSP section 100 may assist management when designing, implementing, and operating controls over security, availability, processing integrity, confidentiality, and privacy. In addition, the points of focus may assist both management and the service auditor when evaluating whether controls stated in the description were suitably designed and operated to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

1.45 As previously discussed, a service organization faces risks that threaten its ability to achieve its service commitments and system requirements. The criterion for determining whether controls are suitably designed is that the controls stated in the description[16] would, if operating as described, provide reasonable assurance that such risks would not prevent the service organization from achieving its service commitments and system requirements.

1.46 In a type 2 examination, the criterion for determining whether the controls stated in the description of the service organization's system operated effectively to provide reasonable assurance that its service commitments and system requirements were achieved is that the suitably designed controls were consistently operated as designed throughout the specified period, including that manual controls were applied by individuals who have the appropriate competence and authority.

1.47 The trust services criteria in TSP section 100 were promulgated by ASEC. In establishing and developing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. BL section 360R designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA Council or the board of directors. Paragraph .A46 of AT-C section 105 indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable. Accordingly, these criteria are suitable criteria for evaluating controls in a SOC 2 examination. ASEC has also published the trust services criteria and made them available to users. Therefore, the trust services criteria meet the requirements

---

[15] ©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

[16] Description criterion DC5 in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)*, indicates that the description of the service organization's system should include the applicable trust services criteria and the related controls designed to meet those criteria.

in paragraph .27*b*ii of AT-C section 105 for criteria that are both suitable and available for use in an attestation engagement.

Categories of Trust Services Criteria

1.48 The trust services criteria are classified into the following five categories:

a. *Security*. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

b. *Availability*. Information and systems are available for operation and use to meet the entity's objectives.

c. *Processing integrity*. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

d. *Confidentiality*. Information designated as confidential is protected to meet the entity's objectives.

e. *Privacy*. Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

1.49 Depending on which category or categories are included within the scope of the examination, the applicable trust services criteria consist of

- criteria common to all five of the trust services categories (common criteria) and
- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

For example, if the SOC 2 examination is on only availability, the controls should address all the common criteria and the additional specific criteria for availability. This is important because a control deficiency related to the common criteria may affect the service organization's ability to achieve its service commitments and system requirements related to availability. Therefore, the service auditor still has to evaluate the suitability of design and, in a type 2 examination, the operating effectiveness of controls related to all the common criteria (CC1.1 through CC9.2), which encompass controls such as those over logical and physical access, system operations, and change management, in addition to controls necessary to meet the criteria related to the availability category.

Common Criteria

1.50 The common criteria presented in TSP section 100 (CC1–CC5) are organized into the following classifications:

a. Control environment (CC1 series)

b. Information and communication (CC2 series)

c. Risk assessment (CC3 series)

d. Monitoring activities (CC4 series)

e. Control activities (CC5 series) (Control activities are further broken out into the following subclassifications: logical and physical access controls [CC6 series], system operations [CC7 series], change management [CC8 series], and risk mitigation [CC 9 series].)

1.51 ASEC has determined that the common criteria are suitable for evaluating the effectiveness of controls to achieve a service organization's service commitments and system requirements related to security; no additional control activity criteria are needed. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of (*a*) the common criteria and (*b*) the control activity criteria applicable to the specific category. Table 1-1 identifies the trust services criteria to be addressed when evaluating the effectiveness of controls for each of the trust services categories and indicates how each category is labeled in the table presented in TSP section 100.

Table 1-2

Criteria for Evaluating the Design and Operating Effectiveness of Controls

Trust Services Category	*Common Criteria*	*Additional Category-Specific Criteria*
Security	X	
Availability	X	X (A series)
Processing integrity	X	X (PI series)
Confidentiality	X	X (C series)
Privacy	X	X (P series)

1.52 Because each system and the environment in which it operates are unique, the combination of risks that would prevent a service organization from achieving its service commitments and system requirements, and the controls necessary to address those risks, will be unique in each SOC 2 examination. Management needs to identify the specific risks that threaten the achievement of the service organization's service commitments and system requirements and the controls necessary to provide reasonable assurance that those service commitments and system requirements are achieved based on the category or categories to be addressed by the examination, as discussed beginning at paragraph 1.32.

1.53 Service organization management is responsible for evaluating whether controls stated in the description were effective to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to one or more of the trust services categories addressed by the examination. Such criteria are referred to throughout this guide as the *applicable trust services criteria*. For example, in an examination that addresses security, the trust services criteria relevant to security, which are the common criteria (CC1.1–CC9.2) presented in TSP section 100, are the applicable trust services criteria.

Using the Trust Services Criteria in an Engagement That Addresses Privacy

1.54 Some points of focus relevant to criteria in the privacy category may apply only to an organization that is a *data controller* or only to an organization that is a *data processor*. This distinction has been noted within the

privacy-related points of focus to assist management and the service auditor in identifying situations in which certain points of focus may be particularly relevant. It may also assist management and the service auditor in understanding how the specific facts and circumstances of the organization's operations may affect the identification and application of points of focus in an engagement where privacy is included in the scope of the examination.

Using the Trust Services Criteria to Evaluate Suitability of Design and Operating Effectiveness in a SOC 2 Examination

1.55 As previously discussed, the trust services criteria presented in TSP section 100 are used to evaluate the effectiveness (suitability of design and operating effectiveness) of controls in a SOC 2 examination. These criteria are based on the COSO framework, which notes that "an organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them." Internal control supports the organization in achieving its objectives. Consequently, to evaluate internal control, the evaluator needs to understand the organization's objectives. Many of the trust services criteria refer to the achievement of "the entity's objectives." In a SOC 2 examination, the service organization's objectives for its services and the system used to deliver those services are embodied in the service commitments it makes to user entities and the requirements it has established for the functioning of the system used to deliver those services (service commitments and system requirements). For example, when applying CC3.2, *The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed*, the service organization identifies risks to the achievement of its service commitments and system requirements and analyzes those risks as a basis for determining how best to manage them. Chapter 3 discusses in further detail how the service auditor uses the trust services criteria when evaluating whether controls stated in the description were suitably designed and, in a type 2 examination, operating effectively based on the applicable trust services criteria.

Evaluating The Service Organization's Service Commitments and System Requirements

1.56 A service organization's system of internal control is evaluated by using the trust services criteria to determine whether the service organization's controls provide reasonable assurance that its business objectives and sub-objectives are achieved. When a service organization provides services to user entities, its objectives and sub-objectives relate primarily to (*a*) the achievement of the service commitments made to user entities related to the system used to provide the services and the system requirements necessary to achieve those commitments, (*b*) compliance with laws and regulations regarding the provision of the services by the system, and (*c*) the achievement of the other objectives the service organization has for the system. These are referred to as the service organization's service commitments and system requirements.

1.57 Service organization management is responsible for establishing its service commitments and identifying its system requirements. Service commitments are the declarations made by service organization management to user entities (its customers) about the system used to provide the service. Commitments can be communicated in written individualized agreements, standardized contracts, service-level agreements, or published statements (for example,

a security practices statement). Commitments may be made on many different aspects of the service being provided, including the following:

- Specification of the algorithm used in a calculation
- The hours a system will be available
- Published password standards
- Encryption standards used to encrypt stored customer data
- Implementation of controls to meet the requirements of a particular process or control framework (for example, the National Institute of Standards and Technology's Cybersecurity Framework [NIST CSF])

1.58 Service commitments may also be made about one or more of the trust services categories addressed by the description. As an example, if controls over privacy are addressed by the description, a service organization may make commitments such as the following:

- The organization will not process or transfer information without obtaining the data subject's consent.
- The organization will provide a privacy notice to customers once every six months or when there is a change in the organization's business policies.
- The organization will respond to access requests within 10 working days of receiving the requests from its customers.

1.59 System requirements are the specifications about how the system should function to (*a*) meet the service organization's service commitments to user entities and others (such as user entities' customers); (*b*) meet the service organization's commitments to vendors and business partners; (*c*) comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (*d*) achieve other objectives of the service organization that are relevant to the trust services categories addressed by the description. Requirements are often specified in the service organization's system policies and procedures, system design documentation, contracts with customers, and in government regulations. The following are examples of system requirements:

- Workforce member fingerprinting and background checks established in government banking regulations
- Legal requirements to prevent certain types of transactions
- Entity policies establishing maximum acceptable intervals between periodic review of workforce member logical access as documented in the security policy manual
- Data definition and tagging standards, including any associated metadata requirements (for example, the Simple Object Access Protocol [SOAP]) established by industry groups or other bodies
- Business processing rules and standards established by regulators (for example, security requirements under the Health Insurance Portability and Accountability Act [HIPAA])

1.60 System requirements may result from the service organization's commitments relating to one or more of the trust services categories (for example, a commitment to programmatically enforce segregation of duties between data

entry and data approval creates system requirements regarding user access administration).

1.61 Service organization management is responsible for achieving its service commitments and system requirements. It is also responsible for stating in the description the service organization's *principal* service commitments and system requirements with sufficient clarity to enable report users to understand the nature of system operation and management's and the service auditor's basis for evaluating the suitability of the design of controls and, in a type 2 examination, the operating effectiveness of controls. Because of the importance of the service commitments and system requirements to the SOC 2 examination, the principal service commitments and system requirements disclosed by management should be appropriate for the engagement. Chapter 2, "Accepting and Planning a SOC 2 Examination," discusses the service auditor's responsibility for assessing whether the principal service commitments and system requirements disclosed by service organization management in the description are appropriate.

Meeting the Requirements of a Process or Control Framework

1.62 In some situations, governmental bodies, industry consortiums, or groups of subject matter experts may develop process or control frameworks (for example, International Organization for Standardization and International Electrotechnical Commission [ISO/IEC] Standards 27001 and 27002, NIST CSF) for obtaining and sharing specific information from other entities, including service organizations, about a particular subject matter of interest to them (for example, security controls over sensitive information). Most process or control frameworks identify specific sets of processes or controls (referred to in this guide as requirements of the process or control framework) for entities to implement. In addition, many frameworks establish certification programs to demonstrate that entities have met the requirements of the process or control framework.[17] The most common types of process or control frameworks focus on information security and privacy. A governmental body, industry consortium, or group of experts that develops and maintains such a framework is referred to as a *sponsoring organization* throughout this document.

1.63 In some situations, a process or control framework may be required by law or regulation (for instance, the security and privacy rules established to implement HIPAA); in other situations, the service organization may make commitments to customers or business partners about addressing the requirements of a process or control framework, or the service organization may elect to implement controls that address the requirements of such a framework as part of its risk management program.

1.64 When the service organization establishes service commitments and system requirements regarding the requirements of the process or control framework, the evaluation of whether controls were suitably designed and operated effectively would include consideration of whether the implemented

[17] A limited number of process or control framework may have similar objectives to those of the trust services criteria (that is, controls within the system are suitably designed and operating effectively). However, this guide focuses on situations in which the objective is simply implementation of certain controls.

controls met those requirements. In this situation, the requirements of the process or control framework are likely to be additional points of focus when using the trust services criteria.[18,19] For example, a service organization that provides services to a U.S. government entity would likely consider the requirements of the NIST CSF and NIST Special Publication (NIST SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, as points of focus when evaluating whether its controls are suitably designed and operating effectively.

1.65 Management may decide to provide users with certain information in the SOC 2 report that supports users' understanding of how the controls implemented by the service organization address the requirements of a process or control framework. If management considers such disclosures to be supplemental to the information included in the SOC 2 report, management would ordinarily present such disclosures in section 5, "Other Information Provided by XYZ Service Organization That Is Not Covered by the Service Auditor's Report" of the SOC 2 report. The service auditor's responsibility for other information is discussed beginning in paragraph 4.101.

1.66 In other situations, management may include such disclosures in the description of the system. This is likely to be the case when management has identified a principal service commitment or system requirement related to the process or control framework. In this situation, management would generally include information about how the system components, including processes and controls (DC3),[20] addressed requirements of the process or control framework and how the implemented controls met those requirements (DC5). Paragraph 3.48 describes different ways that these disclosures may be made. The service auditor's responsibility for such disclosures is discussed beginning at paragraph 3.50.

1.67 To meet the requests of users, management may engage the service auditor to examine and report on whether the service organization's controls were implemented to meet the requirements of the process or control framework in a SOC 2+ examination, which is discussed beginning at paragraph 1.69.

1.68 Chapter 2 provides additional guidance on how the service organization's service commitments and system requirements related to the implementation of controls to meet the requirements of a process or control framework may affect the service auditor's planning and risk assessment procedures; chapter 3 further discusses the effect on the evaluation of the suitability of design and operating effectiveness of controls; and chapter 4 discusses the impact on forming an opinion and issuing the report.

---

[18] As discussed in paragraph 1.44, points of focus are important characteristics of the criteria that assist both management and the service auditor when applying the criteria. Some points of focus may not be suitable or relevant to the service organization or to the SOC 2 engagement. In other situations, management may identify and consider other characteristics based on the specific circumstances of the entity.

[19] To facilitate the consideration of the requirements of some of the more commonly-used process and control frameworks as complementary or additional points of focus, the AICPA has mapped those requirements to the trust services criteria. Such mappings can be found on the AICPA website.

[20] "(DCX)," as used in this guide, refers to the specific number of the description criterion that addresses the issue discussed.

SOC 2 Examination That Addresses Additional Criteria (SOC 2+)

1.69 As discussed in paragraph 1.63, there are situations in which a service organization makes commitments about implementing a set of processes or controls to meet the requirements of a specific process or control framework and establishes system requirements to support the achievement of those commitments. If management determines that intended users of the report are likely to want assurance about whether the service organization achieved those commitments and requirements, it may engage the service auditor to also examine and issue a separate opinion about whether the organization has implemented processes or controls to meet the requirements of the process or control framework. In this situation, both management and the service auditor evaluate the controls that management has implemented to meet the objective of the process or control framework (additional criteria) to support management's assertion and the service auditor's additional opinion, respectively. In many cases, the objective of the process or control framework is the implementation of a specific set of processes or controls.[21]

1.70 A SOC 2 examination that includes an additional opinion about matters that are not normally within the scope of the SOC 2 examination is typically referred to as a SOC 2+ examination. Although the additional matters in a SOC 2+ examination most frequently relate to whether controls were implemented to meet the requirements of a process or control framework, a SOC 2+ examination may also include other matters not ordinarily addressed by a SOC 2 examination. For example, management may want to provide customers and business partners with certain metrics that demonstrate how the service organization has achieved its availability commitments. Because it believes such metrics are important to judgments made by users, management may engage a service auditor to determine whether such metrics are presented in accordance with additional specified criteria.

1.71 In this guide, guidance related to SOC 2+ examinations assumes that the service auditor's additional opinion is on whether controls were implemented to meet the requirements of a process or control framework.[22] *Process or control frameworks*, as that term is used in this guide, are discussed in further detail beginning at paragraph 1.62.

1.72 A SOC 2+ examination is performed in accordance with AT-C section 205 and relevant guidance in this guide. To address the additional criteria in the SOC 2+ examination, in accordance with paragraph .20 of AT-C section 205, the service auditor should perform procedures to obtain sufficient appropriate evidence about whether the service organization's controls were implemented to meet the control requirements in the process or control framework. Chapter 2 discusses the impact of additional criteria on the service auditor's planning and risk assessment procedures, chapter 3 discusses the impact on the evaluation of

---

[21] A limited number of process or control frameworks may have similar objectives to those of the trust services criteria (that is, controls within the system are suitably designed and operating effectively). In this situation, the evaluation of the suitability of design and operating effectiveness of controls using the trust services criteria and the other framework should result in a similar conclusion.

[22] In some situations, two separate engagements with two separate reports may meet the users' needs better than a SOC 2+ engagement. Management and the service auditor may work together to determine the type of engagement and report that would best meet the needs of the user.

controls, and chapter 4 discusses the impact on forming an opinion and issuing the SOC 2+ report.

SOC 3 Examination

1.73 A service organization may wish to provide prospective customers (user entities) with information regarding the effectiveness of controls over its system. However, the prospective customers may not have signed a nondisclosure agreement required by the service organization to access the system description in the SOC 2 report. In other situations, prospective customers may not have sufficient knowledge about the system, which might cause them to misunderstand the information in the SOC 2 report. In these circumstances, a SOC 3 report, which is designed for general use, may be appropriate. Because the procedures performed in a SOC 2 examination are substantially the same as those performed in a SOC 3 examination, the service organization may ask the service auditor to issue two reports at the end of the examination: a SOC 2 report to meet the governance needs of its existing customers and a SOC 3 report to meet the needs of a broader set of users. Because these users may not have sufficient understanding of the service organization's system, the disclosure of the service auditor's tests performed and results of tests may overshadow the service auditor's overall opinion or may cause users to misunderstand the service auditor's report. As a result, the SOC 3 report includes only the following elements as identified in paragraph 4.119:

a. An assertion by service organization management about whether the controls were effective throughout the period

b. An opinion by the service auditor on service organization management's assertion about whether controls within the system were effective throughout the period

1.74 There is no type 1 equivalent for a SOC 3 report. In a SOC 3 examination, service organization management prepares, and includes in the SOC 3 report, a written assertion about whether the controls within the system were effective[23] throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. In connection with the assertion, management also describes (*a*) the boundaries of the system and (*b*) the service organization's principal service commitments and system requirements. Such disclosures, which ordinarily accompany the assertion, enable report users to understand the scope of the SOC 3 examination and how management evaluated the effectiveness of controls. The SOC 3 report also includes the service auditor's opinion on whether management's assertion was fairly stated based on the applicable trust services criteria. As in a SOC 2 examination, a service auditor may be engaged to report on one or more of the five trust services categories included in TSP section 100.

1.75 Unlike a SOC 2 report, a SOC 3 report does not include a description of the system, so the detailed controls within the system are not disclosed. In addition, the SOC 3 report does not include a description of the service auditor's

[23] Throughout this guide, the term *effective* (as it relates to controls) encompasses both the suitability of design of controls and the operating effectiveness of controls.

tests of controls and the results thereof.[24] Appendix A, "Comparison of SOC 1, SOC 2, and SOC 3 Examinations and Related Reports," compares a SOC 2 and a SOC 3 report.

1.76 Chapter 2 discusses planning considerations in a SOC 3 examination, and chapter 4 discusses the reporting elements of a SOC 3 report.

Other Types of SOC Examinations: SOC Suite of Services

1.77 The term *system and organization controls* (SOC) refers to a suite of services that practitioners may provide relating to system-level controls of a service organization and system- or entity-level controls of other organizations. The SOC suite of services currently comprises the following individual reporting frameworks:

1. SOC 1 — SOC for Service Organizations: ICFR[25]
2. SOC 2 — SOC for Service Organizations: Trust Services Criteria
3. SOC 3 — SOC for Service Organizations: Trust Services Criteria for General Use Report
4. SOC for Cybersecurity
5. SOC for Supply Chain

SOC 1 — SOC for Service Organizations: ICFR

1.78 AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, provides performance and reporting requirements for an examination of controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. A service organization's controls are relevant to a user entity's internal control over financial reporting when they are part of the user entity's information and communications component of internal control maintained by the service organization.[26] Such an examination is known as a *SOC 1 examination*, and the resulting report is known as a *SOC 1 report*. The controls are generally those that a service organization implements to prevent, or detect and correct, misstatements[27] in the information or services it provides to user entities.

---

[24] Because the SOC 3 report was designed as a general use report, a description of the service auditor's procedures and results is not included in the report. According to paragraph .A85 of AT-C section 205, the addition of such information may increase the potential for the report to be misunderstood, which may lead the service auditor to add a restricted-use paragraph to the report; therefore, a SOC 3 report containing such information is unlikely to be appropriate for general use.

[25] ICFR stands for internal control over financial reporting.

[26] Controls also may be relevant when they are part of one or more of the other components of a user entity's internal control over financial reporting. The components of an entity's internal control over financial reporting are described in detail in appendix B, "Internal Control Components," of AU-C section 315A, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*.

All AU-C sections can be found in AICPA *Professional Standards*.

[27] Paragraph .12 of AT-C section 105, *Concepts Common to All Attestation Engagements*, defines a *misstatement* as a difference between the measurement or evaluation of the underling subject matter and the appropriate measurement or evaluation of the underlying subject matter in accordance with (or based on) the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions. Throughout this guide, the terms *description misstatements*, *deviations*, and *deficiencies* all refer to types of misstatements.

1.79 Service organizations frequently receive requests from user entities for SOC 1 reports because they are useful in designing, implementing, and evaluating the user entities' own internal control over financial reporting and are needed by the auditors of the user entities' financial statements (user auditors) to obtain information about controls at the service organization that may affect assertions in the user entities' financial statements. A SOC 1 report is intended solely for the information and use of management of the service organization, user entities of the service organization's system during some or all of the period covered by the report, and the auditors who audit and report on such user entities' financial statements or internal control over financial reporting. AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)* contains application guidance for service auditors.

1.80 Appendix A of this guide includes a table that presents the differences between SOC 1, SOC 2, and SOC 3 examinations and related reports.

SOC for Cybersecurity

1.81 Cybersecurity has become a top concern for boards of directors and senior executives of many entities, regardless of their size or the industry in which they operate. Government officials are also concerned about cybersecurity at governmental agencies and departments. For most entities, cybersecurity is a significant business risk that needs to be identified, assessed, and managed along with other business risks the entity faces, and it is management's responsibility to ensure that all employees throughout the entity, not only those in the information technology department, address cybersecurity risks. Managing this business issue is especially challenging because even an entity with a highly sophisticated cybersecurity risk management program has a residual risk that a material cybersecurity breach can occur and not be detected in a timely manner. Furthermore, the combined effects of an entity's dependency on information technology, the complexity of information technology networks and business applications, extensive reliance on third parties, and human nature (for instance, susceptibility to social engineering) are only likely to increase the need for effective cybersecurity risk management programs in the foreseeable future.

1.82 For those reasons, the AICPA has developed a framework for organizations to describe their cybersecurity risk management programs and for practitioners to examine and report on a description of an entity's cybersecurity risk management program and the effectiveness of controls within the program. This examination is known as a *cybersecurity risk management examination*; the related report is known as a *cybersecurity risk management examination report*. Criteria for describing a cybersecurity risk management program can be found in DC section 100, *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*, and the performance and reporting requirements for an examination of the description are found in AT-C section 105 and AT-C section 205. AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* contains interpretive application guidance for practitioners performing these engagements.

1.83 The cybersecurity risk management examination report includes three key components: (*a*) the description of the entity's cybersecurity risk management program, (*b*) management's assertion about whether the description is presented in accordance with the description criteria and whether the controls

within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria, and (*c*) the practitioner's opinion about whether the description is presented in accordance with the description criteria and whether the controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

1.84 In the cybersecurity risk management examination, management selects the criteria to be used to prepare the description of the entity's cybersecurity risk management program (description criteria) and the criteria to be used to evaluate the effectiveness of controls within that program (control criteria).

1.85 Because the practitioner's report is designed to be included in the cybersecurity risk management examination report, which is intended for general distribution, the practitioner's report is appropriate for general use. Nevertheless, practitioners may decide to restrict the use of the report to specified users.

1.86 Appendix B, "Comparison of SOC 2, SOC for Supply Chain, and SOC for Cybersecurity Examinations and Related Reports," of this guide presents the differences between a SOC 2 examination and a cybersecurity risk management examination.

SOC for Supply Chain

1.87 Due to rapid technological advancement, the production, manufacturing, or distribution of products often involves a high level of interdependence and connectivity between the entity and (*a*) organizations that supply raw materials or components for the manufacturing process (suppliers) and (*b*) its customers and business partners. These relationships are often considered part of the supply chain. A supply chain is a system of organizations, people, activities, information, and resources involved in moving a product from supplier to customer. Supply chain activities involve the transformation of natural resources, raw materials, and components into finished goods.

1.88 Although these relationships may increase revenues, expand market opportunities, and reduce costs for the entity, they also result in additional risks to the suppliers, customers, and business partners with whom the entity does business. Accordingly, those suppliers, customers, and business partners are responsible for identifying, evaluating, and addressing those additional risks as part of their supply chain risk management programs.

1.89 To identify, assess, and address the risks arising from interactions between the entity and the system it uses to produce, manufacture, or distribute products, suppliers, customers, and business partners usually need information about the design, operation, and effectiveness of controls within the system. To support their risk assessments, suppliers, customers, or business partners may request an attestation report from the entity. Such a report is the result of an attestation engagement in which a practitioner examines and opines on (*a*) whether the description of the entity's system that produces, manufactures, or distributes products (the *description of the system* or *description*) presents the system that was designed and implemented in accordance with the description criteria and (*b*) whether the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its system objectives, were effective throughout the period, based on the applicable trust services criteria.

1.90 Appendix B of this guide presents the differences between a SOC 2 examination and a SOC for Supply Chain examination.

Professional Standards

1.91 This guide provides guidance for a service auditor performing either a type 1 or a type 2 SOC 2 examination in accordance with the attestation standards. In addition to the performance and reporting guidance in the attestation standards, a service auditor performing a SOC 2 examination is required to comply with the requirements of other professional standards, such as professional ethics and quality control standards. This section discusses each of the professional standards that apply to a SOC 2 examination.

Attestation Standards

1.92 The service auditor performs a SOC 2 examination under AT-C section 205, which supplements the requirements and guidance in AT-C section 105. In performing an assertion-based examination, the practitioner is required to comply with both of these sections.

1.93 This guide provides additional application guidance to assist a service auditor engaged to perform and report in a SOC 2 examination. Because this guide is an interpretive publication, paragraph .21 of AT-C section 105 requires the service auditor to consider this guidance when planning and performing a SOC 2 examination.

1.94 In some cases, this guide repeats or refers to the requirements in AT-C section 105 and AT-C section 205 when describing the performance and reporting requirements with which a service auditor should comply in a SOC 2 examination. Although not all the requirements in AT-C section 105 and AT-C section 205 are repeated or referred to in this guide, the service auditor is responsible for complying with all relevant requirements contained in those sections.

Code of Professional Conduct

1.95 The AICPA Code of Professional Conduct provides guidance and rules that apply to all members in the performance of their professional responsibilities. The code includes the fundamental principles that govern the performance of all professional services performed by CPAs and, among other things, calls for CPAs to maintain high ethical standards and to exercise due care in the performance of all services. When providing attestation services, the "Considering or Subsequent Employment or Association With an Attest Client" subtopic (ET sec. 1.279)[28] of the "Independence Rule" (ET sec. 1.200.001) requires CPAs to be independent in both fact and appearance. Independence in a SOC 2 examination is discussed further beginning in paragraph 2.41.

Quality in the SOC 2 Examination

1.96 Paragraphs .06–.07 of AT-C section 105 discuss the relationship between the attestation standards and the AICPA quality control standards. Quality control systems, policies, and procedures are the responsibility of a firm

[28] All ET sections can be found in AICPA *Professional Standards*.

when conducting its attestation practice. Under QM section 10A, *A Firm's System of Quality Control*,[29] a CPA firm has an obligation to establish and maintain a system of quality control to provide it with reasonable assurance that

a. the firm and its personnel comply with professional standards and applicable legal and regulatory requirements and

b. reports issued by the firm are appropriate in the circumstances.

1.97 QM section 10A additionally states that the firm should establish criteria against which all engagements are to be evaluated to determine whether an engagement quality control review should be performed. If the engagement meets the established criteria, the nature, timing, and extent of the engagement quality control review should follow the guidance discussed in that standard and the requirements in paragraph .45 of AT-C section 105.

1.98 Paragraph .35 of AT-C section 105 states that the engagement partner should take responsibility for the overall quality of the attestation engagement, including matters such as client acceptance and continuance, compliance with professional standards, and maintenance of appropriate documentation, among others. As part of those responsibilities, paragraph .34 of AT-C section 105 states that the engagement partner should be satisfied that all members of the engagement team, including external specialists, have the competence and capabilities to perform the engagement in accordance with professional standards and applicable legal and regulatory requirements. Chapter 2 discusses assessing the competence and capabilities that members of the engagement team need to possess to perform a SOC 2 examination.

1.99 Additionally, paragraph .36 of AT-C section 105 states that the engagement partner should remain alert, through observation and making inquiries as necessary, for evidence of noncompliance with relevant ethical requirements by members of the engagement team. If matters come to the engagement partner's attention through the firm's system of quality control or otherwise that indicate that members of the engagement team have not complied with relevant ethical requirements, the engagement partner, in consultation with others in the firm, should determine the appropriate action.

Definitions

1.100 Definitions of the terms used in this guide are included in appendix H, "Definitions."

---

[29] All QM sections can be found in AICPA *Professional Standards*.

Chapter 2

Accepting and Planning a SOC 2 Examination

Service organization management and the service auditor each have specific responsibilities in a SOC 2 examination. This chapter describes the service auditor's responsibilities, including the preconditions of engagement acceptance and the need to obtain a written assertion from and establish an understanding about the terms of the engagement with management. As part of establishing the terms of the engagement, the service auditor should understand management's responsibilities in the engagement; therefore, this chapter also provides a brief overview of management's responsibilities.

Introduction

2.01 AT-C section 105, *Concepts Common to All Attestation Engagements*,[1] establishes certain preconditions prior to accepting a SOC 2 examination. Among other things, those preconditions include the service auditor determining whether the engagement team meets the ethical and competency requirements set forth in the professional standards and whether the engagement meets the relevant requirements of the attestation standards. AT-C section 105 also addresses establishing an understanding with service organization management.

2.02 Once an engagement has been accepted, AT-C section 205, *Assertion-Based Examination Engagements*, sets forth the requirements for developing an overall strategy and planning the engagement. This chapter discusses considerations for accepting and planning a SOC 2 examination.

Understanding Service Organization Management's Responsibilities

2.03 In accordance with paragraph .29 of AT-C section 105, the service auditor should accept a SOC 2 examination only when the service auditor has reached a common understanding with service organization management about the terms of the engagement. Paragraph .08 of AT-C section 205 indicates that these terms should include the responsibilities of both management and the service auditor. This section provides an overview of management's responsibilities. Because many of the decisions service organization management makes prior to engaging the service auditor can affect the nature, timing, and extent of procedures the service auditor performs, this section also discusses those aspects of management's responsibilities.

Management Responsibilities Prior to Engaging the Service Auditor

2.04 Service organization management is responsible for having a reasonable basis for asserting that (*a*) the description of the service organization's

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

system is presented in accordance with the description criteria, (*b*) the controls stated in the description were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and (*c*) in a type 2 examination, those controls were operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Management's assertion is based, in part, on management having (*a*) identified the service commitments and system requirements, (*b*) identified and analyzed the risks that threaten the achievement of those service commitments and system requirements, and (*c*) designed, implemented, and operated controls that provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria.

2.05 Service organization management[2] is responsible for making a variety of decisions that affect the nature, timing, and extent of procedures to be performed in a SOC 2 examination, including the following:

- Defining the scope of the examination, which includes the following:
  - — Identifying the services provided to user entities, which will establish the subject matter of the examination
  - — Identifying the system used to provide those services
  - — Identifying the boundaries of the system
  - — Identifying the risks from business partners providing intellectual property or services to the service organization related to the system
  - — Selecting the trust services category or categories to be included within the scope of the examination
  - — Determining the type (type 1 or type 2) of SOC 2 examination to be performed
  - — Determining the period to be covered by the examination or, in the case of a type 1 report, the specified "as of" date
  - — If services are provided to the service organization by other entities, evaluating the effect of those services on the service organization's achievement of its service commitments and system requirements and concluding whether those other entities are subservice organizations (paragraph 2.07)
  - — Determining whether subservice organizations, if any, are to be addressed in the report using the inclusive method or the carve-out method (paragraph 2.14)
  - — If a subservice organization is to be presented using the inclusive method, obtaining agreement from subservice

[2] In a SOC 2 engagement, service organization management is the responsible party. This guide uses the terms *service organization management* and *responsible party* interchangeably. In most cases, but not all, service organization management is also the engaging party. This guide also provides guidance for situations in which service organization management is not the engaging party and there are specific requirements for such an engaging party.

organization management to participate in the examination

- Specifying the principal service commitments made to user entities and the system requirements needed to operate the system
- Specifying the principal system requirements related to commitments made to business partners
- Identifying and assessing risks that could prevent the service organization from achieving its service commitments and system requirements
- Designing, implementing, operating, monitoring, and documenting controls that are suitably designed and, in a type 2 examination, operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria
- Identifying known system incidents that
  - were the result of controls that were not suitably designed or operating effectively or
  - otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements

2.06 Before service organization management can fulfill those responsibilities, management may need clarification of certain matters from the service auditor. For example, management may have questions about whether certain processes are part of the system used to provide the services, whether a vendor is a subservice organization, and what factors to consider in determining whether to use the inclusive or the carve-out method to present information about a subservice organization. When providing assistance to management, the service auditor needs to exercise care that the service auditor's independence is not impaired by taking on the role of management, otherwise assuming management responsibilities, or being placed in a position of evaluating the service auditor's own work. Independence is discussed beginning in paragraph 2.41.

Considerations in Identifying Subservice Organizations

2.07 Most entities, including service organizations, outsource various functions to other organizations (vendors). The functions provided by these vendors may affect the delivery of services to user entities. Although management can delegate responsibility for these functions, management retains responsibility for the achievement of the service organization's service commitments and system requirements. When controls at the vendors are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria, the vendor is considered a *subservice organization*. A subservice organization may be a separate entity that is external to the service organization or may be a related entity, for example, a subservice organization that is a subsidiary of the same entity that owns the service organization.

2.08 In this guide, a vendor is considered a subservice organization only if the following apply:

- The services provided by the vendor are likely to be relevant to report users' understanding of the service organization's system as it relates to the applicable trust services criteria.
- Controls at the vendor are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria.

2.09 If the service organization's controls alone provide reasonable assurance that its service commitments and system requirements are achieved, or if the service organization's monitoring of the vendor's services and controls is sufficient to provide reasonable assurance that its service commitments and system requirements are achieved, the vendor's controls over its services are not likely to be relevant to the SOC 2 examination. Although service organization management is responsible for determining whether one or more of its vendors are considered subservice organizations, it is important that the service auditor agree with management's determinations.

2.10 Determining whether a vendor is a subservice organization is easy in some situations but not in others. The following examples may be helpful when evaluating management's conclusion as to whether a vendor is considered a subservice organization:

- ABC Vendor is responsible for performing quarterly maintenance on the service organization's backup power system; service organization personnel participate in post-maintenance testing used to verify the backup power system is working as intended, which serves as a primary control. In this instance, ABC Vendor's controls are not necessary for the service organization to achieve its service commitments and system requirements based on the applicable trust services criteria for availability; therefore, ABC Vendor would not be considered a subservice organization.
- XYZ Vendor is responsible for monitoring service capacity and usage and for projecting future capacity demands based on historical trends. Without additional controls at the service organization, controls at the vendor are necessary for the service organization to achieve its service commitments and system requirements related to availability based on the applicable trust services criteria. Therefore, XYZ Vendor would be considered a subservice organization. However, if the service organization were to independently perform high-level capacity monitoring activities and review the future capacity demands projected by XYZ Vendor for appropriateness, XYZ Vendor might not be considered a subservice organization because the vendor's controls may not be necessary for the service organization to achieve its service commitments and system requirements based on the applicable trust services criteria. The service auditor would need to use judgment to determine whether the review controls were precise enough that the vendor controls would not be necessary.

- A service organization outsources its application development testing to DEF Vendor and contractually specifies that certain controls be executed by DEF Vendor. The service organization designates a service organization employee to oversee the outsourced services, and that employee compares DEF Vendor's test plans, test scripts, and test data to the service organization's application change requests and detailed design documents. The designated service organization employee also reviews the results of testing performed by DEF Vendor before approving changes to the application and submitting them to the service organization for user acceptance testing. In this instance, even though the controls expected to be performed by DEF Vendor are stipulated in the contract, management concluded and the service auditor concurred that the controls at DEF Vendor are not necessary for the service organization to assert that its controls provide reasonable assurance that the service organization's availability commitments were achieved based on the applicable trust services criteria. Because the controls are not necessary, DEF Vendor would not be considered a subservice organization.
- A service organization purchases from JKL Vendor a tool to monitor and report on the status of configuration settings that affect the operation of control activities. JKL Vendor also provides services around the use of that tool through a software-as-a-service (SaaS) model. In this situation, management has effectively outsourced monitoring of the configuration settings to JKL Vendor. Because management considers this function and related controls necessary to the achievement of the service organization's service commitments and system requirements, JKL Vendor would be considered a subservice organization.

Management's Use of Specialists

2.11 Increasingly, service organizations are using external specialists (management's specialists)[3] to leverage knowledge, technologies, experience, and expertise not resident within the service organization. If information produced by the management's specialist is used by the service auditor, the service auditor may need to perform further procedures to determine if such information is sufficiently reliable for the service auditor's purposes, as discussed further in paragraph 3.145. Such management's specialists may include the following:

- Security penetration testers
- Cybersecurity breach investigators
- Software vulnerability scanning service providers
- Disaster recovery simulation providers

---

[3] The term *management's specialist*, as used in this guide, is defined as an individual or organization possessing expertise in a field other than accounting or attestation, whose work in that field is used by the service organization to assist the service organization in preparing the description or enhancing the effectiveness of controls. Although this term is not used in the attestation standards, this definition is consistent with that in AU-C section 620A, *Using the Work of an Auditor's Specialist*. A management's specialist is separate and distinct from a *service auditor's specialist* as described in paragraph .37 of AT-C section 205 and paragraph 2.176 of this guide.

All AU-C sections can be found in AICPA *Professional Standards*.

2.12 In some situations, service organization management engages a management's specialist to provide information about the operation of controls that will assist management in enhancing the effectiveness of the service organization's controls. Determining whether management's specialist is also a subservice organization is not always clear cut. Factors that may be useful to management and the service auditor when determining whether a management's specialist is also a subservice organization include the following:

- *Significance of management's specialist services*. When the services provided by a management's specialist include controls (such as remediation of identified vulnerabilities in the service organization's key IT infrastructure when the specialist has been engaged to provide software vulnerability scanning services) that are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria, the management's specialist is likely to be considered a subservice organization.
- *Regularity of services being provided*. A management's specialist engaged to perform services on a regular rather than an ad hoc basis is more likely to be considered a subservice organization.

Regardless of whether management's specialist is considered a subservice organization, management is responsible for oversight of the specialist's work.

2.13 If the management's specialist is a subservice organization, the service organization's description of its system would include the information set forth in description criterion DC7 presented in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*.[4] That information varies depending on whether the inclusive or carve-out method is used with respect to the subservice organization.

Considerations in Determining Whether to Use the Inclusive or Carve-Out Method

2.14 If the service organization uses a subservice organization, service organization management is responsible for determining whether to use the carve-out or inclusive method when addressing the subservice organization in the description of the system. Service organization management may need assistance from the service auditor to understand the differences between the two methods and the implications that arise from the choice of one method over the other. The two methods are defined as follows:

- *Carve-out method*. Method of addressing the services provided by a subservice organization in which the components of the subservice organization's system used to provide the services to the service organization are excluded from the description of the service organization's system and from the scope of the examination. However, the description identifies
  - — the nature of the services performed by the subservice organization;

[4] All DC sections can be found in AICPA *Description Criteria*.

- the types of controls expected to be performed at the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and
- the controls at the service organization used to monitor the effectiveness of the subservice organization's controls.

- *Inclusive method*. Method of addressing the services provided by a subservice organization in which the description of the service organization's system includes a description of
  - the nature of the services provided by the subservice organization;
  - the components of the subservice organization's system used to provide services to the service organization, including the subservice organization's controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and
  - the controls at the service organization used to monitor the effectiveness of the subservice organization's controls.

  Note that when using the inclusive method, controls at the subservice organization are subject to the service auditor's examination procedures. Because the subservice organization's system components are included in the description, those components are included in the scope of the examination.

2.15 When a service organization uses multiple subservice organizations, it may prepare its description using the carve-out method for one or more subservice organizations and the inclusive method for others.

2.16 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 report users is not available from the subservice organization.
- Information about the subservice organization is not readily available from other sources.

2.17 Although the inclusive method provides more information for report users than the carve-out method, the inclusive method would not be appropriate in situations in which the service auditor is not independent of both the service organization and the subservice organization because they are both responsible parties under this method. Independence is discussed further in paragraph 2.43.

2.18 Examples of circumstances in which the use of the carve-out method may be the most practical approach include the following:

a. The challenges entailed in implementing the inclusive method, which are described in paragraphs 2.101–.102, are sufficiently onerous that it is not practical to use the inclusive method.

b. A service auditor's report on the subservice organization that meets the needs of report users is available. (Management of the service organization may need to work with the subservice organization to obtain authorization to redistribute the subservice organization's SOC 2 report or establish a process by which the subservice organization distributes a copy of its SOC 2 report to the service organization's report users.)

c. The service organization is unable to obtain a contractual or other commitment from the subservice organization regarding its willingness to be included in the SOC 2 examination.

2.19 In some cases, the subservice organization's services and controls have a pervasive effect on the service organization's system. In these circumstances, it is important that management and the service auditor consider whether the use of the carve-out method may result in a description of the service organization's system that is so limited that it may be misleading to the intended users of the report. In such situations, the service organization's system alone may not be an appropriate subject matter. Examples of circumstances in which a SOC 2 report that uses the carve-out method may be misleading include the following:

- A significant portion of the system used to provide services to users is operated by the subservice organization.
- The achievement of the service organization's service commitments and system requirements depends primarily on controls performed by the subservice organization.
- It is unlikely that users of the SOC 2 report would be able to obtain information about the design and, in a type 2 examination, the operating effectiveness of controls at the subservice organization through other means.

Considerations in the Identification of Complementary Subservice Organization Controls

2.20 As discussed earlier, a vendor is considered a subservice organization when controls performed by the subservice organization are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements can be achieved based on the applicable trust services criteria. When the inclusive method is used, management would describe those controls in the system description with the assistance of the subservice organization. When the carve-out method is used, however, service organization management would disclose only the *types of controls* the subservice organization is expected to implement. These controls are referred to as *complementary subservice organization controls* (CSOCs).

2.21 Examples of the types of CSOCs the subservice organization is expected to have implemented may include the following:

- Controls relevant to the completeness, accuracy, and timeliness of transaction processing on behalf of the service organization

- Controls relevant to the completeness, accuracy, and timeliness of specified reports provided to and used by the service organization
- Logical access controls relevant to the processing performed for the service organization
- Controls over the procedures to detect and respond to potential system incidents
- The processes in place to communicate significant system incidents and deviations in the effectiveness of controls to service organization management
- The risk assessment process and the policies and procedures implemented to mitigate those risks
- Activities such as internal audit procedures or quality control reviews that the subservice organization has in place to monitor the effectiveness of its control activities

Service organization management may request the service auditor's assistance when determining how to present the CSOCs in the description of the system. In this case, the service auditor may provide examples of CSOC disclosures made by others and make recommendations to improve the presentation of the CSOCs in the description. The ultimate decision about what to disclose, however, rests with service organization management.

2.22 Chapter 3, "Performing the SOC 2 Examination," discusses the service auditor's responsibilities for obtaining an understanding of CSOCs in the examination and for determining whether disclosures about CSOCs in the description are presented in accordance with the description criteria.

Considerations in Identifying Complementary User Entity Controls and User Entity Responsibilities

2.23 Usually, user entities must perform specific activities to benefit from the services of a service organization. Such activities may include specifying the configuration of services to be provided, submitting authorized input for processing, managing user entity employee access to data, and reviewing the outputs of processing. These activities may be specified in agreements between the user entity and the service organization, user manuals, and other communications. Most of these activities are needed for the user entity to derive value from the services but do not affect the ability of the service organization to achieve its service commitments and system requirements. This guide refers to such activities as *user entity responsibilities*.

2.24 In contrast, when a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements would be achieved without the user entity performing certain controls in a defined manner, those controls are referred to as *complementary user entity controls* (CUECs). Service organization management expects the user entity to implement CUECs completely and accurately in a timely manner.

2.25 In most circumstances, a service organization's controls alone are sufficient to enable the achievement of its service commitments or system requirements. This is because, when making its service commitments, management only makes commitments that it is able to control. Similarly, system requirements are generally derived only from those commitments that are the

service organization's responsibility. Therefore, management typically does not identify CUECs to be implemented by user entities.

2.26 For example, when considering the achievement of a service commitment to provision user credentials based on instructions from the user entity, service organization management may consider the controls that would be necessary based on trust services criterion CC6.2, *Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized*. Trust services criterion CC6.2 requires only that the system register a user (a user identified by the user entity as an *authorized user*) and issue system credentials to that user after the user entity supplies the service organization with a list of authorized users. If the user entity supplies the service organization with a list of authorized users and inadvertently includes employees who should not have access, the service organization has still met both trust services criterion CC6.2 and its service commitment to the user entity. Because providing the service organization with a list of authorized users is necessary for the user entity to benefit from the services provided by the service organization, it is a user entity responsibility. However, because the service organization's controls provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criterion without such information, or without such information being complete and accurate, identifying the authorized users and communicating that information to the service organization are not considered CUECs.

2.27 In other situations, controls at the user entity may be necessary for the service organization's controls to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. Consider, for example, controls relevant to trust services criterion CC6.4, *The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to achieve the entity's objectives*. A service organization may install portions of its infrastructure at a user entity (for example, servers installed at user entity data centers to support the transmission of files between the user entity and the service organization). In these circumstances, the user entity needs to implement physical access controls to protect the components of the service organization's system located at the user entity.

2.28 Although there is no prescribed format for presenting CUECs in the system description, they are typically included at the end of the system description or at the end of the section that includes the service auditor's description of tests of controls and results and are related to specific trust services criteria. To assist report users in understanding their role in the system, CUECs may also be associated with the specific service commitments or system requirements to which they relate.

Considerations in Identifying Controls That a Subservice Organization Expects the Service Organization to Implement

2.29 In addition to the controls that the service organization expects the subservice organization to implement (CSOCs), there may be activities that a subservice organization expects the service organization, as a user entity, to

perform for the subservice organization's controls to be effective. When a subservice organization undergoes a SOC 2 examination, such activities may be identified in the section of the service organization's description that describes CUECs. This would be the case when the subservice organization's controls cannot provide reasonable assurance that its commitments to the service organization (user entity) would be achieved without the service organization performing certain controls in a defined manner. For example, a service organization may outsource aspects of its technology infrastructure to a subservice organization that maintains its servers in the service organization's data center facilities. In this situation, service organization management may find the following CUEC identified in the SOC 2 report obtained from the subservice organization:

> User entities should have controls in place to restrict physical access to data center facilities to authorized user entity personnel.

2.30 To address that CUEC, service organization management might include in its description the following controls:

- Access to the data center requires a documented access request form and manager approval prior to access being provisioned.
- A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.
- Access to the data center is reviewed quarterly by management.
- Persons are identified and authenticated through the badging access system prior to accessing the data center.

2.31 In addition to the CUECs, the subservice organization may also identify user entity responsibilities that should be considered by the service organization to effectively use the subservice organization's system but that do not affect the subservice organization's ability to achieve its commitments to the service organization. Such activities may also be described in user documentation published by the subservice organization or in the agreement between the service organization and subservice organization.

Management Responsibilities During the Examination

2.32 During the SOC 2 examination, service organization management is responsible for the following:

- Preparing a description of the service organization's system, including the completeness, accuracy, and method of presentation of the description
- Providing a written assertion that accompanies the description of the service organization's system, both of which will be provided to report users
- Identifying the risks that threaten the service organization's achievement of its service commitments and system requirements stated in the description
- Designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the service commitments and system requirements will be achieved based on the applicable trust services criteria
- Having a reasonable basis for its assertion

- If the service auditor plans to use internal auditors to provide direct assistance, providing the service auditor with written acknowledgment that internal auditors providing direct assistance to the service auditor will be allowed to follow the service auditor's instructions and that the service organization will not intervene in the work the internal auditors perform for the service auditor
- Providing the service auditor with the following:
  - Access to all information, such as records, documentation, service-level agreements, and internal audit or other reports, that management is aware of and that is relevant to the engagement
  - Access to additional information that the service auditor may request from management for purposes of the engagement
  - Unrestricted access to personnel within the service organization from whom the service auditor determines it is necessary to obtain evidence relevant to the SOC 2 examination
- Disclosing to the service auditor the following:
  - Incidents of noncompliance with laws and regulations, fraud, or uncorrected misstatements that are clearly not trivial and that may affect one or more user entities and whether such incidents have been communicated appropriately to affected user entities
  - Knowledge of any actual, suspected, or alleged fraud or noncompliance with laws and regulations affecting the description, suitability of design of controls, or, in a type 2 examination, operating effectiveness of controls
  - All deficiencies in the design of controls of which management is aware
  - All instances in which controls have not operated as described
  - All identified system incidents that were the result of controls that were not suitably designed or operating effectively or resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements as of the date of the description (for a type 1 examination) or during the period of time covered by the description (for a type 2 examination)

2.33 Management acknowledges these responsibilities in an engagement letter or other suitable form of written communication. Further information about management's responsibilities in the SOC 2 examination can be found on the AICPA website.

2.34 In a SOC 2 examination in which the service organization uses the services of a subservice organization and management elects to use the inclusive method to present certain information about the services provided by the subservice organization, subservice organization management is also responsible for many of the matters described in paragraph 2.32 as they relate to the

subservice organization. Accordingly, during planning, the service auditor determines, with the assistance of service organization management, whether it will be possible to obtain (*a*) an assertion from subservice organization management and (*b*) evidence that supports the service auditor's opinion on the subservice organization's description of its system, the suitability of design of controls, and in a type 2 examination, the operating effectiveness of the subservice organization's controls (including written representations from management of the subservice organization). If subservice organization management will not provide a written assertion and appropriate written representations, service organization management will be unable to use the inclusive method but may be able to use the carve-out method. Additional guidance on the use of the inclusive method is provided beginning in paragraph 2.101.

Management's Responsibilities During Engagement Completion

2.35 The responsibilities of management of the service organization toward the end of the engagement include the following:

- Modifying the description, if appropriate (Chapter 4, "Forming the Opinion and Preparing the Service Auditor's Report," describes a few situations in which the service auditor would generally recommend that management modify the description.)
- Modifying management's written assertion, if appropriate (See discussion beginning at paragraph 3.257.)
- Providing the service auditor with written representations (See discussion beginning at paragraph 3.229.)
- Disclosing to the service auditor any known events, subsequent to the period covered by the description of the service organization's system, up to the date of the service auditor's report, that would have a material effect on the description, suitability of design of controls, and in a type 2 engagement, operating effectiveness of controls (See discussion beginning at paragraph 3.245.)

Responsibilities of the Service Auditor

2.36 During engagement acceptance and planning, the service auditor is responsible for the following:

- Determining whether to accept or continue an engagement for a particular client. In making this determination, the service auditor needs to consider whether the preconditions for accepting an examination as discussed in paragraphs .26–.27 of AT-C section 105 have been met (see paragraph 2.51)
- Agreeing on the terms of the engagement with service organization management, including establishing an understanding about the responsibilities of management and the service auditor (see paragraph 2.76)
- Reaching an understanding with management regarding management's willingness and ability to provide a written assertion at the conclusion of the examination (see paragraph 2.72)
- Establishing an overall strategy for the examination that sets the scope, timing, and direction of the engagement and guides the development of the engagement plan, including the consideration of

materiality and the identification of the risks of material misstatement (see paragraph 2.97)

- Performing procedures to assess the risk of material misstatement, including obtaining an understanding of the service organization's system and how the system controls were designed, implemented, and operated to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria (see paragraph 2.108)

Engagement Acceptance and Continuance

2.37 With respect to the acceptance and continuance of client relationships and specific engagements, paragraph .27 of QM section 10A, *A Firm's System of Quality Control*,[5] states that the firm should establish policies and procedures for the acceptance and continuance of client relationships and specific engagements that are designed to provide the firm with reasonable assurance that it will undertake or continue relationships and engagements only when the firm

a. is competent to perform the examination and has the capabilities, including time and resources, to do so;

b. can comply with legal and relevant ethical requirements; and

c. has considered the integrity of the client and does not have information that would lead it to conclude that the client lacks integrity.

2.38 The quality control requirements for competence and ethical behavior are reiterated in paragraph .29 of AT-C section 105, which indicates that the service auditor should accept or continue a SOC 2 examination only when the service auditor

a. has no reason to believe that relevant ethical requirements, including independence, will not be satisfied.

b. is satisfied that those persons who are performing the engagement collectively have the appropriate competence and capabilities. (See paragraph 2.46.)

c. has determined that the engagement to be performed meets all the preconditions for an attestation engagement. (See paragraph 2.51.)

d. has reached a common understanding with the engaging party[6] of the terms of the engagement, including the service auditor's reporting responsibilities. (Chapter 4 discusses reporting in a SOC 2 examination.)

2.39 According to paragraph .A12 of QM section 10A, matters to consider when evaluating the integrity of a client include the identity and business reputation of the principal owners of the service organization, key service organization management, and those charged with governance.

---

[5] All QM sections can be found in AICPA *Professional Standards*.

[6] The engaging party is the party or parties that engage the service auditor to perform the examination. In the examination discussed in this guide, service organization management is often, but not always, the engaging party.

2.40 The service auditor may also consider whether management has realistic expectations about the examination or whether the service organization may experience significant negative consequences if the service auditor's opinion is qualified because of a lack of appropriate controls and related documentation. In such situations, the service auditor may choose to decline the engagement.

Independence

2.41 Independence, as defined by the AICPA Code of Professional Conduct (code), is required for examination-level engagements to report on controls at a service organization. The independence assessment process addresses matters such as scope of services, fee arrangements, firm and individual financial relationships, firm business relationships, and alumni and familial relationships with the client and client personnel.

2.42 The "Independence Rule" (ET sec. 1.200.001)[7] of the AICPA Code of Professional Conduct establishes independence requirements for attestation engagements. The "Independence Standards for Engagements Performed in Accordance With Statements on Standards for Attestation Engagements" subtopic (ET sec. 1.297) of the "Independence Rule" establishes independence requirements for a service auditor who provides services under the attestation standards. In addition, the "Conceptual Framework Approach" subtopic (ET sec. 1.210) of the "Independence Rule" discusses threats to independence not specifically detailed elsewhere. The "Independence Rule" is followed by interpretations of the rule that assist the service auditor in assessing independence. The code specifies that, in some circumstances, no safeguards can reduce an independence threat to an acceptable level. For example, the code specifies that a covered member may not own even an immaterial direct financial interest in an attest client because there is no safeguard to reduce the self-interest threat to an acceptable level. A member may not use the conceptual framework to overcome this prohibition or any other prohibition or requirement in an independence interpretation.

2.43 When performing engagements in accordance with the attestation standards, in which independence is required, the service auditor needs to be independent with respect to the responsible party (or parties), as defined in those standards. If the service organization uses a subservice organization, and management elects to use the inclusive method to present certain information about the subservice organization in its description of the service organization's system, subservice organization management is also a responsible party. Consequently, in accordance with paragraph .26 of AT-C section 105, the service auditor should also be independent of the subservice organization. The service auditor need not be independent of each user entity of the service organization.

2.44 When the service auditor is not independent but is required by law or regulation to accept the engagement, paragraph .06 of AT-C section 205 states that the service auditor should disclaim an opinion and should specifically state that the service auditor is not independent. The service auditor is neither required to provide, nor precluded from providing, the reasons for the lack of independence; however, if the service auditor chooses to provide the reasons for

[7] All ET sections can be found in AICPA *Professional Standards*.

the lack of independence, the service auditor should include all the reasons therefor.

IT Services

2.45 The AICPA code describes situations in which there are threats to independence when a practitioner is engaged to design, develop, or implement information systems for an attest client. This guidance may be particularly relevant in engagements where the subject matter is systems and controls such as a SOC 2 engagement. For example, a service organization may implement a governance, risk, and compliance (GRC) tool that includes functionality supporting the identification of threats and vulnerabilities, monitoring the implementation of key software settings, monitoring the effectiveness of automated controls, and accumulating, recording, and maintaining evidence of the operation of controls. If the service organization asks the service auditor for assistance with the design, implementation, or integration of the GRC tool, the service auditor should assess whether self-review and management participation threats to the service auditor's independence exist based on the "Independence Standards for Engagements Performed in Accordance With Statements on Standards for Attestation Engagements" subtopic. Independence is further discussed in paragraph 2.41.

Competence of Engagement Team Members

2.46 Chapter 1, "Introduction and Background," of this guide discusses quality in the SOC 2 examination. Maintaining appropriate quality in the engagement involves having the work performed by engagement team members who have the appropriate competence and capabilities. For that reason, as discussed in paragraph 2.37, the service auditor should not accept the SOC 2 examination unless it has been determined that the individuals who would perform the engagement have the appropriate competence and capabilities to perform it.

2.47 When considering the competence and capabilities of engagement team members, paragraph .34 of AT-C section 105 indicates that the engagement partner should be satisfied that the team and any service auditor's external specialists assigned to the engagement collectively have the appropriate competence or capabilities. Such competencies and capabilities include the following:

- An understanding, or the ability to obtain an understanding, of systems used to provide services, including operating and security of such systems, gained either through experience with engagements of a similar nature and complexity or through appropriate training and participation
- Knowledge of the service organization's industry and business, including whether the industry in which the service organization operates is subject to specific types of or unusual security risks
- An understanding of business processes, risks, and controls
- Knowledge of relevant IT systems and technology, such as CPUs, networking, firewalls or firewall techniques, security protocols, operating systems, and databases
- Knowledge of any uncommon technologies or industry-specific technologies used by the service organization

- An understanding of IT processes and controls, such as the management of operating systems, networking, and virtualization software and related security techniques; security principles and concepts; software development; and incident management and information risk management
- Experience with evaluating the suitability of design and operating effectiveness of controls relevant to security, availability, processing integrity, confidentiality, and privacy
- An understanding of professional standards and the ability to apply professional skepticism and judgment in the examination
- An understanding of the description criteria and trust services criteria used in the engagement
- An understanding of legal and regulatory requirements relevant to the examination

2.48 In addition, in accordance with paragraph .34 of AT-C section 105, the engagement partner should be satisfied that team members are informed of their responsibilities, including the objectives of the procedures that they are to perform and matters that may affect the nature, timing, and extent of such procedures. The engagement partner should also be satisfied that engagement team members have been directed to bring to the partner's attention any significant questions raised during the engagement.

2.49 The engagement partner may decide to supplement the knowledge and skills of the engagement team with the use of specialists. Planning to use the work of a service auditor's specialist is discussed in paragraph 2.176.

2.50 As a member of the engagement team, the engagement partner also needs to have appropriate competence and capabilities to issue an appropriate service auditor's report based on the engagement's particular circumstances. In accordance with paragraph .35 of AT-C section 105, the engagement partner also takes responsibility for overall quality on each engagement, which includes responsibility for the following:

a. Appropriate procedures being performed regarding the acceptance and continuance of client relationships and engagements

b. The engagement being planned and performed (including appropriate direction and supervision) to comply with professional standards and applicable legal and regulatory requirements

c. Reviews being performed in accordance with the firm's review policies and procedures and reviewing the engagement documentation on or before the date of the service auditor's report

d. Appropriate engagement documentation being maintained to provide evidence of achievement of the service auditor's objectives and that the engagement was performed in accordance with the attestation standards and relevant legal and regulatory requirements

e. Appropriate consultation being undertaken by the engagement team on difficult or contentious matters

Preconditions of a SOC 2 Engagement

2.51 In accordance with paragraph .29 of AT-C section 105, the service auditor should accept or continue an engagement to examine and report on

controls at a service organization only if the preconditions for an attestation engagement identified in paragraphs .26–.27 of AT-C section 105 are met:

a. The service auditor is independent in accordance with the attestation standards. (See paragraph 2.41.)

b. Management accepts responsibility for the

i. preparation of the description of the service organization's system in accordance with the description criteria and

ii. suitability of design of controls and the operating effectiveness of controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

c. The subject matters of the SOC 2 examination are appropriate. (The subject matters of SOC 2 examinations are discussed beginning at paragraph 1.05; determining whether the subject matters are appropriate is discussed beginning at paragraph 2.52.)

d. The criteria used to prepare and evaluate the description and controls are both suitable and available to users of the report. (The suitability and availability of both the description criteria and the trust services criteria are discussed at paragraphs 1.42 and 1.47; the appropriateness of the principal service commitments and system requirements stated in the description is discussed beginning at paragraph 2.66.)

e. The service auditor expects to be able to obtain the evidence needed to arrive at the opinion on the description, suitability of design of controls, and in a type 2 examination, operating effectiveness of controls and will have

i. access to all information relevant to the engagement;

ii. access to additional information that the service auditor may request; and

iii. unrestricted access to service organization personnel.

f. The service auditor's opinion, in a form appropriate to the engagement, is to be contained in the service auditor's written examination report.

Determining Whether the Subject Matter Is Appropriate for the SOC 2 Examination

2.52 The information contained in the description of a service organization's system, the suitability of design of controls, and in a type 2 examination, the operating effectiveness of the controls, which are the subject matters of a SOC 2 examination, are relevant to user entities, business partners, and the other parties specified in the SOC 2 report. Consequently, those subject matters are usually appropriate for a SOC 2 examination. However, the determination of the appropriateness of the subject matters, as discussed further later, may be affected in certain situations. In such situations, in accordance with paragraph .27 of AT-C section 105, the service auditor should determine the appropriateness of the subject matter before accepting the engagement.

2.53 Paragraph .A39 of AT-C section 105 states that subject matter is appropriate if it is (*a*) identifiable and capable of consistent measurement or evaluation against the criteria and (*b*) can be subjected to procedures for obtaining

sufficient appropriate evidence to support an opinion. In a SOC 2 examination, consideration of whether the subject matter is appropriate involves consideration of whether the system used to provide the services is identifiable. For instance, the boundaries of a system addressed by a SOC 2 examination may not be as clear as the boundaries of a financial reporting system addressed by a SOC 1 examination; therefore, before accepting a SOC 2 examination, the service auditor and management need to agree on the system being reported on and its boundaries. In doing so, management and the service auditor consider the relationship between the boundaries of each of the components of the system used to provide the services, as discussed in paragraph 1.25.

2.54 In considering whether to accept a type 2 SOC 2 engagement, in accordance with paragraph .27 of AT-C section 105, the service auditor should also consider whether sufficient evidence of the effective operations of controls is likely to be available for the period of time covered by the examination. If the period of time is too short, sufficient appropriate evidence may not be available and the subject matter may not be appropriate. Consider the following examples:

- Service organization management wishes to engage the service auditor to perform a type 2 examination for a period of less than two months. In this situation, the service auditor may conclude that it is unlikely that sufficient appropriate evidence can be obtained to support an opinion on design and operating effectiveness of controls; therefore, the subject matter would not be appropriate for the examination.
- Service organization management requests a SOC 2 report for a period that covers nine months. In this situation, although there may be a risk that annual controls do not operate during the examination period, the service auditor may conclude that it is likely that sufficient appropriate evidence can be obtained to support an opinion on design and operating effectiveness of controls. (Paragraph 3.176 provides guidance for situations in which an annual control did not operate during the period covered by the examination.)

2.55 When the subject matter of the engagement relates to only one part of a broader subject matter, paragraph .A43 of AT-C section 105 indicates that it may be appropriate for the service auditor to consider whether information about the aspect that the service auditor is asked to examine is likely to meet the information needs of intended users. In this case, the service auditor may question accepting the engagement. Factors to consider in this consideration include the functions performed by the system within the context of how user entities make use of the services, the extent of the use of subservice organizations and the importance and complexity of their services, how information about subservice organizations will be presented in the description of the service organization's system (inclusive or carve-out method), and the relevance to the system of the trust services category or categories included within the scope of the examination to the information needs of user entities.

2.56 For example, assume a service organization functions primarily as an intermediary between user entities and a subservice organization and performs few or no functions related to the services it provides them. If the service organization's controls do not materially contribute to the achievement of the subservice organization's service commitments and system requirements, a

report on that service organization's controls that carves out the subservice organization is unlikely to meet the information needs of intended users and would, consequently, not be an appropriate subject matter. In contrast, assume a service organization that provides fleet management services including providing vehicles, maintenance of those vehicles, fuel services, and carbon footprint reporting wants an examination that addresses only the processing integrity of its carbon footprint reporting services. When evaluating whether this represents an appropriate subject matter, the service auditor would consider whether the requested engagement is likely to meet the information needs of the intended users of the report. If the service auditor concludes that the boundaries of the system related to carbon footprint reporting are identifiable and the services within those boundaries can be subject to procedures to obtain sufficient appropriate evidence, the service auditor may be able to conclude that the carbon footprint reporting services are an appropriate subject matter. If the service auditor concludes that the requested engagement is likely to meet the information needs of only a subset of the intended users and, consequently, the subject matters of the report are appropriate only for that subset of users, the service auditor may conclude that the engagement may be accepted with use of the report restricted to that subset of users.

2.57 The service auditor may also consider whether the intended users of the report are likely to understand the nature of the examination, the criteria used, and the tests performed and results thereof (for example, acceptable deviation rates or inherent limitations on the effectiveness of controls). If intended users are unlikely to understand that information, a greater potential exists for them to misunderstand the report; in that case, the service auditor may decide not to accept the examination.

Determining Whether Service Organization Management Is Likely to Have a Reasonable Basis for Its Assertion

2.58 Service organization management is responsible for having a reasonable basis for its assertion about the description, suitability of design of controls and, in a type 2 engagement, operating effectiveness of controls stated therein. Furthermore, because management's assertion generally addresses the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls over a period of time, management's basis for its assertion covers the same time frame. Having a reasonable basis necessitates the performance of risk assessment, the implementation of effective processes and controls to mitigate identified risks, and the performance of controls and other activities to monitor the effectiveness of such controls. Also inherent is the assumption that service organization management possesses the necessary skills and competence to perform these functions. Such skills and competence are necessary to enable management to oversee the work of vendors, management's specialists, and other third parties who assist management with the effective operation of internal control. The procedures performed by the service auditor during a type 1 or type 2 examination are not considered a basis for management's assertion because the service auditor is not part of the service organization's internal control. In accordance with paragraph .10 of AT-C section 205, the service auditor should use professional judgment in determining whether management has a reasonable basis for making its assertion.

2.59 AT-C section 205 does not include specific requirements for the service auditor to perform procedures to determine whether management has a

reasonable basis for its assertion. Because of the relationship between (*a*) the evaluation of the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls and (*b*) monitoring, the service auditor ordinarily discusses the basis for its assertion with management prior to engagement acceptance. This assists the service auditor in determining whether the basis appears reasonable for the size and complexity of the service organization and whether the service auditor expects to be able to obtain sufficient appropriate evidence to arrive at the opinion, which is also a precondition of the examination.

2.60 Management's basis for its assertion usually relies heavily on monitoring of controls. Such monitoring activities typically include ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are ordinarily built into the normal recurring activities of the service organization. Monitoring activities are particularly important because the service organization frequently interacts with third parties such as user entities, business partners, subservice organizations, vendors, and others who have access to the service organization's system or otherwise transmit information back and forth between, or on behalf of, the service organization. Therefore, it is important for service organization management to assess the risks arising from interactions with those parties, particularly when they operate controls necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

2.61 If service organization management determines the risks associated with third parties such as user entities, business partners, subservice organizations, vendors, and others with whom the service organization interacts are likely to be material to the service organization's achievement of its service commitments and system requirements (for example, because of the nature of those parties' access to the system or because of the controls they operate on behalf of the service organization), monitoring controls are necessary to enable management to determine whether the processes and controls performed by those users effectively address the identified risks. Such monitoring controls may include a combination of the following:

- Testing controls at the third party by members of the service organization's internal audit function
- Reviewing and reconciling output reports
- Holding periodic discussions with the third-party personnel and evaluating the third party's performance against established service-level objectives and agreements
- Making site visits to the third party
- Inspecting a type 2 SOC 2 report on the subservice organization's or business partner's system
- Monitoring external communications, such as complaints from user entities relevant to the services performed by the third party

2.62 When such monitoring activities do not exist or appear inadequate, it may be difficult for service organization management to demonstrate that it has a reasonable basis for its assertion.

2.63 Service organization management usually documents the assessment in a variety of ways, including through the use of policy manuals,

narratives, flowcharts, decision tables, procedural write-ups, or questionnaires. The nature and extent of documentation usually varies, depending on the size and complexity of the service organization and its monitoring activities.

2.64 If the service auditor believes that the subject matter is not appropriate because management does not have a reasonable basis for its assertion, or that sufficient appropriate evidence to support the basis is unlikely to be available, the service auditor should not accept or continue the engagement based on the guidance in paragraph .27 of AT-C section 105.

Assessing the Suitability and Availability of Criteria

2.65 As discussed in chapter 1, two distinct sets of criteria are used in the SOC 2 examination: description criteria and trust services criteria. The description criteria in DC section 200 and the trust services criteria in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*,[8] were promulgated by the Assurance Services Executive Committee, which is designated by the Council of the AICPA under the AICPA Code of Professional Conduct to issue measurement criteria. Therefore, such criteria are considered suitable for use in a SOC 2 examination. Because the criteria are published by the AICPA and made available to the public, they are also considered available to report users. Therefore, they meet the definition in paragraph .27*b*ii of AT-C section 105 for criteria that are both suitable and available for use in an attestation engagement.

Determining Whether the Service Organization's Principal Service Commitments and System Requirements Are Reasonable in the Circumstances

2.66 As stated in chapter 1, service organization management is responsible for identifying and achieving the service commitments it makes to user entities as well as for the requirements of the system that will enable the service organization to achieve them. Management is also responsible for designing, implementing, and operating controls that provide reasonable assurance of achieving the service organization's service commitments and system requirements.

2.67 *Principal* service commitments and system requirements are those that are likely to be useful to support the understanding of the services provided, the system, and the design and operation of controls by a broad range of SOC 2 report users. For example, it may be common for a service organization to make the same system availability commitment to the majority of its user entities. Because information about the availability commitments (for example, transaction response time, maximum hours of unscheduled outage per year) common to most user entities is likely to be useful to the broad range of SOC 2 report users, those commitments would be principal service commitments; as such, they would be presented in the description of the system.

2.68 In another situation, however, a service organization may make a different commitment about system availability to an individual user entity than to other user entities. That commitment would not ordinarily be considered a principal service commitment because it is likely to be relevant only to

[8] TSP sections can be found in AICPA *Trust Services Criteria*.

the individual user entity to which it was made and not to the broad range of SOC 2 report users. Because only principal service commitments are disclosed in the service organization's description, the individual user entity may need to obtain additional information from the service organization regarding the achievement of its specific availability commitment.

2.69 Because of the close relationship between the trust services criteria and the service organization's service commitments and system requirements, consideration of whether the principal service commitments and system requirements identified by management are appropriate for the SOC 2 examination is critical. Early evaluation can help the service auditor identify potential risks to the successful completion of the engagement and establish a more thorough understanding of the engagement scope and risks prior to engagement acceptance.

2.70 When considering whether the principal service commitments and system requirements established by management are reasonable in the circumstances, the service auditor may consider the following questions:

- Do the principal system requirements address the types of risks that would have a substantial likelihood of influencing the judgments made by intended users of the service organization's services? For example, to address cybersecurity risks to users of the service organization's system that are affected by logical access controls, management may identify a system requirement that indicates the service organization has implemented logical access controls to prevent or detect unauthorized access to the system.
- Are the principal service commitments and system requirements described in a level of detail that will enable report users to understand the evaluation of controls based on the trust services criteria? For example, disclosure of a principal service commitment to comply with privacy laws and regulations may not be sufficient. Instead, a disclosure that identifies the specific privacy laws and regulations, such as the European Union's General Data Protection Regulation (GDPR) may be necessary for users to understand the evaluation of controls, as illustrated in the next bullet.
- Do the principal service commitments and system requirements include compliance with legal requirements or contractual agreements? For example, if user entities are required by law to comply with the GDPR, these requirements are often included in the service-level agreements that they have with the service organization; the service organization would likely identify service commitments to support user entities' compliance with the GDPR. The service organization would also identify the system requirements necessary to enable that compliance. When those commitments are important to a broad range of users, management would generally identify them as principal service commitments and system requirements.

  If the service organization is required to comply with the GDPR, management would also generally identify a related service commitment and establish system requirements to support the achievement of that commitment. This is true whether or not the privacy criteria are included within the scope of the examination. When those commitments are important to a broad range of users,

management would generally identify them as principal service commitments and system requirements.

- Are the principal service commitments and system requirements complete? For example, in a SOC 2 examination that includes processing integrity, the service auditor would expect principal service commitments and system requirements to be identified related to completeness, validity, accuracy, timeliness, and authorization. An examination based on a complete set of principal service commitments and system requirements can provide intended users with the information they need to assess the effect of the service organization's controls on the risks associated with doing business with the service organization. However, the service auditor ordinarily will not be able to determine how the service organization's controls specifically address the risks specific to an individual intended user; accordingly, the service auditor need not consider completeness from the perspective of individual intended users. Instead, individual intended users are expected to assess whether the principal service commitments and system requirements disclosed in the description include those that are relevant to them.

2.71 If the service auditor believes that the service commitments and system requirements identified by management are not appropriate for the SOC 2 examination, the service auditor should discuss the appropriateness of the subject matter with management in accordance with paragraph .28 of AT-C section 105. It is usually helpful if management provides the service auditor with a draft of its principal service commitments and system requirements during the engagement acceptance process. If, as a result of the service auditor's initial review, the service auditor believes that this disclosure is inadequate and could result in the service auditor concluding that the description would be materially misstated, the service auditor may request that management revise the disclosure. If management is unwilling to revise the disclosure of the principal service commitments and system requirements, the service auditor may refuse to accept the engagement. Chapter 3 discusses considering the disclosures that service organization management makes about its principal service commitments and system requirements as part of the evaluation of whether the description presents the system that was designed and implemented in accordance with the description criteria. It also discusses the situation when, after accepting the engagement, the service auditor obtains evidence that causes him or her to believe that the service organization's service commitments and system requirements are not appropriate for the examination.

Requesting a Written Assertion and Representations From Service Organization Management[9]

2.72 According to paragraph .10 of AT-C section 205, the service auditor should request a written assertion from the responsible party that addresses

[9] As discussed in paragraph 2.43, if the service organization uses a subservice organization and elects the inclusive method, subservice organization management is also a responsible party and the guidance in this section also applies to them. If subservice organization management refuses to provide a written assertion, service organization management cannot use the inclusive method but may be able to use the carve-out method.

whether (*a*) the description presents the system designed and implemented in accordance with the description criteria, (*b*) the controls were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved, and (*c*) in a type 2 examination, the controls operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. The service auditor's responsibility for determining whether management has a reasonable basis for its assertion is discussed in paragraph 2.58.

2.73 Management's assertion is included in the SOC 2 report along with the description and the service auditor's report. Because of the important role that the assertion plays in the engagement, it may be useful for the service auditor to provide management with an example of a written assertion prior to engagement acceptance. However, service organization management is responsible for drafting its written assertion and may word the assertion in accordance with its practices, as long as it addresses management's conclusions about the description and effectiveness of controls and is not materially inconsistent with the description or the service auditor's report. Illustrative examples of management assertions are presented in appendix C-1, "Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination (Carved-Out Controls of a Subservice Organization and Complementary Subservice Organization Controls and Complementary User Entity Controls)," appendix C-2, "Illustrative Service Organization and Subservice Organization Management Assertions and Service Auditor's Report for a Type 2 Examination (Subservice Organization Presented Using the Inclusive Method and Complementary User Entity Controls)," and appendix C-3, "Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation."

2.74 If service organization management (responsible party) refuses to provide a written assertion, paragraph .84 of AT-C section 205 states the service auditor should withdraw from the engagement when withdrawal is possible under applicable laws and regulations.[10] Consequently, it is important to obtain management's agreement to provide the written assertion prior to engagement acceptance. If law or regulation does not allow the service auditor to withdraw, the service auditor should disclaim an opinion on the description, the suitability of design of controls, and in a type 2 examination, operating effectiveness of controls.

2.75 Service organization management is also required to provide the service auditor with written representations at the conclusion of the engagement. It may be useful for the service auditor to provide management with an example of the types of expected representations prior to engagement acceptance. Illustrative management representation letters are available on the AICPA website.

Agreeing on the Terms of the Engagement

2.76 Paragraph .07 of AT-C section 205 states that the service auditor should agree on, and document in a written communication such as an

[10] A SOC 2 examination, as described in this guide, is based on service organization management providing a written assertion to accompany the service auditor's report. Paragraph .86 of AT-C section 205, *Assertion-Based Examination Engagements*, permits a practitioner to report on a subject matter when the responsible party is not the engaging party and the responsible party refuses to provide a written assertion, as long as the report discloses management's refusal and restricts use to the engaging party. However, this approach is unlikely to be appropriate in most SOC 2 engagements.

engagement letter, the terms of the engagement with the engaging party. A written agreement, such as an engagement letter, reduces the risk that either the service auditor or service organization management may misinterpret the needs or expectations of the other party. For example, it reduces the risk that management may rely on the service auditor to protect the service organization against certain risks or to perform certain management functions. The service auditor would ordinarily request a signed engagement letter from the engaging party. The engaging party's refusal to provide the service auditor with an engagement letter may cause the service auditor to question whether a mutual understanding regarding the terms of the engagement has been reached and, in turn, may affect the service auditor's decision about whether to accept or continue the engagement.

2.77 Paragraph .08 of AT-C section 205 states that the agreed-upon terms of the engagement should include the following:

a. The objective and scope of the engagement

b. The responsibilities of the service auditor

c. A statement that the engagement will be conducted in accordance with attestation standards established by the AICPA

d. The responsibilities of the responsible party and the responsibilities of the engaging party, if different

e. A statement about the inherent limitations of an examination engagement

f. Identification of the criteria for the measurement, evaluation, or disclosure of the subject matter

g. An acknowledgment that the engaging party agrees to provide the service auditor with a representation letter at the conclusion of the engagement

2.78 Paragraph .42 of AT-C section 205 indicates that, if the service auditor plans to use internal auditors to provide direct assistance, prior to doing so, the service auditor should obtain written acknowledgment from the responsible party (management of the service organization) that internal auditors providing direct assistance to the service auditor will be allowed to follow the service auditor's instructions and that the responsible party will not intervene in the work the internal auditors perform for the service auditor. When the engaging party is the responsible party, the service auditor may wish to include this matter in the engagement letter.

2.79 In addition to these matters, the service auditor may decide to include other matters in the understanding, such as the identification of the service organization's service commitments and system requirements.

Accepting a Change in the Terms of the Examination

2.80 After the engagement agreement is executed but prior to the completion of the engagement, management may communicate a desire to change the scope of the engagement (for example, a change from the inclusive method to the carve-out method for subservice organizations or a change in the trust services category or categories, services, boundaries of the service organization's system, or components of the system covered by the examination). A change in the services covered by the examination might occur, for example, because the service organization has discontinued providing a particular part of its service.

When management requests a change in the scope of the engagement, paragraph .31 of AT-C section 105 states that the service auditor should not agree to the change in the terms of the engagement unless there is reasonable justification for the change. Examples of situations in which there may be reasonable justification for a change include the following:

- Misunderstanding concerning the nature of the examination originally requested
- Change in the informational needs of report users
- Identification of additional system components or expansion of the boundaries of the system to be included in the description to enhance the presentation of the description
- Determination that certain system components are not relevant to the services provided
- Determination that certain services are not relevant to report users
- The inability to provide the service auditor with access to a subservice organization after the subservice organization initially agreed to provide access
- A change from the inclusive method to the carve-out method when subservice organization management refuses to provide a written assertion after initially agreeing to do so

2.81 Changes to the scope of the engagement may not be considered reasonable, however, if they relate to information that is incorrect, incomplete, or otherwise unsatisfactory. For example, a request to change the period covered by the examination or to exclude from the scope of the examination portions of the system that are necessary to provide the services are likely to be unreasonable, particularly if the change is requested to avoid a qualified opinion from the service auditor. A request to change the scope of the examination to prevent the disclosure of deviations identified at a subservice organization by changing from the inclusive method to the carve-out method would also be unreasonable.

2.82 If, after using professional judgment, the service auditor believes there is reasonable justification to change the terms of the engagement from those originally agreed on, the service auditor may continue with the engagement and issue an appropriate report on the service organization's system. Paragraph .32 of AT-C section 105 states that the report should not include a reference to (*a*) the original engagement, (*b*) any procedures that may have been performed, or (*c*) scope limitations that resulted in the changed engagement. The service auditor may also decide to document the change in the engagement in an addendum to the engagement letter to evidence agreement to the change among the parties.

2.83 However, if the service auditor and the engaging party are unable to agree to a change of the terms of the SOC 2 examination, the service auditor and management may agree to continue the engagement in accordance with the original terms or mutually agree to terminate the engagement. If management does not accept either of these alternatives, the service auditor may consider whether to (*a*) disclaim an opinion on the description, suitability of design of controls, and in a type 2 examination, operating effectiveness of controls or (*b*) withdraw from the engagement.

Additional Considerations for a Request to Extend or Modify the Period Covered by the Examination

2.84 A service auditor may encounter situations in which service organization management requests that the period covered by an existing type 2 report be extended or modified. For example, the service auditor has previously reported on the period January 1, 20X1, to June 30, 20X1, (the original period) and management requests that the period be extended by three months to cover the period January 1, 20X1, to September 30, 20X1, (the extended period). In this case, the service auditor would have tested the first six months of the extended period but would not yet have tested the last three months of the extended period. In other cases, the service auditor may be requested to modify the original period (modified period). For example, the service auditor might be asked to add one or more additional months to or delete one or more months from the original period covered by the examination. Based on the requirements in paragraph .31 of AT-C section 105, the service auditor should determine whether there is reasonable justification for the request. The following paragraphs provide guidance to a service auditor who has decided that there is reasonable justification for management's request.

2.85 When there have been no significant changes to the processes, procedures, or controls of the service organization, the description of the service organization's system for the revised period may be unchanged or have only limited changes from the description for the original period. If the description of the service organization's system for the extended or modified period is the same as that of the original period, any procedures performed by the service auditor to obtain evidence about the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls are likely to be appropriate evidence for the service auditor's opinion addressing the extended or modified period; however, the service auditor should use professional judgment to determine the additional evidence needed.

2.86 As an example, assume the service auditor has been asked to extend the original period of January 1, 20X1, to June 30, 20X1, to cover through September 30, 20X1. The service auditor performed tests of the operating effectiveness of controls for a sample of 13 items during the original period. In this case, the tests of operating effectiveness performed on the sample of 13 items also provide evidence of the operating effectiveness of controls during the modified period. However, the service auditor uses professional judgment to determine the additional evidence of the operation of the controls for the period July 1 through September 30 necessary to support the service auditor's opinion on the operating effectiveness of controls during the modified period.

2.87 Based on the requirements in paragraph .47 of AT-C section 205, the service auditor service auditor should consider the additional evidence obtained for the extended or modified period when forming an opinion about the description, suitability of the design of controls, or in a type 2 examination, operating effectiveness of controls for the extended or modified period.

2.88 Paragraph .31 of AT-C section 105 states that if a change in the terms of the engagement is made, the service auditor should not disregard evidence that was obtained prior to the change. Therefore, when forming the opinion, the service auditor should consider conclusions reached during the original period in addition to the results of tests performed and other evidence obtained related to the extended or modified period. In making a determination about

the nature and extent of the additional evidence needed for the extended or modified period, the service auditor may consider the following:

- The overall control environment
- The significance of the assessed risks
- The specific controls that were tested during the portion of the original report period included in the extended or modified period and the nature and extent of the evidence obtained for that period
- The nature, timing, and extent of procedures performed for the portion of the original period included in the extended or modified period
- The length of the extended or modified period

2.89 When there is a change in the period covered by the examination, the service auditor's understanding of any significant changes to the service organization's system that occurred during the extended or modified period, including significant changes to the services provided to user entities and significant changes to any of the components of the system used to provide such services, affect the service auditor's judgment on whether an engagement for an extended or modified period is appropriate (see paragraph 2.84) and, if it is appropriate, the additional evidence that is necessary. Paragraphs 3.78 and 3.134, respectively, discuss the service auditor's responsibilities for obtaining an understanding of and performing procedures that address significant changes in the service organization's system.

2.90 If there have been significant changes in the service organization's system, it may not be appropriate for the service auditor to perform an engagement for an extended or modified period. For example, if a service organization converted from one application processing system to another during the new period and made significant modifications to the controls and those changes did not occur during the original period, the service auditor may decide that communicating information about changes in controls may present challenges for the broad range of report users of the SOC 2 report. Therefore, the service auditor may decide that an engagement covering an extended or modified period would not be appropriate in this situation.

Management's Written Representations for the Extended or Modified Period

2.91 Obtaining management's written representations is discussed beginning in paragraph 3.228. Based on the requirements in paragraph .55 of AT-C section 205, when the examination covers an extended period, and the service auditor has requested written representations from management, the representation letter should be dated as of the same date as the service auditor's report that covers the entire extended or modified period (that is, the new period).

Deficiencies That Occur During the Original, Extended, or Modified Period

2.92 The service auditor assesses any deficiencies identified in the original period and corrected during the extended or modified period to determine their overall effect on, and the need for additional disclosures in, the service auditor's report. Similarly, based on the requirements in paragraph .47 of AT-C section 205, deficiencies noted in the extended or modified period should also

be evaluated to determine their effect on the service auditor's report. Chapter 3 discusses evaluation of deficiencies.

2.93 Any material deficiencies identified in the portion of the original period that is included in the extended or modified period would be included in the report on the extended or modified period, even if they were corrected during the extended or modified period. The service auditor needs to consider the status of any deviations, deficiencies, or other matters noted in the portion of the original period that is also included in the extended or modified period, plus any exceptions, deficiencies, or other matters noted during the new period. For example, assume the original report covered the period January 1, 20X1, to June 30, 20X1, and included a deficiency in operating effectiveness. Also assume that the deficiency was corrected on August 15, 20X1. For a report covering an examination period of January 1 through September 30, the deficiency in operating effectiveness would be reported for the period from January 1 through August 15, 20X1. No reference to the original report would be made in the extended or modified report.

2.94 For deficiencies identified during the original period that have not been remediated, the service auditor would generally evaluate the reasons that the deficiencies have not been remediated and should consider the effect on the examination, based on the requirements in paragraph .47 of AT-C section 205.

2.95 The service auditor may use evidence obtained for the original period that is included in the extended or modified period. Assume that the original period covered by the report is January 1, 20X1, to August 31, 20X1, and the modified period is April 1, 20X1, to December 31, 20X1. Five months of the modified period were tested, and four months were untested. In the original period, 25 items were tested, of which 12 related to the 5 months that were included in the modified period. There was 1 test exception noted for those 12 items. For the period from August 31, 20X1, to December 31, 20X1, 13 items were tested and 1 exception was identified. The results of tests reported would identify the total number of exceptions identified based on the total number of tests performed (for example, "Two exceptions were identified in a sample of 25 items selected for testing"). The service auditor's conclusion on the achievement of the applicable service commitment or system requirement would be based on a deviation rate of 2 of 25.

Establishing an Overall Examination Strategy for and Planning the Examination

2.96 When planning the SOC 2 examination, the engagement partner and other key members of the engagement team develop an overall strategy for the scope, timing, and conduct of the engagement and an engagement plan, consisting of a detailed approach for the nature, timing, and extent of procedures to be performed. Adequate planning helps the service auditor devote appropriate attention to important areas of the engagement, identify potential problems on a timely basis, and properly organize and manage the engagement to make sure it is performed in an effective and efficient manner. Adequate planning also assists the service auditor in properly assigning work to engagement team members and facilitates the direction, supervision, and review of their work. Furthermore, if the work of internal auditors, other service auditors, or service auditor's specialists is used in the engagement, proper planning helps the service auditor coordinate their work.

2.97 According to paragraph .11 of AT-C section 205, the service auditor should establish an overall engagement strategy that sets the scope, timing, and direction of the engagement and guides in the development of the engagement plan. In establishing the overall engagement strategy, the service auditor ordinarily would do the following:

a. Obtain an understanding of the services provided by the service organization, the system used to provide them, and the service organization's service commitments and system requirements that define the engagement.

b. Ascertain the expected timing and nature of required communications.

c. Consider the factors that, in the service auditor's professional judgment, are significant in directing the engagement team's efforts.

d. Consider the results of preliminary engagement activities, such as client acceptance and, when applicable, whether knowledge gained on other engagements for the service organization is relevant.

e. Plan the engagement process, including possible sources of evidence and choices among alternative measurement or evaluation methods.

f. Obtain an understanding of the influences and pressures on service organization management and other appropriate parties within the entity.

g. Consider the common informational needs of the broad range of intended users of the SOC 2 report.

h. Consider the risk of fraud relevant to the engagement.

i. Ascertain the nature, timing, and extent of resources necessary to perform the engagement, including the use of other service auditor's or service auditor's specialists.

j. Assess the effect on the engagement of using the work of an internal audit function or obtaining direct assistance from internal audit function personnel.

k. Consider whether service organization management intends to disclose information about how the service organization's controls meet the requirements of one or more process or control frameworks as discussed in chapter 1 and, if so, the nature of such disclosures.

2.98 The nature and extent of planning activities will vary depending on the following factors:

- The service auditor's previous experience with the service organization, including whether security events were identified in prior periods
- The circumstances of the particular examination

2.99 Paragraph .13 of AT-C section 205 includes more detailed requirements related to developing the engagement plan.

2.100 Planning is a cumulative and iterative process that occurs throughout the engagement. Accordingly, the service auditor may need to revise the overall strategy and engagement plan based on unexpected events, changes

in conditions, or evidence obtained that contradicts information previously considered.

Planning Considerations When the Inclusive Method Is Used to Present the Services of a Subservice Organization

2.101 The inclusive method is frequently difficult to implement and may not be feasible in certain circumstances. The approach entails extensive planning and communication between the service auditor, the service organization, and the subservice organization. Use of 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 report users, service organization management may use the inclusive method for one or more subservice organizations and the carve-out method for other subservice organizations. In these instances, the 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 service organization management has selected, whether that approach is the inclusive or the carve-out method.

2.102 Because of the additional complexities involved with the use of the inclusive method, both the service organization and the subservice organization ought to agree on the use of the inclusive approach before it is selected for the examination. In addition, to facilitate the process, service organization management generally coordinates the use of the inclusive method with the subservice organization. If the inclusive method is used, matters to be agreed on 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 subservice organization management that it will provide the service auditor with a written assertion and representation letter (Both service organization management and subservice organization management are responsible for providing the service auditor with a written assertion and representation letter.)
- The planned content and format of the inclusive description
- The representatives of the subservice organization and the service organization and who will be responsible for
  - — providing each entity's description and
  - — integrating the descriptions
- For a type 2 examination, the timing of the tests of operating effectiveness of controls

2.103 To avoid issues with the engagement, during planning, the service auditor would generally determine whether subservice organization management is willing to provide a written assertion and representation letter. In addition, in accordance with paragraph .27 of AT-C section 105, the service auditor should determine whether it will be possible to obtain evidence that supports the portion of the opinion that addresses the subservice organization. If service organization management wishes to use the inclusive method, but subservice

organization management 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.

2.104 In addition to providing the service auditor with a written assertion and representation letter at the end of the examination, subservice organization management is also responsible for preparing a description of the subservice organization's system, including the completeness, accuracy, and method of presentation of the description. Service organization management is responsible for evaluating the description of the subservice organization's system, as well as its own.

2.105 As a responsible party, subservice organization management is also responsible for the following based on AT-C section 205:

- Implementing and operating specific controls identified by the service organization or, if the service organization has not identified specific controls, designing, implementing, and documenting controls that are suitably designed and operating effectively
- Having a reasonable basis for its assertion
- Providing the service auditor with written representations at the conclusion of the engagement
- If the service auditor plans to use internal auditors to provide direct assistance, providing the service auditor with written acknowledgment that internal auditors providing direct assistance to the service auditor will be allowed to follow the service auditor's instructions and that the subservice organization will not intervene in the work the internal auditors perform for the service auditor (paragraph 2.168)
- Providing the service auditor with the following:
  - Access to all information, such as records, documentation, service-level agreements, and internal audit or other reports, that subservice organization management is aware of and that is relevant to the engagement (paragraph .27*b*iii(1) of AT-C section 105)
  - Access to additional information that the service auditor may request from subservice organization management for the examination (paragraph .27*b*iii(2) of AT-C section 105)
  - Unrestricted access to personnel within the subservice organization from whom the service auditor determines it is necessary to obtain evidence relevant to the SOC 2 examination (paragraph .27*b*iii(3) of AT-C section 105)
- Disclosing to the service auditor the following:
  - Incidents of noncompliance with laws and regulations, fraud, or uncorrected misstatements that are clearly not trivial and that may affect one or more user entities, and whether such incidents have been communicated appropriately to affected user entities
  - Knowledge of any actual, suspected, or alleged fraud or noncompliance with laws and regulations affecting the

description of the service organization's system, the suitability of design of controls,[11] or in a type 2 examination, the operating effectiveness of controls (Paragraph 2.107 discusses a situation in which service organization management designs the controls at the subservice organization.)

- All deficiencies in the design of controls of which it is aware
- All instances in which controls have not operated as described
- All identified system incidents that resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements as of the date of the description (for a type 1 examination) or during the period of time covered by the description (for a type 2 examination)
- Any known events subsequent to the period covered by the description of the service organization's system, up to the date of the service auditor's report, that would have a material effect on the subject matter or subservice organization management's assertion (paragraph .51 of AT-C section 205)

2.106 Unless the subservice organization is also an engaging party (which is not the case in most SOC 2 examinations in which the inclusive method is used), subservice organization management is not responsible for any of the items in AT-C sections 105 or 205 that relate to an engaging party (for example, the requirement in paragraph .07 of AT-C section 205 for the service auditor to agree on the terms of the engagement with the engaging party.) A non-engaging-party subservice organization has no contractual relationship with the service auditor.

2.107 Subservice organization management's assertion ordinarily would be expected to address the same matters addressed by service organization management in its assertion, including (*a*) whether the description presents the services that the subservice organization provides to the service organization and to user entities, which are part of the service organization's system, in accordance with the description criteria; (*b*) the suitability of the design of the controls; and (*c*) in a type 2 examination, the operating effectiveness of controls. However, in some cases, service organization management might design the controls for the subservice organization. This may happen, for example, when the controls of the subservice organization are necessary, in combination with the controls of the service organization, to provide reasonable assurance that one or more of the service organization's service commitments or system requirements were achieved. When service organization management designs the controls for the subservice organization, service organization management takes responsibility for the suitability of the design of its own controls and the

[11] Subservice organization management's written assertion addresses the same matters addressed by service organization management's assertion. However, paragraph 2.107 discusses a situation in which service organization management designs the controls for the subservice organization. In this case, subservice organization management's assertion is limited to the matters discussed in that paragraph.

subservice organization's controls; therefore, the subservice organization's assertion may be limited to whether the description presents the services provided by the subservice organization to the service organization and user entities in accordance with the description criteria and whether the controls at the subservice organization operated as described.

Performing Risk Assessment Procedures

2.108 In accordance with paragraph .14 of AT-C section 205, the service auditor should obtain an understanding of the description, suitability of design of controls, and in a type 2 examination, operating effectiveness of controls and other engagement circumstances sufficient to

a. enable the service auditor to identify and assess the risks of material misstatement related to the description, suitability of design of controls, and in a type 2 examination, operating effectiveness of controls and

b. provide a basis for designing and performing procedures to respond to the assessed risks and to obtain reasonable assurance to support the service auditor's opinion.

2.109 In accordance with paragraph .14 of AT-C section 205, the service auditor should obtain an understanding of the service organization's system and related controls. Obtaining such an understanding provides the service auditor with a frame of reference for exercising professional judgment throughout the engagement. This assists the service auditor in, among other things, the following:

- Determining the appropriateness of the subject matter, which may include matters such as the system being examined, the boundaries of the system, and how the system interfaces with other service organization systems
- Assessing whether the description of the service organization's system presents the system that has been designed and implemented in accordance with the description criteria
- Understanding which controls are necessary to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria, whether the controls were suitably designed to achieve them, and in a type 2 report, whether controls were operating effectively throughout the period to achieve them

2.110 In accordance with paragraph .15 of AT-C section 205, the service auditor should also obtain an understanding of the service organization's internal control over the preparation of the description of the service organization's system in accordance with the description criteria. This includes understanding how service organization management identified the service organization's principal service commitments and system requirements as well as how management evaluated the design of controls relevant to the achievement of those service commitments and system requirements and how it determined whether such controls were implemented.

2.111 In addition to obtaining an understanding of the service organization's system, including its internal controls, as described earlier, in accordance with paragraph .16 of AT-C section 205, the service auditor should inquire of

service organization management[12] regarding whether it has used any specialists in the preparation of the description, or evaluation of the suitability of design or operating effectiveness of controls, and whether the service organization has an internal audit function. If the service organization has an internal audit function, that function may be a key component of internal control over the system being examined. Paragraph .16 of AT-C section 205 also notes that the service auditor should make further inquiries to obtain an understanding of the following:

a. The activities performed or to be performed by the internal audit function as it relates to the service organization

b. The main findings of the internal audit function as it relates to the description, suitability of design of controls, and in a type 2 examination, operating effectiveness of controls

2.112 The service auditor's responsibilities when a service organization has an internal audit department are discussed further beginning in paragraph 2.149.

Description of the System

2.113 The processes service organizations use to prepare the description may vary widely and are usually affected by the size and complexity of the service organization. Service organizations may have either informal or formal processes to prepare the description. A small service organization that prepares only one description per year, for example, is likely to have an informal process in which a few employees with personal knowledge of the system's operation are assigned responsibility for drafting the description before it is reviewed by senior management. A larger, more complex service organization with a variety of interrelated services through multiple systems that span many functional units is likely to have a more formal process. Such a process is likely to include a project manager who coordinates preparation of the description by functional area and a review of the description by key executives across the organization. The two different processes are likely to give rise to different types of misstatements.

2.114 If a service organization has an informal preparation process, the service auditor is unlikely to perform extensive procedures to obtain an understanding of that process; instead, the service auditor is likely to focus on procedures to obtain evidence about whether the description presents the system that was designed and implemented in accordance with the description criteria.

2.115 If a service organization has a more formal preparation process, understanding the service organization's preparation process and controls may assist the service auditor in

- identifying possible sources of material misstatement,
- determining the likelihood of such misstatements, and

[12] Inquiries regarding specialists and internal audit should be made of the responsible party. As noted in paragraph 2.43, If the service organization uses a subservice organization and the inclusive method is used, subservice organization is also a responsible party and inquiries should be made of them as well.

- designing procedures to evaluate the description, suitability of design of controls, and in a type 2 engagement, effectiveness of controls.

2.116 In any event, the service auditor needs to remember that the initial system description prepared by service organization management is ordinarily revised several times during the examination, as the service auditor's procedures provide further insight into the nature and extent of appropriate disclosures. Therefore, the initial draft of the system description often does not reflect what the final system description will look like. Nevertheless, when obtaining the understanding of the description and the process used to develop it, it may be helpful for the service auditor to consider certain factors that may affect the nature, timing, and extent of further procedures. When reading the initial draft of the description, the service auditor may compare it to certain expectations developed based on the understanding of the service organization's system. For example, if the service organization uses a subservice organization and the subservice organization's controls are necessary, alone or in combination with the entity's controls, for the service organization to achieve its service commitments and system requirements based on the applicable trust services criteria, the service auditor would expect the description to include the appropriate disclosures required by description criterion DC7. Conversely, if there have been no significant changes to the service organization's system and controls for the specified period, the service auditor would not expect to see disclosures required by description criterion DC9.

Design and Effectiveness of Controls

2.117 As discussed in paragraph 2.58, service organization management would usually be unable to make an assertion about the suitability of design and, in a type 2 engagement, operating effectiveness of controls without first having performed a risk assessment. The risk assessment enables management to identify and assess the risks that threaten the achievement of the service organization's service commitments and system requirements; such assessments are necessary for management to implement effective controls to mitigate those risks.

2.118 When there is extensive documentation of the service organization's risk assessment process, inspecting such documentation may assist the service auditor in identifying deficiencies in the design of controls. However, as discussed beginning at paragraph 2.108, the service auditor is responsible for performing an engagement risk assessment as part of a SOC 2 examination. Reviewing management's risk assessment process, while it may be useful, is not a substitute for the service auditor's own procedures. For that reason, a service auditor may decide to focus only on understanding the process that management uses to evaluate control effectiveness.

2.119 A service organization's monitoring activities, and the reports generated from those activities, enable service organization management to periodically or continuously monitor the effectiveness of controls.

2.120 Examples of monitoring activities that service organization management may perform include the following:

- Reviewing results of control evaluations performed by the internal audit function

- Periodic evaluation of control effectiveness through self-assessment programs
- A combination of the various assessment techniques

2.121 Service organization management generally documents the performance of monitoring activities, which permits the service auditor to inspect the documentation as part of obtaining an understanding of the effectiveness of controls within the system.

Procedures to Obtain the Understanding

2.122 The service auditor's procedures to obtain an understanding of the service organization's system may include the following, usually in some combination:

a. Making inquiries of service organization management, those charged with governance, and others within the service organization who, in the service auditor's judgment, may have relevant information

b. Observing operations and inspecting documents, reports including those prepared for user entities, and printed and electronic records of transaction processing

c. Inspecting a selection of agreements between the service organization and its user entities and business partners

d. Reperforming the application of a control

e. Reading relevant reports received from regulators

2.123 One or more of the preceding procedures may be accomplished through the performance of a walk-through, which is discussed further beginning at paragraph 3.51. In addition, the service auditor may perform such procedures concurrently with procedures to obtain evidence about whether the description is presented in accordance with the description criteria and whether the controls within the system were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

2.124 When the service organization uses one or more subservice organizations, the service auditor may also consider whether a SOC 2 report is available for those subservice organizations. When a separate SOC 2 report exists for a subservice organization, obtaining and reading the SOC 2 report helps the service auditor evaluate whether controls at the service organization are suitably designed. It also assists the service auditor in evaluating whether

- the CSOCs identified by service organization management are identified as controls in the subservice organization's SOC 2 report
- there are any CUECs identified in the subservice organization's SOC 2 report that are the responsibility of the service organization or user entities and that should be included in the controls identified by the service organization or CUECs to be addressed by user entities.

2.125 The service auditor may seek the assistance of a service auditor's specialist (for example, an IT specialist with experience with a system

component such as an unusual or proprietary operating system) when obtaining the understanding of the system and the related processes and controls. A service auditor's specialist may assist the service auditor by providing technical expertise that may be useful to the service auditor's understanding of the system.

Assessing the Risks of Material Misstatement

2.126 Once the service auditor has obtained an understanding of the service organization's system and the related processes and controls, the service auditor should assess the risks of material misstatement in accordance with paragraph .19 of AT-C section 205. Inherent and control risks reflect the likelihood that the subject matter is materially misstated. The service auditor cannot control those risks. The service auditor controls detection risk through the nature, timing, and extent of substantive procedures and further examination procedures. When considering the effectiveness of controls, however, the service auditor can only obtain sufficient appropriate evidence through the performance of tests of controls. Nevertheless, the service auditor's identification and assessment of the risks of material misstatement enable the service auditor to plan tests of controls that address controls that are necessary for the achievement of the service organization's service commitments and system requirements. In addition, based on the assessment, the service auditor can plan and perform a variety of different tests of controls to obtain reasonable assurance that controls were operating effectively in support of the opinion on the effectiveness of controls in a type 2 examination. Chapter 3 provides additional guidance on planning and performing tests of controls, including which tests may be more effective than others and which may provide more persuasive evidence about operating effectiveness of controls.

2.127 In a SOC 2 examination, attestation risk is the risk that the service auditor will issue an inappropriate opinion when any of the following occurs and is not detected by the service auditor's procedures:

a. The description of the service organization's system was not presented in accordance with the description criteria, in all material respects.

b. Because of deficiencies in the design of controls, the controls stated in the system description were not suitably designed throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved, in all material respects, based on the applicable trust services criteria.

c. In a type 2 examination, the controls stated in the system description did not operate effectively throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved, in all material respects, based on the applicable trust services criteria.

Defining Misstatements in This Guide

2.128 Based on the definition of *misstatement* in paragraph .12 of AT-C section 105, this guide uses the following terms when discussing misstatements related to the different subject matters in the SOC 2 examination:

- The term *description misstatement* is used when describing differences between (or omissions in) the description and the description criteria.
- The term *deficiency* is used to identify misstatements resulting from controls that were not suitably designed or did not operate effectively.
- The term *deviation* is used to identify the failure of a control to operate in a specific instance. A deviation may, individually or in combination with other deviations, result in a deficiency.

Identifying and Assessing Inherent Risks

2.129 The service auditor's risk assessment procedures begin with the identification and assessment of inherent risks that may affect the description of the system, suitability of design of controls, and in a type 2 examination, the operating effectiveness of controls. This guide uses *inherent risk* to refer to the susceptibility of the description, design of controls, and in a type 2 examination, operating effectiveness of controls to a material misstatement before consideration of any related controls. Inherent risks may include those arising from new or changed controls, system changes, significant changes in processing volume, new personnel or significant changes in key management or personnel, new types of transactions, new products or technologies, or modifications to the service auditor's opinion in the service auditor's report for the prior year. They may also include inherent risks arising from interactions with third parties. Table 2-1 lists additional factors that can result in inherent risks to the service organization.

Table 2-1

Factors That Might Result in Inherent Risks

System Characteristics	*Organizational and User Entity Characteristics*	*Physical, Environmental, and Technological Characteristics and Changes Therein*
• Nature and importance of key controls to the achievement of the service organization's service commitments and system requirements • Use of supporting information systems such as overall architecture, cloud computing, and other IT-hosted services	• The size and structure of the service organization (for example, centralized versus decentralized, insourced or outsourced) • Types of subservice organizations and other third parties that are significant to the services provided by the service organization	• Changes to business unit or supporting IT and related personnel • Changes to the risk assessment and controls that monitor processes resulting from the failure of controls designed to achieve service commitments and system requirements

Factors That Might Result in Inherent Risks — *continued*

System Characteristics	*Organizational and User Entity Characteristics*	*Physical, Environmental, and Technological Characteristics and Changes Therein*
• The types and number of employee personnel (finance, administrative, operations, IT, sales and marketing, and so on) and third parties (contractors, subservice organizations, business partners, and so on) with access to the service organization's system • Use of subservice organizations and other third parties on which the service organization depends to achieve its service commitments and system requirements • Types of physical and logical access of third parties to information systems, including whether access to a system not addressed in the SOC 2 examination could provide access to the system being examined • Types of information technology, applications, and infrastructure used, and their source (for example, whether software is internally developed or purchased without modification)	• Whether the service organization's information systems or subservice organizations are located in countries or regions deemed high risk by service organization management • The distribution of responsibilities related to the service organization's risk management program between business functions (for example, operating units, risk management, IT management, and legal) • Business units with information systems administered under a separate management structure (for example, outside of a centralized IT function) • Changes to the service organization's service model	• Significant changes to the service organization's IT architecture and applications and the processes and systems used by subservice organizations • Changes to legal and regulatory requirements that affect information systems

(*continued*)

Factors That Might Result in Inherent Risks — *continued*

System Characteristics	*Organizational and User Entity Characteristics*	*Physical, Environmental, and Technological Characteristics and Changes Therein*
• Nature of external-facing web applications and the nature of applications developed in-house • Dependency on strategically significant systems that are no longer made or supported or that would be difficult to repair or replace in the event of failure • Dependency on IT equipment and information systems critical to the services provided, including those based on emerging technologies		

2.130 In accordance with paragraph .33 of AT-C section 205, the service auditor should also consider whether risk assessment and other procedures related to understanding the description, suitability of design of controls, and in a type 2 examination, operating effectiveness of controls indicate there is a risk of material misstatement due to fraud or noncompliance with laws or regulations. For example, fraud risks related to a service organization might include management override of controls at the service organization, misuse of user entity or business partner information assets by service organization personnel, and creation, by service organization personnel, of false or misleading documents or records of transactions processed by the service organization.

2.131 Inherent risks may also include risks derived from user entities and subservice organizations that threaten the achievement of the service organization's service commitments and system requirements if not addressed by effective CUECs and CSOCs. CUECs are discussed further beginning at paragraph 2.23, and CSOCs are discussed beginning at paragraph 2.20.

Identifying and Assessing Control Risk

2.132 As used in this guide, *control risk* is the risk that a material misstatement will not be prevented, or detected and corrected, on a timely basis by

the service organization's controls. Considering the controls the service organization has designed and implemented to mitigate inherent risks at a high level enables the service auditor to focus further procedures on those controls that are necessary for the service organization to achieve its service commitments and system requirements.

Procedures to Assess the Risks of Material Misstatement

2.133 When assessing the risks of material misstatement, the service auditor may perform one or more of the following procedures:

- *Reviewing service organization management's risk assessment.* As discussed beginning at paragraph 2.58, service organization management must have a reasonable basis for its assertions about the description, suitability of design of controls, and in a type 2 examination, operating effectiveness of controls. An important element of the system and related controls involves the process that service organization management uses to identify and assess risks to the achievement of the service organization's service commitments and system requirements; as such, that process is part of the reasonable basis service organization management relies on to make its assertions.

    — Reviewing service organization management's risk assessment enables the service auditor to understand and compare the risks considered by management with those identified by the service auditor. In addition, the service auditor's independent review of service organization management's risk assessment, in combination with the service auditor's knowledge, assists with the identification of risks not previously considered.

- *Reviewing reports by internal audit, compliance teams, and quality teams.* Such reports may identify unique service organization risks and control deficiencies.
- *Reviewing reports by regulators.* Such reports may describe risks or deficiencies identified by regulators.
- *Reviewing user entity complaints or litigation,* which may indicate the service organization's failure to achieve one or more service commitments and system requirements.
- *Making inquiries of service organization management about fraud or noncompliance with laws or regulations* as discussed in paragraph 3.195.
- *Making inquiries of service organization management about evidence that contradicts assertions* about the suitability of design of controls or, in a type 2 examination, the operating effectiveness of controls. A major change to system procedures may have been made to address a material failure of controls to achieve a service commitment or system requirement. When a major change has been made, inquiry of management about why the change was made may not only reveal a prior control deficiency but may also assist the service auditor in understanding the nature of risks affecting the system.

2.134 Chapter 3 provides additional guidance on designing and performing further procedures that are responsive to the service auditor's assessed risk.

Considering Materiality During Planning

2.135 In accordance with paragraph .17 of AT-C section 205, the service auditor should consider materiality when establishing the overall engagement strategy. Because of the vast number of controls within a system, even at a small service organization, the service auditor needs to consider materiality during planning to determine the nature, timing, and extent of procedures necessary to obtain sufficient appropriate evidence to support the opinions in the SOC 2 examination. Adoption of an appropriate materiality also allows the service auditor to prioritize testing efforts and supports an effective and efficient engagement.

2.136 Paragraph .A19 of AT-C section 205 states that materiality in an attestation engagement is considered in the context of qualitative factors and, when applicable, quantitative factors. The relative importance of each of those factors when considering materiality in a particular engagement is a matter of professional judgment and is affected by the service auditor's perception of the common information needs of intended users, as identified beginning at paragraph 1.07. In this context, it is reasonable for the service auditor to assume that intended users possess a certain level of knowledge, as described in paragraph 1.08.

2.137 When considering materiality, the service auditor typically considers whether there is substantial likelihood that description misstatements or deficiencies in control design (and control effectiveness in a type 2 engagement) would influence judgments made by intended users based on the subject matter.

2.138 If the service auditor becomes aware, during the conduct of the examination, of information that would have caused the service auditor to have initially determined a different materiality, paragraph .18 of AT-C section 205 states that the service auditor should reconsider materiality. Chapter 3 of this guide discusses materiality considerations during the performance of the examination in further detail.

Description of the System

2.139 Because the description of the system is a narrative presentation, considering materiality during planning involves some unique considerations. Certain aspects of the description of the system may be quantitatively measured but others may not be. When considering aspects of the description that cannot be quantitatively measured, it may be necessary for the service auditor to consider other ways to identify and measure description misstatements. This necessitates consideration of the nature of potential misstatements during planning.

2.140 For instance, the service auditor may consider any of the following to be a description misstatement:

- Inclusion of misleading or inappropriate information (for example, information that obscures the information required by the description criteria such as excessive or irrelevant disclosures)

- Omission of information required by the description criteria (for example, inadequate or incomplete information)
- Changes to disclosures made in a previous period without reasonable justification
- Misstatements of fact

In accordance with paragraph .17 of AT-C section 205, once a misstatement is identified, the service auditor should evaluate whether the description misstatement is material to the description, as discussed further in chapter 3.

2.141 An initial draft of a narrative presentation that contains misstatements (such as omissions of certain disclosures that the service auditor expected or insufficient or inappropriate disclosures about matters required by the criteria) may prompt the service auditor to discuss the misstatements with service organization management. This discussion ordinarily would be held as early as possible to enable service organization management to revise the description. In addition, the misstatements in the draft may cause the service auditor to conclude that it will be necessary to obtain more persuasive evidence about one or more of the significant disclosures identified during planning to determine whether the final description will be prepared in accordance with the description criteria.

Effectiveness of Controls

2.142 When considering materiality during planning, a service auditor may consider following a process such as this:

a. Identifying the risks that threaten the achievement of the service organization's service commitments and system requirements

b. Assessing the likelihood and magnitude of those risks

c. Understanding the processes and controls the service organization has designed, implemented, and operated to mitigate those risks to an acceptable level based on the applicable trust services criteria

d. Designing tests of controls that focus on controls necessary to mitigate the risks that threaten the achievement of the service organization's service commitments and system requirements

e. Developing a materiality threshold for evaluating control deviations (Although there is no requirement in the attestation standards to develop a threshold below which deviations would be considered immaterial, doing so may assist a service auditor in the development of appropriate procedures and in the evaluation of the results of the procedures.)

2.143 For example, because a service organization updates software frequently, the service auditor may believe that (*a*) controls are unlikely to operate effectively if application software changes are not tested prior to implementation in the production environment and (*b*) the likelihood of the realization of that risk is high. Therefore, the service auditor may determine that the extent of evidence needed to support a conclusion that controls over software application changes are effective is greater than that needed to support a conclusion about the effectiveness of controls that are less significant to the achievement of the service organization's service commitments and system requirements (and the service auditor's opinion). In that case, when designing tests of controls over software application change controls, the service auditor would be likely to establish a low acceptable rate of error for such testing.

Considering Entity-Level Controls

2.144 The service organization designs, implements, and operates controls at the entity level that are necessary to support the achievement of its service commitments and system requirements. That is particularly true for controls that address the trust services criteria for the control environment component of internal control (CC1.1–1.5). Although entity-level controls can also address the achievement of service commitments and system requirements based on the trust services criteria for the information and communication (CC2.1–2.3), risk assessment (CC3.1–3.4), and monitoring (CC4.1–4.2) components of internal control, management often addresses those criteria by designing and implementing controls that operate at the system level. As an example, assume that the service organization performs an enterprise-wide risk assessment and also assesses its information security risk and its infrastructure risk at the system level. Because the latter two assessments are likely to be more relevant in the SOC 2 examination, the service auditor ordinarily devotes more time and attention to obtaining an understanding of those assessments than to the enterprise-wide risk assessment.

2.145 Nevertheless, effective entity-level controls, particularly those designed and implemented to meet the control environment criteria, may enable the service auditor to place greater confidence in the processes and controls the service organization has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved. Thus, effective entity-level controls may reduce the nature and extent of the procedures the service auditor believes are necessary to perform to obtain sufficient appropriate evidence about the operating effectiveness of the controls stated in the description to support the opinion. They may also affect decisions related to when such procedures are planned to be performed.

2.146 In contrast, deficiencies in entity-level controls often have a pervasive effect on other controls. If the service auditor determines that certain entity-level controls did not operate effectively, the service auditor may be able to adjust the nature, timing, and extent of procedures performed to obtain evidence about whether the controls stated in the description were effective. In some situations, however, deficiencies in the operation of entity-level controls may lead the service auditor to conclude that controls did not operate effectively. For example, consider a service organization that has been unable to retain knowledgeable employees. In that situation, the service auditor may decide to increase the extent of testing of controls that prevent and detect system incidents (for example, inspection of security configurations and event management scan logs) to obtain sufficient appropriate evidence about whether the controls stated in the description operated effectively.

2.147 The service auditor may find it necessary to understand the root cause of any identified deficiencies in entity-level controls to assess the impact they may have on the operating effectiveness of the related controls stated in the description. Ways in which a service auditor may respond to ineffective entity-level controls in a SOC 2 examination include the following:

- Selecting different types of procedures, or changing the timing of those procedures, to obtain evidence about the operating effectiveness of controls
- Obtaining more extensive evidence about the operating effectiveness of controls

2.148 Because of the important effect entity-level controls may have on the operating effectiveness of controls stated in the description, the description of the system often includes disclosures about the entity-level controls designed, implemented, and operated to address the risks that would threaten the service organization's achievement of its service commitments and system requirements. A sample description, illustrating such disclosures, is available on the AICPA website. It also illustrates, in section 4 of the description, the tests the service auditor may perform to determine whether the entity-level controls applicable to the trust services criteria relevant to the control environment operated effectively throughout the period.

Understanding the Internal Audit Function

2.149 An internal audit function performs assurance and consulting activities designed to evaluate and improve the effectiveness of the service organization's governance, risk management, and internal control processes. Activities similar to those performed by an internal audit function may be conducted by functions with other titles within a service organization. Some or all of the activities of an internal audit function may also be outsourced to a third-party service provider. For example, a service organization may engage a service provider to perform (*a*) penetration testing, (*b*) responsibilities of the internal audit function that the function itself does not have the competency or qualifications to perform (for example, performing the IT internal audit function), or (*c*) a one-time special assessment at the request of the board of directors. Neither the title of the function nor whether it is performed by the service organization or a third-party service provider is a sole determinant of whether the service auditor can use the work of internal auditors. Rather, it is the nature of the activities, the extent to which the internal audit function's organizational status and relevant policies and procedures support the objectivity of the internal auditors, the competence of internal auditors, and the systematic and disciplined approach of the function that are relevant. References in this guide to the work of the internal audit function include relevant activities of other functions or third-party providers that have these characteristics.

2.150 If the service organization has an internal audit function, that function may be important to the service organization's internal control over the system being examined. Activities of the internal audit function that may be relevant to the SOC 2 examination include those that provide information or evidence about whether the description is presented in accordance with the description criteria or whether controls were suitably designed and, in a type 2 examination, operating effectively.

2.151 If the internal audit function does not perform activities related to the SOC 2 examination, or if the service organization does not have a function that performs similar activities, the service auditor would ordinarily determine whether other monitoring activities provide sufficient appropriate evidence about the effective operation of controls.

2.152 Based on the requirements in paragraph .27 of AT-C section 205, when obtaining an understanding of the internal audit function's responsibilities and activities, the service auditor should make inquiries of internal audit personnel and read information about the internal audit function stated in the description. Ordinarily, the service auditor also requests and reads any relevant internal audit reports related to the period covered by the examination.

For example, reading the internal audit plan and reports issued by the internal audit function enables the service auditor to understand the nature of the internal audit function's responsibilities and how the internal audit function fits into the service organization's structure. Additionally, any findings in internal audit reports that relate to the presentation of the description or the suitability of design of controls or, in a type 2 examination, the operating effectiveness of controls may affect the risk assessment and the determination of the nature, timing, and extent of the service auditor's planned procedures.

Planning to Use the Work of Internal Auditors

2.153 If, after obtaining an understanding of the internal audit function, the service auditor concludes that (*a*) the activities of the internal audit function are not relevant to the SOC 2 examination or (*b*) it may not be efficient to consider the work of the internal audit function, the service auditor does not need to consider the work of the internal audit function.

2.154 The service auditor may determine, however, that the examination can be performed more effectively or efficiently by using the work of the internal audit function or obtaining direct assistance from internal audit function personnel. The phrase "using the work of the internal audit function" usually refers to using work designed and performed by the internal audit function, in accordance with an internal audit plan, to obtain evidence to support the achievement of the service organization's service commitments and system requirements. This differs from work the internal audit function performs to provide direct assistance to the service auditor, including assistance in performing tests of controls that are designed by the service auditor and performed by members of the internal audit function under the service auditor's direction, supervision, and review. When members of the internal audit function provide direct assistance, the procedures they perform are similar to work performed by the engagement team.[13]

Evaluating the Competence, Objectivity, and Systematic Approach Used by Internal Auditors

2.155 In accordance with paragraph .40 of AT-C section 205, if the service auditor determines that the work of the internal audit function is relevant to the SOC 2 examination, and the service auditor intends to use the work of the internal audit function in obtaining evidence, or plans to use internal auditors to provide direct assistance during the examination, the service auditor should determine whether the work can be used for purposes of the examination by evaluating several factors. The factors the service auditor should evaluate include the following:

a. The level of competence of the internal audit function or the individual internal auditors providing direct assistance

b. The extent to which the internal audit function's organizational status and relevant policies and procedures support the objectivity of the internal audit function as a whole or, for internal auditors providing direct assistance, the existence of threats to the objectivity

[13] Regardless of whether the service auditor plans to use internal audit's work or to use the internal audit function in a direct assistance capacity, the term *engagement team*, as used throughout this guide, does not include individuals within the service organization's internal audit function.

of those internal auditors and the related safeguards applied to reduce or eliminate those threats

c. The application by the internal audit function of a systematic and disciplined approach, including quality control

2.156 When evaluating competence, the service auditor would generally consider the attainment and maintenance of knowledge and skills of the internal audit function at the level required to enable assigned tasks to be performed diligently and with the appropriate level of quality, particularly as it relates to the work of the internal audit function that is to be used or, when using individuals for direct assistance, the individual. Consideration of factors such as the following may assist the service auditor with that evaluation:

a. Hiring policies

b. The adequacy of resources relative to the size of the entity

c. Technical training and proficiency of individuals

d. Knowledge of the areas being examined, including industry-specific or technical knowledge required to perform the work

e. Whether internal auditors are members of relevant professional bodies or have certifications that oblige them to comply with the relevant professional standards, including continuing professional education requirements

2.157 When evaluating objectivity, the service auditor would generally consider whether the internal audit function as a whole or, when using individuals for direct assistance, the individual performs tasks without allowing bias, conflict of interest, or undue influence of others to override professional judgments. Factors that may affect the service auditor's evaluation of objectivity include the following:

a. Whether the organizational status of the internal audit function, including the function's authority and accountability, supports the ability of the function to be free from bias, conflict of interest, or undue influence of others (for example, whether the internal audit function reports to those charged with governance or to an officer with appropriate authority, or if the function reports to management, whether it has direct access to those charged with governance)[14]

b. Whether the internal audit function is free of any conflicting responsibilities (for example, having managerial or operational duties or responsibilities that are outside of the internal audit function)

c. Whether those charged with governance oversee employment decisions related to the internal audit function (for example, whether they determine the appropriate remuneration in accordance with policy)

---

[14] As indicated in paragraph .A18 of AT-C section 105, *Concepts Common to All Attestation Engagements*, management and governance structures vary by organization, reflecting influences such as size and ownership characteristics. Because of the diversity that exists among organizations, the attestation standards do not specify the persons or groups at each organization with specified responsibilities. Identifying the appropriate service organization management personnel or those charged with governance to whom the internal audit function should report may require the exercise of professional judgment.

2.158 When evaluating the application by the internal audit function of a systematic and disciplined approach, including quality control, the service auditor may consider the function's approach to planning, performing, supervising, reviewing, and documenting its activities. Relevant factors to consider may include, among others, (*a*) the existence, adequacy, and use of documented internal audit procedures or guidance covering such areas as risk assessments, work programs, documentation, and reporting or (*b*) whether the internal audit function has appropriate quality control policies and procedures.

2.159 The objectivity and competence of internal auditors are important considerations when determining whether to use their work and, if so, the nature and extent to which their work may be used. However, as noted in paragraph .A50 of AT-C section 205, a high degree of objectivity cannot compensate for a low degree of competence, nor can a high degree of competence compensate for a low degree of objectivity. Additionally, when the service auditor is considering whether to use the work of the internal audit function, neither a high level of competence nor strong support for the objectivity of the internal auditors compensates for the lack of a systematic and disciplined approach by the internal audit function.

2.160 Based on an evaluation of the preceding factors, it is up to the service auditor to determine whether the risks to the quality of the work of the internal audit function or the individual, when using direct assistance, are too significant and whether it is appropriate to use any of the work of the function or individual as examination evidence.

Determining the Extent to Which to Use the Work of Internal Auditors

2.161 The extent to which the service auditor plans to use the work of the internal audit function is a matter of professional judgment. In accordance with paragraph .40 of AT-C section 205, because the service auditor has sole responsibility for expressing an opinion on the description, the suitability of design of controls, and in a type 2 examination, the operating effectiveness of controls, the service auditor should make all significant judgments in the examination, including when to use the work of the internal audit function in obtaining evidence.

2.162 To prevent undue use of the internal audit function in obtaining evidence, paragraph .40 of AT-C section 205 also notes that the service auditor should use less of the work of the internal audit function and perform more of the work directly when more judgment is involved in planning and performing relevant procedures or in evaluating the evidence obtained. As indicated in paragraph .44 of AT-C section 205, the service auditor should plan to use less of the work of the function and perform more of the work directly,

a. the more judgment is involved in
    i. planning and performing relevant procedures or
    ii. evaluating the evidence obtained.
b. the higher the assessed risk of material misstatement.
c. the less the internal audit function's organizational status and relevant policies and procedures adequately support the objectivity of the internal auditors.
d. the lower the level of competence of the internal audit function.

2.163 Relevant factors in determining whether to use the work of the internal audit function to obtain evidence about the operating effectiveness of controls include the pervasiveness of the control, the potential for management override of the control, and the degree of judgment and subjectivity required to evaluate the effectiveness of the control. As the significance of these factors increases, so does the need for the service auditor, rather than the internal audit function, to perform the procedures, and conversely, as these factors decrease in significance, the need for the service auditor to perform the tests decreases.

Coordinating Procedures With the Internal Auditors

2.164 When the service auditor plans to use the work of the internal audit function, the service auditor may find it helpful to review the internal audit function's audit plan and discuss the planned use of the work of the internal audit function with service organization management. The audit plan provides information about the nature, timing, extent, and scope of the work performed by the internal audit function, as well as the work that is planned to be performed.

2.165 As part of this discussion and as a basis for coordinating the respective activities between the service auditor and the internal auditors when planning to use the work of the internal audit function, it may be useful to address the following:

- The nature of the work performed
- The timing of such work
- The extent of coverage
- Proposed methods of item selection and sample sizes
- Documentation of the work performed
- Review and reporting procedures

2.166 Coordination between the service auditor and the internal audit function is effective when discussions take place at appropriate intervals throughout the period to which management's assertion pertains. It is important that the service auditor inform the internal audit function of significant matters as they arise during the engagement. Equally important is that the service auditor has access to relevant reports of the internal audit function and is advised of any significant matters that come to the attention of the internal auditors, when such matters may affect the scope of the examination and the potential nature, timing, or extent of the examination procedures. Communication throughout the engagement provides opportunities for internal auditors to bring up matters that may affect the service auditor's work. The service auditor is then able to take such information into account (for example, when assessing the risks that the description does not present the system that was designed and implemented in accordance with the description criteria or that controls were not suitably designed or, in a type 2 examination, not operating effectively).

2.167 Although the service auditor is not precluded from using work that the internal audit function has already performed, coordination of activities between the service auditor and the internal audit function is likely to be most effective when appropriate interaction occurs before the internal audit function performs the work.

2.168 In accordance with paragraph .42 of AT-C section 205, when planning to use internal auditors to provide direct assistance, the service auditor should obtain written acknowledgment from service organization management, as the responsible party, that internal auditors providing direct assistance will be allowed to follow the service auditor's instructions without management's interference.

Evaluating Whether the Work of Internal Auditors Is Adequate for the Service Auditor's Purposes

2.169 When using the work of the internal audit function, paragraph .41 of AT-C section 205 indicates that the service auditor should perform sufficient procedures, including reperformance, on the body of work of the internal audit function that the service auditor plans to use to evaluate whether such work is adequate for the service auditor's purposes. Chapter 3 provides guidance on the service auditor's considerations when performing procedures on that work.

Planning to Use the Work of an Other Practitioner

2.170 In certain situations, the service auditor might plan to use the work of an other practitioner. For example, if the service organization operates divisions or business units in other geographic locations, the service auditor might plan to use the work of a practitioner located in the other geographic region to obtain sufficient appropriate evidence to enable the service auditor to express an opinion on the description, suitability of design of controls and, in a type 2 examination, operating effectiveness of controls.

2.171 Paragraph .33 of AT-C section 105 indicates that when the service auditor expects to use the work of an other practitioner, the service auditor has the following reporting options:

a. Assume responsibility for the work of the other practitioner

b. Make reference to the other practitioner in the service auditor's report

2.172 If the service auditor expects to use the work of the other practitioner, paragraph .33 of AT-C section 105 states that the service auditor should do the following:

a. Obtain an understanding of whether the other practitioner understands, and will comply with, the ethical requirements that are relevant to the engagement and, in particular, is independent. (The discussion beginning in paragraph 2.41 also applies to the other practitioner.)

b. Obtain an understanding of the other practitioner's professional competence. (The service auditor may make inquiries about the other practitioner to the other practitioner's professional organization or to other practitioners, inquire about whether the other practitioner is subject to regulatory oversight, and read any publicly available regulatory reports, including reviews or inspections of the other practitioner's working papers.)

c. Communicate clearly with the other practitioner about the scope and timing of the other practitioner's work and findings. (Such communication enables the service auditor to plan the nature, timing, and extent of any procedures that relate to the work of the other

practitioner, including the involvement of the service auditor in the work of the other practitioner. Due to complexities involved in the planning of the engagement and obtaining agreement between all parties, using the work of an other practitioner is most likely to be successful when these matters are addressed early in engagement planning.)

d. Be involved in the work of the other practitioner, if assuming responsibility for the work of the other practitioner.

e. Evaluate whether the other practitioner's work is adequate for the service auditor's purposes. (To make this evaluation, the service auditor should obtain an understanding of the results of the other practitioner's work and findings associated with that work. The service auditor may obtain such an understanding through review of the report of the results of the other practitioner's procedures, discussions with the other practitioner, and inspection of the other practitioner's working papers.)

f. Determine whether to make reference to the other practitioner in the service auditor's report. (As stated in paragraph 2.173*c*, the service auditor ordinarily would not choose to refer to the other practitioner in the report because doing so is substantially equivalent to presenting a subservice organization using the carve-out method.)

2.173 In applying paragraph .33 of AT-C section 105 in a SOC 2 examination, consider a situation in which service organization management engages a service auditor to perform a type 2 examination that includes the service organization and a subservice organization. The service auditor determines that the subservice organization has already engaged an other practitioner (a subservice auditor) to perform a type 2 examination, which covers the same period as the period to be covered by the SOC 2 examination of the service organization and addresses the services provided to the service organization and relevant controls. The following are some options for the SOC 2 examination:

a. Service organization management may elect to carve out the subservice organization's services and controls, in which case certain report users will need to obtain a type 2 report from the subservice organization.

b. Service organization management may elect to present the subservice organization's services and controls using the inclusive method. In this case, a number of alternatives may be available for management and the service auditor, including the following:

i. The service auditor performs all the work and does not use the work of the subservice auditor, other than to consider whether the subservice auditor's type 2 report provides evidence that relevant controls at the subservice organization are not suitably designed or operating effectively. (However, the subservice auditor's type 2 report, if covering the same period as the service auditor's inclusive type 2 report, is unlikely to be available in time for use by the service auditor.)

ii. The service auditor uses the work of the subservice auditor and assumes responsibility for that work. In this scenario, the service auditor should comply with the requirements in paragraph .33 of AT-C section 105. The

description would include those aspects of the subservice organization's system that are relevant to the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria, and the description of tests of controls and results would include the tests performed by the subservice auditor and the results, without attributing the tests to the subservice auditor.

c. Although AT-C section 205 permits the service auditor to make reference to the subservice auditor, this option is rarely used for a number of reasons:

i. First, even if planning to make reference to the subservice auditor, a service auditor who plans to use the work of a subservice auditor should comply with all the requirements in paragraph .33 of AT-C section 105, including communicating clearly about the scope and timing of the subservice auditor's work and findings and evaluating whether the subservice auditor's work is adequate for the service auditor's purposes.

ii. Second, this option is substantially equivalent to presenting the subservice organization using the carve-out method in that report users would need to obtain the subservice auditor's report on the subservice organization that includes a description of the system, the tests performed, and results of tests.

iii. Third, report users are unlikely to understand the responsibilities of the service auditor and the subservice auditor in a SOC 2 report prepared under this approach.

2.174 When using the work of an other practitioner, paragraph .A59 of AT-C section 105 clarifies that the service auditor is responsible for directing, supervising, and performing the engagement in compliance with professional standards, applicable regulatory and legal requirements, and the firm's policies and procedures. The service auditor is also responsible for determining whether the report issued is appropriate in the circumstances.

2.175 Chapter 4 discusses reporting when the work of an other practitioner is used.

Planning to Use the Work of a Service Auditor's Specialist

2.176 When planning a SOC 2 examination, a service auditor may decide that engaging or assigning a specialist with specific skills and knowledge is necessary to execute the planned examination. If a service auditor's specialist will be used in the SOC 2 examination, paragraph .37 of AT-C section 205 states that the service auditor should do the following:

a. Evaluate whether the specialist has the necessary competence, capabilities, and objectivity for the service auditor's purposes. In the case of a specialist, the evaluation of objectivity should include inquiry regarding interests and relationships that may create a threat to the objectivity of the specialist.

b. Obtain an understanding of the specialist's field of expertise to enable the service auditor to determine the nature, scope, and objectives of the specialist's work and to evaluate the adequacy of that work.

c. Agree with the specialist regarding

i. the nature, scope, and objectives of the specialist's work;

ii. the respective roles and responsibilities of the service auditor and the specialist;

iii. the nature, timing, and extent of communication between the service auditor and the specialist, including the form of any report or documentation to be provided by the specialist; and

iv. the need for the service auditor's specialist to observe confidentiality requirements.

2.177 By communicating with the service auditor's specialist about these matters early in the engagement, the service auditor will be in a better position to plan the scope and timing of the specialist's work on the engagement. In addition, the service auditor will be better able to plan the nature, timing, and extent of any procedures that relate to the work of the specialist, including the direction, supervision, and review of the specialist's work, particularly if that work will be used during initial engagement planning and risk assessment. Though not required, the service auditor would generally consider documenting, in an engagement letter or other appropriate form of written communication, the understanding reached with the service auditor's specialist about the matters discussed. When evaluating the service auditor specialist's competence and capabilities, the service auditor may obtain information from a variety of sources, including discussions with the specialist, personal experience with the specialist's work, discussions with others who are familiar with the specialist's work, or published papers or books written by the specialist, among other things. In addition, the service auditor needs to determine that the specialist has a sufficient understanding of the attestation standards relevant to the SOC 2 examination and this guide to enable the specialist to understand how the specialist's work will help achieve the objectives of the engagement.

2.178 When evaluating the objectivity of the service auditor's external specialist, the service auditor may inquire of service organization management (or the engaging party, if different) about any known interests or relationships (such as financial interests, business and personal relationships, and provision of other services by the service auditor's external specialist) that management has with the specialist that may affect the objectivity of the specialist. In certain cases, the service auditor may decide to request written representations from the service auditor's external specialist about any interests or relationships with service organization management (or the engaging party, if different) of which the specialist is aware.

2.179 The service auditor may also discuss with the service auditor's specialist any safeguards applicable to the specialist and evaluate whether the safeguards are adequate to reduce known threats to independence to an acceptable level. There may be some circumstances in which safeguards cannot reduce such threats to an acceptable level. For example, if the service auditor's specialist has played a significant role in implementing or operating significant aspects of the service organization's system and controls necessary to achieve

its service commitments and system requirements, the specialist is likely not objective (independent) when measuring or evaluating the suitability of design of controls or, in a type 2 examination, the operating effectiveness of controls within that program.

2.180 Paragraph .A43 of AT-C section 205 states the following may be relevant to obtaining an understanding of the specialist's field of expertise:

a. Whether the specialist's field includes areas of specialty relevant to the engagement

b. Whether professional or other standards and regulatory or legal requirements apply

c. Assumptions and methods used by the specialist and whether they are generally accepted within the specialist's field and appropriate in the engagement circumstances

d. The nature of internal and external data or information used by the service auditor's specialist

2.181 The nature, timing, and extent of the service auditor's procedures to evaluate the matters discussed in this section vary depending on the circumstances of the engagement. When determining the nature, timing, and extent of those procedures, paragraph .39 of AT-C section 205 indicates that the service auditor should consider the following:

a. The significance of the service auditor's specialist's work in the context of the engagement

b. The nature of the matter to which the service auditor's specialist's work relates

c. The risks of material misstatement in the matter to which the service auditor's specialist's work relates

d. The service auditor's knowledge of and experience with previous work performed by the service auditor's specialist

e. Whether the service auditor's specialist is subject to the service auditor's firm's quality control policies and procedures

2.182 In addition to the matters discussed in this section, paragraph .37*d* of AT-C section 205 also indicates that the service auditor should evaluate the adequacy of the work of the service auditor's specialist for the service auditor's purposes. That evaluation is discussed further beginning in paragraph 3.210.

Meeting the Requirements of a Process or Control Framework

2.183 When management has included disclosures about a process or control framework in the description, the service auditor may need to broaden the understanding of the system to include an understanding of (1) the requirements of the process or control framework and (2) how the controls implemented by management met those requirements. Such an understanding assists the service auditor in evaluating (1) whether controls were implemented to achieve the related service commitments and related system requirements and (2) whether the description is presented in accordance with the description criteria.

SOC 2 Examination That Addresses Additional Criteria (SOC 2+)

2.184 In a SOC 2+ examination, management would be expected to modify its assertion to also address the evaluation of controls against the requirements of the process or control framework.

2.185 It is likely that the process or control framework is important to a broad range of users and management would identify meeting the requirements of the framework as a principal service commitment or service requirement. Management is also likely to disclose information about how the system components, including processes and controls (DC3), addressed requirements of the process or control framework and how the implemented controls met these requirements (DC5). The service auditor's responsibility for such disclosures is discussed in paragraphs 3.35 and 3.45.

2.186 In a SOC 2+ examination, the service auditor needs to evaluate whether the requirements of the process or control framework (additional criteria) are suitable criteria. Paragraphs .A44–.A52 of AT-C section 105 provide additional guidance on assessing the suitability of criteria. Likewise, the service auditor needs to determine whether such criteria are or will be available to the intended users. Paragraphs .A53–.A54 of AT-C section 105 provide additional guidance on assessing the availability of criteria. In accordance with paragraph .64 of AT-C section 205, if the additional criteria are appropriate for or will be available to only a subset of intended users, the service auditor's report should include an alert restricting the report's use to those users. Restricting the service auditor's report is discussed further in paragraph 4.36.

2.187 When the service organization uses subservice organizations, there may be additional considerations in the SOC 2+ examination. For example, if required controls are implemented at the subservice organization but management has elected to use the carve-out method to present the subservice organization, the service auditor should determine whether the subject matter is appropriate for the SOC 2+ examination. Based on the requirements in paragraph .28 of AT-C section 105, if the service auditor determines that the subject matter is not appropriate, the service auditor should discuss with service organization management the need to use the inclusive method. Unless management agrees to use the inclusive method, the service auditor may decide not to accept the engagement.

2.188 The scope of a SOC 2+ examination also includes the evaluation of controls against additional criteria. In accordance with paragraph .08 of AT-C section 205, the written agreement with the client about the terms of the engagement should identify the additional criteria in addition to management's and the service auditor's responsibilities related to them.

2.189 Because the process or control framework represents additional criteria, in accordance with paragraph .10 of AT-C section 205, the service auditor should request that management's written assertion also address its evaluation of whether the controls implemented by the service organization met the requirements of the process or control framework.

Accepting and Planning a SOC 3 Examination

2.190 For a SOC 3 examination, service organization management's responsibilities are substantially the same as those for a SOC 2 examination

except that management does not prepare a system description. Although management does not prepare a system description, it does disclose the boundaries of the system and the service organization's principal service commitments and system requirements as part of its written assertion. That is discussed beginning in paragraph 4.119.

2.191 Management's responsibilities, as the engaging party, during acceptance and planning of a SOC 3 examination, include the following:

- Defining the scope of the examination, as discussed in paragraph 2.05
- Specifying the principal service commitments made to user entities and the system requirements needed to operate the system
- Identifying and analyzing risks that could prevent the service organization from achieving its service commitments and system requirements
- Designing, implementing, monitoring, and documenting effective controls to provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria
- Identifying subservice organizations and determining whether to present them under the inclusive or carve-out method and, if using the carve-out method, identifying CSOCs, as discussed beginning in paragraph 2.14 and throughout this chapter

2.192 Because there is no description of the system in a SOC 3 report, some report users may not have a sufficient understanding of the service organization's system to understand how controls within the system operate. Before agreeing on a SOC 3 examination, management and the service auditor need to consider whether a SOC 3 report, which includes only management's assertion and the service auditor's opinion about the effectiveness of controls at the service organization, is likely to meet the information needs of intended report users or whether it is likely that a SOC 3 report will be misunderstood by potential report users. For example, a service organization that provides security monitoring services to commercial customers may determine that a SOC 3 report is likely to be misunderstood by consumers of its commercial customer user entities because those consumers are unlikely to have an adequate understanding of how commercial customers use the monitoring services. In such instances, management and the service auditor may agree to restrict the use of the SOC 3 report to the subset of potential report users (commercial customers) whose informational needs are likely to be met by a SOC 3 report.

2.193 The lack of a description may cause some report users to misunderstand a SOC 3 report of a service organization that uses a subservice organization when the subservice organization is presented using the carve-out method. Although the use of the carve-out method is permitted, consideration should be given to whether use of the carve-out method for presenting a subservice organization in a SOC 3 report may be misleading to users. A SOC 2 report of a service organization that presents a subservice organization using the carve-out method includes a description of the services provided by the subservice organization and describes the service organization's controls over those services, which permits report users to understand the role of the subservice organization in the context of the specific controls at the service organization. A SOC 3 report does not provide such information. In some cases, the disclosures

discussed in paragraph 2.190 regarding the boundaries of the system would include disclosure of the services performed by the carved-out subservice organization because it is likely to affect the boundary of the system to be addressed in the examination. In that case, such disclosures may provide users with the information they need to understand the role of the subservice organization and the activities the service organization performs to monitor the subservice organization. If, however, disclosures regarding the boundaries of the system do not contain sufficient information for users to understand how the carved-out subservice organization may affect the achievement of the service organization's service commitments and system requirements in the SOC 3 report, there may be a risk that the report will be misleading to report users. As a result, the SOC 3 report may need to be restricted to an appropriate subset of potential report users, such as user entities that have access to a SOC 2 report or a SOC 3 report from the subservice organization.

2.194 Similarly, some report users may misunderstand a SOC 3 report that indicates that CUECs are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. However, without the information provided in a system description, some SOC 3 report users may not have a sufficient understanding of the service organization's system to understand the context for implementing CUECs. As a result, the service auditor may consider restricting the SOC 3 report to an appropriate subset of potential report users that are likely to understand CUECs, such as user entities that have access to detailed communications about the nature of user entity responsibilities, CUECs, and how those CUECs interact with the service organization's own controls.

2.195 In a SOC 3 examination, the responsibilities of the service auditor are substantially the same as those in a SOC 2 examination and include the following:

- Determining whether to accept or continue the engagement
- Agreeing on the terms of the engagement
- Reaching an understanding with service organization management regarding the provision of a written assertion
- Establishing an overall strategy for the examination
- Performing risk assessment procedures

Chapter 3

Performing the SOC 2 Examination

This chapter discusses responding to the assessed risks, considering materiality, and other matters affecting the nature, timing, and extent of procedures the service auditor may perform to obtain sufficient appropriate evidence about whether (*a*) the description presents the system that was designed and implemented in accordance with the description criteria, (*b*) controls were suitably designed, and (*c*) in a type 2 examination, controls operated effectively.

Introduction

3.01 After the service auditor has assessed the risks of material misstatement, paragraphs .21–.22 of AT-C section 205, *Assertion-Based Examination Engagements*,[1] discuss how the service auditor should respond to the assessed risks when designing and performing examination procedures with regard to the following:

- The presentation of the description in accordance with the description criteria
- The suitability of design of controls to achieve the service commitments and system requirements based on the trust services criteria
- For a type 2 engagement, the operating effectiveness of controls to achieve the service commitments and system requirements based on the trust services criteria

Specifically, in accordance with those paragraphs, the service auditor should (*a*) design and implement overall responses to address the assessed risks of material misstatement and (*b*) design and perform further procedures whose nature, timing, and extent are based on, and responsive to, the assessed risks of material misstatement.

Designing Overall Responses to the Risk Assessment

3.02 The service auditor's assessment of the risk of material misstatement provides a basis for the design and implementation of procedures that are responsive to the risk assessment.

3.03 Aspects of the control environment or other components of internal control may enhance or mitigate the effectiveness of specific system controls. Conversely, ineffective aspects of the control environment or other components of the service organization's internal control may cause the service auditor to design and perform further procedures whose nature, timing, and extent are based on, and responsive to, the higher assessed risks related to the

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

ineffective aspects of the control environment or other components of internal control.

3.04 For example, consider a service organization that provides bonuses to employees who make no processing errors. In this environment, service organization personnel may be tempted to suppress the reporting of errors to receive bonuses. The service auditor may decide to increase the testing of controls that prevent, or detect and correct, errors in system processing (for example, reconciliations of inputs to outputs designed to identify exceptions) or may decide to test the entire population to determine whether controls are operating effectively.

3.05 Other overall responses a service auditor may select to address the assessed risks of material misstatement include the following:

- Emphasizing to the engagement team the need to maintain professional skepticism
- Assigning more-experienced staff or using specialists
- Providing more supervision
- Incorporating additional elements of unpredictability in the selection of procedures to be performed
- Making changes to the nature, timing, or extent of procedures (for example, selecting different types of procedures, or changing the timing of those procedures, to obtain evidence about the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls)

Designing and Performing Procedures

3.06 In accordance with paragraph .22 of AT-C section 205, the service auditor should design and perform further procedures whose nature, timing, and extent are based on, and responsive to, the assessed risks of material misstatement. Those further procedures relate to the presentation of the description in accordance with the description criteria and the suitability of design and operating effectiveness of controls. Designing and performing further procedures is discussed further throughout this chapter.

Considering Materiality in Responding to the Assessed Risks

3.07 In accordance with paragraph .17 of AT-C section 205, the service auditor should consider materiality both during risk assessment and when determining the nature, timing, and extent of procedures to perform during the SOC 2 examination. Adoption of an appropriate materiality for each of the subject matters in the SOC 2 examination, as discussed in chapter 2, "Accepting and Planning a SOC 2 Examination," allows the service auditor to prioritize testing efforts and supports an effective and efficient engagement.

3.08 Paragraph .A19 of AT-C section 205 states that materiality in an attestation engagement is considered in the context of qualitative factors and, when applicable, quantitative factors. The relative importance of each of those factors when considering materiality in a particular engagement is a matter of professional judgment, and those judgments are made considering the surrounding circumstances.

3.09 In accordance with paragraph .17 of AT-C section 205, when considering materiality regarding the description, the service auditor should consider whether there is substantial likelihood that description misstatements (including omissions), individually or in the aggregate, would influence the judgment made by the broad range of report users. Paragraph 3.84 discusses materiality considerations when evaluating whether the description presents the system that is designed and implemented in accordance with the description criteria.

3.10 When considering materiality regarding the suitability of design and operating effectiveness of controls, the service auditor should consider both qualitative and quantitative factors, as discussed beginning in paragraph 3.85.

Obtaining Evidence About Whether the Description Presents the System That Was Designed and Implemented in Accordance With the Description Criteria

3.11 As previously discussed, the description of the service organization's system presented in accordance with the description criteria is designed to enable user entities, business partners, and other intended users of the SOC 2 report (known collectively as *report users*) to understand the service organization's system, including the processing and flow of data and information through and from the system, and other information that may be useful when assessing the risks arising from interactions with the service organization's system, particularly system controls that service organization management has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria. For example, disclosures about the types of services provided, the environment in which the service organization operates, and the components of the system used to provide such services allow users to better understand the context in which the system controls operate.

3.12 Service organization management is responsible for preparing the description of the system that was designed and implemented in accordance with the description criteria presented in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*.[2] The service auditor is responsible for expressing an opinion about whether the description is prepared in accordance with the description criteria and reflects the system and related controls that the service organization has implemented. An unmodified opinion that the description presents the system that was designed and implemented in accordance with the description criteria does not imply that the controls stated in the description are suitably designed or, in a type 2 examination, that controls operated effectively.

3.13 Generally, management prepares the description from documentation supporting the system of internal control and system operations and from consideration of the policies, processes, and procedures (controls) within the system used to provide the services.

---

[2] All DC sections can be found in AICPA *Description Criteria*.

3.14 Although the description is generally narrative in nature, there is no prescribed format for the description. Service organization management may organize the description in a variety of different ways, provided that disclosures called for by the description criteria are included. For example, the description may be organized by components of internal control (the control environment, risk assessment process, control activities, monitoring activities, and information and communications). It may also be organized by components of the system (infrastructure, software, people, data, and processes and procedures). Management may use other logical groupings of information in organizing its system description, including the use of recognized industry frameworks or standards based on management's objectives. For instance, the system description may be organized by control families or control objectives listed in a process or control framework.

3.15 Regardless of the method used to organize the system description, it is supplemented by disclosures of the aspects of the internal control components relevant to the identification and assessment of risks that would prevent the service organization from achieving its service commitments and system requirements and by disclosures of the design, implementation, and operation of controls to address those risks. It is good practice to map the controls listed back to the relevant criteria in each of the trust services categories to ensure the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Flowcharts, matrixes, tables, graphics, context diagrams, or a combination thereof may be used to supplement the narratives contained within the description.

3.16 The extent of disclosures included in the description may vary depending on the size and complexity of the service organization and its activities. In addition, the description need not address every aspect of the service organization's system. For example, although the service organization may use both manual and automated systems to provide services to user entities, the description need not necessarily disclose every step in that process. Furthermore, if certain aspects of those services are not relevant to report users or are beyond the scope of the SOC 2 examination, the description need not address them. For example, a service organization's processes related to billing for services provided to user entities are unlikely to be relevant to report users.

3.17 Although a description prepared in accordance with the description criteria is expected to include disclosures about each description criterion, such disclosures are not intended to be made at such a detailed level that they might increase the likelihood that a hostile party could exploit a security vulnerability, thereby compromising the service organization's ability to achieve its service commitments and system requirements. Instead, the disclosures are intended to enable report users to understand the nature of the risks faced by the service organization and the impact of the realization of those risks.

3.18 When evaluating whether the description is presented in accordance with the description criteria, service organization management and the service auditor may consider the following:

Table 3-1

Characteristics That May Indicate Whether the Description Is Presented in Accordance With the Description Criteria

Characteristics That May Indicate the Description Is Presented in Accordance With the Description Criteria	*Characteristics That May Indicate the Description Is* Not *Presented in Accordance With the Description Criteria*
The description includes the significant components of the system the service organization has designed and implemented (placed into operation).	The description states or implies certain facts that are not true (for example, that system components exist when they do not or that a service organization's controls meet all requirements of a security process or control framework when they do not).
The description does not inadvertently or intentionally omit or distort information that is likely to be relevant to intended users' decisions.	The description states or implies that certain processes or controls have been implemented when they are not being performed.
The description includes information about each description criterion, to the extent it is relevant to the system being described, without using language that omits or distorts the information.	The description inadvertently or intentionally omits or distorts material information about any of the description criteria that might affect the decisions of report users (for example, the failure to include in the description significant aspects of processing performed at another location included within the scope of the examination).
The description includes information relevant to users and which can be measured or evaluated based on the description criteria.	The description contains statements that cannot be objectively evaluated (for example, unsubstantiated advertising claims such as describing a service organization as being "world's best" or "most respected in the industry").
The description is prepared at a level of detail likely to be meaningful to intended users.	The description is prepared at such a high level that it omits significant amounts of information relevant for decision-making by intended users.
The characteristics of the presentation, such as the format, are appropriate, given that the description criteria allow for variations in presentation.	Certain characteristics of the presentation of the description are confusing and obscure critical information about the system.

3.19 Implementation guidance for each criterion, which is presented in DC section 200, is intended to assist management when preparing the description and the service auditor when evaluating whether the description is presented in accordance with the description criteria. The guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. The implementation guidance does not address all possible situations; therefore, service organization management and the service auditor may need to consider other facts and circumstances of the service organization and its environment when applying the description criteria.

3.20 The service auditor's procedures for evaluating whether the description is in accordance with the description criteria begin with obtaining and reading the description of the service organization's system and evaluating whether it presents the system that was designed and implemented based on the service auditor's understanding of the system and other relevant procedures performed. In addition to the more specific procedures described in the remainder of this section, the service auditor may perform any of the following procedures, or a combination thereof, to obtain evidence about whether the description presents the system that was designed and implemented in accordance with the description criteria:

- Making inquiries of management and other service organization personnel about the content of management's assertion and the description of the system
- Reading the service organization's annual report, if there is one, to understand the service organization's objectives and strategy and their relationship to the services provided to user entities
- Inspecting documentation supporting the service organization's identification and assessment of risks, including the determination of how the service organization plans to mitigate such risks
- Reading documents (such as board minutes, organization charts, and communications about the security, availability, and processing integrity of the system and the confidentiality or privacy of the information it uses) to understand the service organization's risk governance structure and processes, including
    - — the involvement of board members,
    - — the organizational structure to support the service organization's system,
    - — the threat and vulnerability assessments the service organization performs (both internal and external), and
    - — the types and frequency of communications made to executive management and others about the security, availability, and processing integrity of the system and the confidentiality or privacy of the information it uses
- Reading documents about the service organization's security awareness and training programs, communication of code of conduct, employee handbooks, information security policies, incident notification procedures, and other available documentation to understand the service organization's processes for communicating to service organization personnel their responsibilities for system security and other related matters

- Reading internal audit reports, third-party assessments, audit committee presentations, and other documentation related to the service organization's monitoring activities, system incidents, or investigative activities
- Reading documents describing laws, regulations, or industry standards relevant to the service organization's service commitments and system requirements

3.21 If the service auditor believes that the description is misstated or otherwise misleading, the service auditor ordinarily would ask service organization management to amend the description by including the omitted information or by revising the misstated or otherwise inappropriate information. If service organization management refuses to amend the description, and the service auditor concludes that the description is not in accordance with the description criteria, in all material respects, the service auditor should modify the opinion in accordance with paragraph .72 of AT-C section 205.

3.22 Determining whether the description of a service organization's system presents the system that was implemented also involves evaluating whether each control stated in the description has been implemented. The service auditor's procedures to determine whether the controls stated in the description have been implemented may be similar to, and performed in conjunction with, procedures to obtain an understanding of the system as discussed in chapter 2. In addition, the procedures described beginning in paragraph 3.50 may be performed to obtain evidence about whether the controls stated in the description have been implemented.

3.23 If the service auditor determines that certain controls identified in the description have not been implemented, the service auditor may ask service organization management to delete those controls from the description. If management does not remove the controls from the description, and the service auditor concludes that the description is not in accordance with the description criteria, in all material respects, the service auditor should modify the opinion on the description in accordance with paragraph .72 of AT-C section 205. Paragraph 4.77 presents a separate paragraph that would be added to the service auditor's report when the description includes controls that have not been implemented. In addition, when evaluating the suitability of the design and, in a type 2 examination, the operating effectiveness of the controls, failure to implement those controls may result in controls not being suitably designed. (Paragraph 3.176 discusses a situation in which controls do not operate during the period of the examination.)

Disclosures About the Types of Services Provided

3.24 Description criterion DC1 requires that service organization management include in the description certain disclosures about the types of services provided by the service organization. Disclosures about the types of services provided by the service organization would generally focus on the services that relate to the systems that are within the scope of the SOC 2 examination. Description criterion DC1 also contains implementation guidance that is intended to assist service auditors when evaluating the nature and extent of disclosures about the services provided. For example, the implementation guidance indicates that when the SOC 2 examination addresses privacy, disclosures about the types of services provided by the service organization should clearly

identify whether the service organization functions as a data processor or data controller.

3.25 When evaluating the nature and extent of disclosures about the services provided by the service organization, the service auditor may perform a combination of the following procedures:

a. Reading the service organization's annual report, if there is one, to understand the nature of the service organization's operations and the types of services provided

b. Reading contracts with customers and business partners (such as performance or service-level agreements), marketing materials distributed to customers and business partners or posted on the service organization's website, and other available documentation to better understand the specific services provided

c. Reading other documents related to the services provided by the service organization

Disclosures About Service Commitments and System Requirements

3.26 As discussed in chapter 2, service organization management is responsible for designing, implementing, and operating the system to achieve its service commitments to user entities and the system requirements that are necessary to enable the system to achieve those commitments and comply with laws and regulations. Description criterion DC2 requires disclosure of only the service organization's principal service commitments and system requirements. Disclosure of the principal service commitments and system requirements enables SOC 2 report users to understand how the system operates and how management and the service auditor evaluated the suitability of the design of controls and, in a type 2 examination, the operating effectiveness of controls based on the trust services criteria.

3.27 The service commitments that a service organization makes to user entities vary based on the needs of the user entities. Service organization management need not disclose every service commitment to every user entity; however, it should disclose those that are likely to be useful to the broad range of SOC 2 report users.

3.28 Likewise, management usually discloses only the principal system requirements that are relevant to or affected by the trust services category or categories addressed by the examination. When identifying which system requirements to disclose, service organization management may consider matters such as internal policies that are relevant to the system being described, key decisions made in the design and operation of the system, and other business requirements for the system. For example, management would ordinarily not disclose internal requirements related to the operating margin for the services associated with the system because such information is unlikely to be useful to the broad range of SOC 2 report users.

3.29 Description criterion DC2 contains implementation guidance that is intended to assist with the evaluation of the nature and extent of disclosures about principal service commitments and system requirements. An example of disclosure of a service organization's principal service commitments and system requirements is available on the AICPA website.

3.30 Disclosure of the types of system commitments and system requirements made or a reference to an external source of such information is not considered disclosure of the principal service commitments or system requirements. Furthermore, such disclosure is unlikely to provide report users with sufficient information to understand the application of the trust services criteria.

3.31 When deciding whether disclosures about principal service commitments and system requirements are appropriate, the service auditor may consider matters such as the following:

a. Are the principal service commitments presented in sufficient detail for report users to understand the relationship between the controls implemented by the service organization and the service commitments and system requirements? For example, a service organization commits to implement certain system components at a second data center to mirror transaction data on a real-time basis to meet a commitment to provide failover processing in the event of a disruption of services. When describing its availability commitment, service organization management would generally include such details to enable users of the report to better understand the organization's failover procedures.

b. When the SOC 2 report is designed for a broad range of users, does the description disclose the principal service commitments that are common to such report users? For example, assume a service organization makes a general system availability commitment to all user entities but makes additional service-level agreements to others. In such situations, the description may be presented in accordance with the description criteria if it discloses as a principal service commitment the availability commitments made commonly to all user entities but not the availability commitments made to specific user entities.

Considering the Appropriateness of the Service Organization's Service Commitments and System Requirements During the Examination

3.32 After accepting the SOC 2 examination, the service auditor may become aware of information that causes him or her to believe that the principal service commitments and system requirements stated in the description are not, in fact, appropriate for the engagement. A failure to disclose principal service commitments or system requirements may cause the practitioner to question whether management also failed to identify its service commitments and system requirements for risk assessment purposes and, as a result, controls may not be suitably designed or operating effectively.

3.33 During the performance of further procedures, for example, the service auditor may become aware of information that contradicts information previously obtained. Assume, for example, that the service organization provides insurance underwriting software-as-a-service that uses both publicly available data and purchased proprietary data. The service organization has not established system requirements related to the completeness and accuracy of the data obtained from public sources. Because the service organization did not establish such a system requirement, it failed to identify and assess the risks that such requirements would not be achieved. In addition, it did not design, implement, and operate controls to mitigate such risks or disclose any principal

system requirement related to that data. Accordingly, the service organization's service commitments and system requirements are incomplete and, therefore, not appropriate in the circumstances. In this situation, the service auditor may conclude that a modification of the opinion is appropriate because of either of the following:

- The service commitments and system requirements identified in the description in accordance with description criterion DC2 are not appropriate; therefore, the description is not presented in accordance with the description criteria.
- Controls over the objective-setting process were not suitably designed and the service organization's controls were not effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on CC3.1, *The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*

In such a situation, the service auditor would generally discuss the matter with service organization management. If service organization management refuses to amend the description and the service auditor concludes that the description is not in accordance with the description criteria, in all material respects, the service auditor should modify the opinion in accordance with paragraph .72 of AT-C section 205.

3.34 Because the service commitments and system requirements need to be appropriate to enable both service organization management and the service auditor to evaluate whether system controls are suitably designed and, in a type 2 examination, operating effectively, the lack of appropriate service commitments and system requirements may have a pervasive effect on the SOC 2 examination. In such situations, an adverse opinion on the description, the suitability of controls, and in a type 2 examination, the operating effectiveness of controls, would be appropriate. Expressing an adverse opinion in a SOC 2 examination is discussed beginning in paragraph 4.57.

Disclosures About Components of the System

3.35 Description criterion DC3 requires that service organization management include in the description an identification and discussion of the components of the system used to provide the services, including the (*a*) infrastructure, (*b*) software, (*c*) people, (*d*) procedures, and (*e*) data. Description criterion DC3 also contains implementation guidance for evaluating the nature and extent of disclosures about components of the system.

3.36 When evaluating the nature and extent of disclosures about components of the system, the service auditor may perform procedures including the following:

a. Reading sample contracts with users (for example, contract templates or a selection of contracts) and associated performance or service-level agreements and other documentation to understand the nature of the inputs provided by users

b. Reading policy and procedure manuals, system documentation, flowcharts, narratives, hardware asset management records, and other system documentation to understand the service organization's use of technology, including its applications, infrastructure,

network architecture, use of mobile devices, use of cloud technologies, and the types of external party access or connectivity to the system

c. Comparing the service auditor's understanding of the system obtained through the performance of procedures to assess the suitability of design and operating effectiveness of controls to information obtained from other sources

3.37 Description of the procedures implemented by the service organization may include information about the service organization's risk assessment process and disclosure of significant risks identified by that process. These disclosures may assist user entities in identifying risks related to their use of the services provided by the service organization. If such disclosures are included, the service auditor would need to make sure that they are consistent with the evidence obtained to support an opinion on the description. For example, the service auditor's review of management risk assessment documentation during risk assessment may help the service auditor make that determination.

Disclosures About System Incidents

3.38 Description criterion DC4 requires that service organization management include in the description certain information related to system incidents that (*a*) were the result of controls that were not suitably designed or operating effectively or (*b*) otherwise resulted in a significant failure in the achievement of one or more of service commitments and system requirements, as of the date of the description (for a type 1 examination) or during the period of time covered by the description (for a type 2 examination), as applicable.

3.39 Both DC section 200 and TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*,[3] provide the following definitions to assist service organization management and the service auditor in determining if an incident has occurred:

system event. An occurrence that could lead to the loss of, or disruption to, operations, services, or functions and result in a service organization's failure to achieve its service commitments or system requirements. Such an occurrence may arise from actual or attempted unauthorized access or use by internal or external parties and (*a*) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems; (*b*) result in unauthorized disclosure or theft of information or other assets or the destruction or corruption of data; or (*c*) cause damage to systems. Such occurrences also may arise from the failure of the system to process data as designed or from the loss, corruption, or destruction of data used by the system.

system incident. A system event that requires action on the part of service organization management to prevent or reduce the impact of the event on the service organization's achievement of its service commitments and system requirements.

[3] All TSP sections can be found in AICPA *Trust Services Criteria*.

3.40 If service organization management determines that a system incident as defined in description criterion DC4 has occurred, the description should include the following information about each incident:

- Nature of the incident
- Timing surrounding the incident
- Extent (or effect) of the incident and its disposition

3.41 The following illustrates a disclosure made about an identified system incident that resulted in a significant failure of the service organization to achieve one of its availability commitments:

> In February 20XX, XYZ experienced a denial-of-service attack on its transportation management system (TMS) that supports the transportation management services provided to its customers. The attack impaired the ability of the system to operate as designed. Although XYZ's security team and engineers resolved the issue through redistribution of traffic and systems, the TMS suffered a significant disruption and customers were unable to schedule or receive transportation for five days. Accordingly, the attack prevented XYZ from achieving its commitment that the maximum duration of a loss of system availability would be no more than 24 hours.

System incidents are not limited to security breaches. For instance, an outage at a cloud service provider that caused disruption of service may necessitate disclosure if it significantly affected the service organization's achievement of its service commitments and system requirements regarding availability.

3.42 When evaluating the completeness, nature, and extent of disclosures about system incidents, the service auditor may perform a combination of the following procedures:

- Understanding service organization management's process for identifying and evaluating the significance of system incidents
- Obtaining the listing of system incidents and their resolution for the examination period from the incident ticketing system and reperforming an independent evaluation of the significance of such incidents
- Inquiring of service organization management and inspecting documentation about the resolution of significant incidents that occurred during the prior period
- Inspecting documentation related to the remediation of significant system incidents

3.43 After performing these procedures, the service auditor may conclude that there were no significant system incidents during the period. Although not required by DC4, if no significant incidents occurred during the examination period, management may include a statement in the description to that effect.

3.44 If management includes in the description disclosures about identified system incidents as defined in description criterion DC4, the service auditor is likely to conclude that those incidents resulted from controls that were not suitably designed or operating effectively. In such instances, a modified opinion on suitability of design or operating effectiveness, or both, would be appropriate.

Disclosures About Individual Controls

3.45 Description criterion DC5 requires that the description disclose the applicable trust services criteria (that is, those that relate to the categories addressed by the description) and the related controls designed and implemented to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. For example, if the description addresses availability, service organization management would provide information about the controls it has implemented to address the common criteria in the trust services criteria and the additional trust services criteria for availability.

3.46 In addition to describing only controls that have been implemented, the description should provide sufficient details about each control to enable report users, particularly user entities and business partners, to understand how each control may affect their interactions with the service organization. Table 3-2 presents information about each control that generally would be included in the description.

Table 3-2

Information About Controls to Be Included in the Description of the System

Information to Be Included in a Description of a Control	*Illustrative Control*
What: The subject matter to which the control is applied	Requests for ***changes to production, source, and object code***[4] are initiated by preparing and submitting a change ticket to the Change Control Board for approval. The system automatically logs ***changes made to production, source, and object code***. On a weekly basis, the change manager reviews the log of system changes and the approved change tickets to identify unauthorized and missing changes by determining that (1) there is an approved change ticket for each entry in the log and (2) all the changes identified in the approved change tickets have been recorded in the log. Any unauthorized or missing changes are entered into an incident record in the Incident Management System. Incident records are assigned to the application manager of the affected application for follow-up and resolution. The change manager tracks open records to resolution and prepares a weekly report to the vice president of application development.

(continued)

[4] ***Boldface italics*** in the right-hand column of this table indicate text that specifically answers the questions posed in the left-hand column.

Information About Controls to Be Included in the Description of the System — *continued*

Information to Be Included in a Description of a Control	*Illustrative Control*
Who: The party responsible for performing the control	Requests for changes to production, source, and object code are initiated by preparing and submitting a change ticket to the ***Change Control Board*** for approval. The system automatically logs changes made to production, source, and object code. On a weekly basis, the ***change manager*** reviews the log of system changes and the approved change tickets to identify unauthorized and missing changes by determining that (1) there is an approved change ticket for each entry in the log and (2) all the changes identified in the approved change tickets have been recorded in the log. Any unauthorized or missing changes are entered into an incident record in the Incident Management System. Incident records are assigned to the application manager of the affected application for follow-up and resolution. The ***change manager*** tracks open records to resolution and prepares a weekly report to the ***vice president of application development***.
How: The nature of the activity performed, including sources of information used in performing the control	Requests for changes to production, source, and object codes are initiated by ***preparing and submitting a change ticket*** to the Change Control Board for approval. The system automatically logs changes made to production, source, and object codes. On a weekly basis, the change manager ***reviews the log of system changes and the approved change tickets to identify unauthorized and missing changes by determining that (1) there is an approved change ticket for each entry in the log and (2) all the changes identified in the approved change tickets have been recorded in the log***. Any unauthorized or missing changes are ***entered into an incident record in the Incident Management System***. Incident records are assigned to the application manager of the affected application ***for follow-up and resolution***. The change manager ***tracks open records to resolution and prepares a weekly report to the*** vice president of application development.

Information About Controls to Be Included in the Description of the System — *continued*

Information to Be Included in a Description of a Control	*Illustrative Control*
When: The frequency with which the control is performed, or the timing of its occurrence	Requests for changes to production, source, and object code are initiated by preparing and submitting a change ticket to the Change Control Board for approval. The system ***automatically*** logs changes made to production, source, and object code. On a ***weekly basis***, the change manager reviews the log of system changes and the approved change tickets to identify unauthorized and missing changes by determining that (1) there is an approved change ticket for each entry in the log and (2) all the changes identified in the approved change tickets have been recorded in the log. Any unauthorized or missing changes are entered into an incident record in the Incident Management System. Incident records are assigned to the application manager of the affected application for follow-up and resolution. The change manager tracks open records to resolution and prepares a ***weekly*** report to the vice president of application development.

3.47 Although service organization management may describe the system controls in the description, it also might refer to a table of controls presented in a separate section of the SOC 2 report. If the description refers to a table of controls, the table is considered part of the description; therefore, it is addressed by the service auditor's examination. Often, as noted later, the service auditor describes the tests of controls performed and the results thereof in the same table. Guidance on the types of information to be included in the description of tests of controls and the results thereof is discussed beginning in paragraph 4.25.

3.48 When deciding how best to present controls, service organization management may select the format that best meets its objectives, the needs of its users, and its users' likely frame of reference; it may also consider the risk that use of a particular format may be misleading to users. The service auditor would generally consider similar factors when evaluating whether the description is presented in accordance with the description criteria. Common formats for presenting controls in a SOC 2 report are included in the following examples:

Example 1:

- Controls, organized by trust services category and criteria, are presented in a table in section 4.
- The service auditor's description of the tests performed and the results of such tests are presented alongside the controls.

Under this format, a control is often listed multiple times when it addresses more than one trust services criterion. The service auditor may choose to present the description of tests performed and the results of such tests only the first time the control is presented; later instances of the control can be cross-referenced back to the first.

Example 2:

- Controls, organized by service organization process (for instance, identity and access management, security incident management, change management) are presented in section 4.
- The service auditor's description of tests performed and the results of such tests are presented alongside the control.
- The relationship of the controls to the trust services criteria is presented in a separate table, typically organized by trust services criteria, in either section 3 or section 4. This format allows the details of a control to be listed only once. For cross-referencing purposes, controls are identified by a unique identifier that is used in both tables. The unique identifier may be a control name, a number, (such as 1, 2, 3) or a reference to the schema used by another process or control framework (for instance, AC-1, AC-2, or SR-12 from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*). To prevent the presentation from being misleading, both tables may include information about any deviations noted.

Example 3:

Example 3 is similar to example 2, but instead of listing controls by service organization process, controls are grouped using the organizational structure of a security process or control framework such as the NIST Cybersecurity Framework (NIST CSF).

3.49 A service organization may have controls that it considers to be outside the boundaries of the system within the scope of the engagement, such as controls related to the conversion of new user entities to the service organization's systems. To avoid any misunderstanding by report users, the description should clearly delineate the boundaries of the system included within the scope of the engagement.

3.50 The service auditor may perform a variety of procedures to obtain evidence about the nature and extent of disclosures related to individual controls and the applicable trust services criteria, including a combination of the following:

- Reading contracts with customers and business partners, such as performance or service-level agreements, marketing materials distributed to customers and business partners or posted on the service organization's website, and other available documentation to evaluate whether the controls the service organization has implemented are suitably designed to achieve the service organization's commitments to customers
- Observing controls or other activities performed by service organization personnel

- Reading documents about the service organization's security awareness and training programs, communication of code of conduct, employee handbooks, security policies, incident notification procedures, and other available documentation to understand the service organization's processes for communicating to service organization personnel their responsibilities for system security and other related matters
- Reading policy and procedure manuals, system documentation, flowcharts, narratives, asset management records, and other system documentation to understand IT policies and procedures and controls over data loss prevention, access provisioning and deprovisioning, user identification and authentication, data destruction, system event monitoring and detection, and backup procedures
- Reading sample contracts with subservice organizations and associated performance or service-level agreements and other documentation to understand how the service organization's contracting process addresses security-related matters; the interrelationship between the service organization and its subservice organizations, including the service organization's process for assessing and managing system risks associated with those subservice organizations; the process the service organization uses to identify its responsibilities for implementing controls that have been communicated by a subservice organization (for example, user entity responsibilities or complementary user entity controls [CUECs] identified in a subservice organization's contract); and the procedures the service organization performs to monitor the effectiveness of controls performed by subservice organizations, when complementary subservice organization controls (CSOCs) have been identified
- Reading incident response and recovery plan documentation to understand the service organization's processes for recovering from identified system events, including its incident response procedures, incident communication protocols, recovery procedures, alternate processing plans, and procedures for the periodic testing of recovery procedures

3.51 Performing walk-throughs provides evidence about whether the controls stated in the description have been implemented. Performing a walk-through involves making inquiries of service organization management and other personnel and requesting them to describe and demonstrate their actions in performing a procedure. Walk-through procedures include following a transaction, event, or activity from origination until final disposition through the service organization's system using the same documents used by service organization personnel. Walk-through procedures usually include a combination of inquiry, observation, inspection of relevant documentation, flowcharts, questionnaires, or decision tables to facilitate understanding the design of the controls. Such procedures enable the service auditor to gain a sufficient understanding of the controls to determine whether they have been implemented as stated in the description of the service organization's system.

3.52 During a walk-through, the service auditor may inquire about instances during the period in which controls did not operate as described or

designed. In addition, the service auditor may inquire about variations in the process for different types of events or transactions. For example, the service organization's processing may take different forms, depending on how information is collected from user entities and business partners. Assume, for example, that the service organization receives transactions by mail, phone, fax, voice response unit, or via the internet. The service organization may design different controls related to the way the information is collected. An appropriately performed walk-through provides an opportunity to verify the service auditor's understanding of the flow of transactions and the design of the controls. If properly performed, walk-throughs may provide evidence about whether controls included in the description, individually or in combination with other controls, were suitably designed and implemented and, in a type 2 examination, operated effectively.

Disclosures About Complementary User Entity Controls and User Entity Responsibilities

3.53 As discussed in chapter 2, CUECs are controls that are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. When there are CUECs, description criterion DC6 requires that the description contain certain disclosures about those controls, including a statement that user entities are responsible for implementing those CUECs.

3.54 As it relates to CUECs, the description is presented in accordance with the description criteria if the CUECs are complete, accurately described, and necessary as discussed in paragraph 3.53. When making this evaluation, the service auditor may review system documentation and contracts with user entities, make inquiries of service organization personnel, and perform other such procedures as considered necessary.

3.55 For a user entity to derive the intended benefits of using the services of the service organization, the user entity has certain additional responsibilities related to the system. For example, the user of an express delivery service is responsible for providing complete and accurate recipient information and for using appropriate packaging materials. In this guide, such responsibilities are referred to as *user entity responsibilities*.

3.56 Trust services criterion CC2.3 states, *The entity communicates with external parties regarding matters affecting the functioning of internal control*, which would include communication of user responsibilities. Because user responsibilities are frequently voluminous, it is often impractical to communicate them in the description of the system; instead, they are usually communicated through other methods (for example, by describing them in user manuals). As a result, description criterion DC6 does not require that service organization management disclose user entity responsibilities. Instead, management ordinarily identifies in the description the types of communications it makes to external users, particularly user entities, about user entity responsibilities. The form and content of such disclosures is the responsibility of service organization management.

3.57 If service organization management has referred to the communications of user entity responsibilities that relate only to specific users, the service auditor would need to consider whether other intended users of the SOC 2

report are likely to misunderstand the description. If the service auditor believes the description is likely to be misunderstood, the service auditor would need to restrict the report to those specified parties to whom the responsibilities relate. If service organization management does not want the report to be restricted, management would include the significant user entity responsibilities in the description of the service organization's system to prevent users from misunderstanding the system and the service auditor's report. In that case, the service auditor's report would be appropriate for the broad range of SOC 2 report users.

3.58 When the description includes significant user entity responsibilities, the service auditor would need to evaluate those disclosures as part of the evaluation about whether the description is presented in accordance with the description criteria.

Disclosures Related to Subservice Organizations

3.59 When the service organization uses a subservice organization, description criterion DC7 requires that certain disclosures about the subservice organization be included in the description. The disclosures to be included depend on whether service organization management has selected the carve-out method or inclusive method, as discussed in chapter 2.

Disclosures When Using the Inclusive Method

3.60 When the inclusive method is used to present the services provided by a subservice organization, description criterion DC7 requires disclosure of the following information:

- The nature of the service provided by the subservice organization
- The controls at the subservice organization that are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria
- Relevant aspects of the subservice organization's infrastructure, software, people, procedures, and data
- The portions of the system that are attributable to the subservice organization

3.61 The description of 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 to the extent that they are relevant to controls at the service organization. The description should separately identify controls at the service organization and controls at the subservice organization; however, there is no prescribed format for differentiating between the two.

3.62 In addition, it may be useful for the service organization to disclose its interactions with vendors related to the services provided by them. When such disclosures are made, it may be helpful if service organization management distinguishes between the services provided by subservice organizations and vendors.

Disclosures When Using the Carve-Out Method

3.63 When the carve-out method is used, management would not include a description of the controls that operate at the subservice organization. Nevertheless, the description should contain sufficient information concerning the carved-out services to do the following:

- Alert report users to the fact that another entity (the subservice organization) is involved in the processing of the user entities' or business partners' transactions, to enable report users to understand the significance and relevance of the subservice organization's services to the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria
- Identify the types of controls that service organization management assumes would be implemented by the subservice organization and that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved (complementary subservice organization controls or CSOCs) based on the applicable trust services criteria (CSOCs are discussed further starting at paragraph 3.69)

3.64 When the carve-out method is used, description criterion DC7 requires disclosure of the following information:

- The nature of the service provided by the subservice organization
- Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization
- The types of controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization and that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved

The description would not include the detailed processing or controls performed by the subservice organization.

Considerations Applicable to Both Methods

3.65 The description of the services provided by a subservice organization should be prepared at a level of detail that could reasonably be expected to meet the common informational needs of the broad range of report users. The following is an example of a description of a service organization that uses a subservice organization to provide its computer processing infrastructure:

> Trust Group Service Organization outsources aspects of its computer processing to Computer Outsourcing Subservice Organization.

This description may not be detailed enough to enable report users to determine the significance of the services provided by the subservice organization. The following is a more detailed description that provides the necessary information:

> Trust Group Service Organization hosts its Trust System at Computer Outsourcing Subservice Organization. Trust Group maintains responsibility for application changes and user access, and Computer

> Outsourcing Subservice Organization provides the computer processing infrastructure and changes thereto.

3.66 Regardless of whether the carve-out or inclusive method is selected, service organization management is not required to disclose the identity of the subservice organization. However, that information may be helpful to report users (particularly user entities and business partners) who wish to obtain information about and perform procedures related to the services provided by the subservice organization. If the description does not disclose the identity of the subservice organization, the service auditor may discuss this matter with management and explain why such information may be needed by some report users.

3.67 Additionally, regardless of the method used, service organization management is responsible for designing, implementing, and operating controls and other activities to monitor the effectiveness of controls performed by the subservice organization; such monitoring should be described in the system description. Monitoring activities are usually a necessary part of the service organization's system of internal control; in other words, they are necessary for controls to provide reasonable assurance that the service organization's service commitments and system requirements are achieved. These types of activities are evaluated using trust services criterion CC9.2, *The entity assesses and manages risks associated with vendors and business partners.*

3.68 Monitoring activities usually include some combination of (*a*) ongoing monitoring to determine that potential issues are identified timely and (*b*) separate evaluations to determine that subservice organization controls are effective over time. Examples of monitoring activities include reviewing and reconciling output reports, holding periodic discussions with subservice organization personnel, making regular site visits to the subservice organization, the internal audit function performing tests of controls at the subservice organization, reviewing type 1 or type 2 SOC reports on the subservice organization's system, and monitoring external communications (such as customer complaints) relevant to the services provided by the subservice organization.

Disclosures About Complementary Subservice Organization Controls

3.69 As discussed in chapter 2, when using the carve-out method, the achievement of one or more of the service organization's service commitments or system requirements is dependent on one or more controls at the subservice organization. Such controls are called complementary subservice organization controls (CSOCs). In such a situation, description criterion DC7 requires that the description identify such CSOCs. To be meaningful to report users, CSOCs included in the description are those that are specific to the services provided by the service organization's system. Typically, service organization management presents the CSOCs as broad categories of controls or types of controls that the subservice organization should have in place. For example, the service organization might identify the following CSOC to address CC6.1, *The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives*:

> Logical access to system infrastructure is restricted by native operating system and application-based security through the use of access control lists.

This broad category of control is more appropriate as it allows the subservice organization greater flexibility to identify and implement suitable controls for its environment than identifying multiple, narrowly defined controls such as the following:

> Passwords for in-scope systems are configured to require 8-character minimum and 90-day password changes.
>
> Management performs quarterly access reviews to ensure access is restricted appropriately.

3.70 The following are additional examples of CSOCs related to logical access that service organization management may assume are in place at the subservice organization:

- XYZ Service Organization outsources the management of IT infrastructure to a subservice organization. Using the service organization's systems, subservice organization personnel manage access 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 Organization's controls assumes that the subservice organization has suitably designed, implemented, operated, and monitored controls that restrict access to authorized users identified at the operating system and database layers.

- XYZ Service Organization outsources the promotion of program changes to the production environment to a subservice organization. In this scenario, the service organization has granted privileged access to the operating system and database layers to personnel from the subservice organization to facilitate the movement of program 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 suitably designed, implemented, operated, and monitored a control requiring periodic review of users with privileged access at the operating system and database layers and requiring notification of the service organization of necessary changes in access.

3.71 Because CSOCs are necessary, in combination with the service organization's controls, to provide reasonable assurance that certain service commitments and system requirements are achieved based on the applicable trust services criteria, it is important that the description also include the subservice organization's responsibilities for implementing them and indicate that the service organization can only achieve the related service commitments and system requirements if the CSOCs are suitably designed and, in a type 2 examination, operating effectively throughout the period. The service auditor also considers CSOCs when evaluating the suitability of design of controls, as discussed beginning at paragraph 3.166.

Disclosures About Nonrelevant Criteria

3.72 Description criterion DC8 requires the description to disclose any specific applicable trust services criterion that is not relevant to the system being described and the reasons it is not relevant. One way a trust services criterion may not be relevant is if it does not apply to the system being examined. For example, consider trust services criterion P2.1, which reads as follows: *The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.*) When a user entity is responsible for providing individuals with choice and consent, a service organization that only processes that information does not have any obligations related to choice and consent. In that situation, the service organization would disclose that trust services criterion P2.1 is not relevant and the reason why it is not relevant.

3.73 If a criterion is relevant to the services provided, it is relevant even if all components of the system used to provide the related aspect of the services have been outsourced to a subservice organization. For example, a service organization utilizes an infrastructure-as-a-service cloud provider for all IT systems related to the services provided. The subservice organization is responsible for deleting information from its hosting environment before ending logical and physical access of storage devices. Because the service organization still has a contractual commitment to protect the information of its customers, CC 6.5, *The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives,* is still relevant, even if the subservice organization is carved out. In this situation, users may find it helpful for management to reference the related CSOCs when presenting the service organization's controls. Language such as the following may be used:

> Controls related to this criterion are the responsibility of ABC subservice organization and are described in the CSOCs presented in the description.

Disclosures About Significant Changes to the System During the Period Covered by a Type 2 Examination

3.74 Description criterion DC9 requires that the description disclose the relevant details of significant changes to the service organization's system during the period that are relevant to the service organization's service commitments and system requirements. Relevant changes are those that are likely to be relevant to the system being examined (for example, the service organization's migration to a cloud infrastructure). In that case, disclosure of the changes is likely to be important to report users.

3.75 If the service auditor believes that the changes would be considered significant by the broad range of report users, those changes would generally

be included in the description. The narrative discussing the change would be expected to contain an appropriate level of detail, including the date the change occurred and how the affected aspects of the system differed before and after the change.

3.76 Examples of changes to a system that might be considered significant include the following:

- Changes to the services provided
- Changes to IT and security personnel
- Changes to system processes, IT architecture and applications, and the processes and system used by subservice organizations
- Changes to legal and regulatory requirements that could affect system requirements
- Changes to organizational structure resulting in a change to internal control over the system (for example, a change to the legal entity)
- Implementation of new software and information security controls

3.77 If the service organization has used the inclusive method, changes to be considered may exist at both the service organization and the subservice organization. Paragraph 4.79 presents an example of a separate paragraph that would be added to the service auditor's report when information about such changes is omitted from the description of the service organization's system.

Changes to the System That Occur Between the Periods Covered by a Type 2 Examination

3.78 In some cases, a type 2 report does not cover the period immediately following the period covered by the prior SOC 2 report, which results in a gap between the periods covered by the reports.

3.79 If a significant change occurs during the gap period, service organization management may decide that the change is likely to be considered significant to report users. In that case, management may include a description of the change in the section of the type 2 report titled "Other Information Provided by the Service Organization." An example of such a change is a conversion to a new computer system or application during the gap period that results in (*a*) new or additional controls that are considered significant to report users and (*b*) controls over the conversion process that were not tested by the service auditor.

Controls Remediated After the Period Covered by a Type 2 Examination

3.80 When a SOC 2 report identifies controls that are not operating effectively, management generally takes steps to remediate the control deficiencies. Management may wish to provide customers and business partners with information about the improvements made to their controls before the next SOC 2 report is available. To enhance the trust and confidence that users can place in such information, management may engage the service auditor to perform procedures on such disclosures. The service auditor may be able to do so by performing such procedures as an agreed-upon procedures engagement under AT-C section 215, *Agreed-Upon Procedures Engagement,* or as part of an examination under AT-C section 205.

Evaluating Description Misstatements

3.81 As discussed in paragraph 2.128, the term *description misstatement* is used in this guide to describe differences between the description and the description criteria or omissions in the description. When considering whether a description misstatement exists, the service auditor may consider the following:

- The expectations the service auditor developed related to the nature and extent of disclosures that should be included in the description of the system. Examples include the following:
  - *Expectations may be developed based on the description criteria.* If a service organization uses the services of a subservice organization, and the subservice organization's controls are necessary, alone or in combination with the service organization's controls, for the service organization to achieve its service commitments and system requirements, the service auditor would expect to see a description of the subservice organization's controls when the inclusive method is used. In addition, the service auditor may have developed expectations about the nature and extent of such disclosures based on the significance (that is, the importance or the materiality) of the subservice organization's controls to the achievement of the service organization's service commitments and system requirements.
  - *Expectations may be developed based on laws or regulations.* If a service organization is required by law to comply with the European Union's General Data Protection Regulation (GDPR), the service auditor may expect service organization management to describe compliance with the GDPR as a principal service commitment in the description. Furthermore, the service auditor may have developed certain expectations about the nature and extent of disclosures that should be included in the description about the processes and controls to achieve that commitment. Management's failure to describe a principal service commitment involving compliance with the GDPR and the lack of related disclosures might be considered a misstatement.
- Qualitative factors that may affect the nature and extent of such disclosures. (See paragraph 3.86 for a more detailed discussion on qualitative factors.)

3.82 The following are examples of description misstatements:

- *Inclusion of inappropriate information.* For example, information that is not objectively measurable (such as unsubstantiated advertising claims)
- *Omission of necessary information.* For example, omission of information about relevant subsequent events or changes to controls, relevant service commitments and system requirements, CUECs, or CSOCs

- *Changes without reasonable justification.* For example, revision of service commitments and system requirements during the engagement without reasonable justification or changes from the inclusive method to the carve-out method without reasonable justification
- *Misstatements of fact.* For example, the inclusion of controls that have not been implemented or service commitments and system requirements that are incomplete

3.83 When the service auditor identifies a material description misstatement, the service auditor ordinarily discusses the misstatement with service organization management. In many situations, service organization management would elect to revise the description to correct the misstatement.

3.84 If the description is not revised, the service auditor would need to assess whether the identified description misstatement is material by considering whether there is a substantial likelihood that such misstatements or omissions in the description, individually or in the aggregate, would influence judgments made by users of the SOC 2 report. As an example, assume that a service organization is required by law to comply with the GDPR. When reading the description, however, the service auditor determines that service organization management has not disclosed a principal service commitment related to compliance with the GDPR. The service auditor determines that such information would influence the judgments made by SOC 2 report users; therefore, the service auditor concludes that omission of such information from the description results in a material misstatement. In that case, the service auditor would request that management amend the description by including the relevant information.[5]

3.85 Paragraph .A19 of AT-C section 205 indicates that the service auditor should consider the concept of materiality in the context of qualitative factors (as discussed in the next paragraph) and quantitative factors (for example, when service organization management elects to disclose the percentage of time that its internet-based systems were available during the period). Because the description criteria call for disclosure of primarily nonfinancial information, most descriptions are presented in narrative form. Thus, the service auditor's materiality considerations are mainly qualitative in nature.

3.86 When evaluating the materiality of a description misstatement, the following qualitative factors may be considered:

- The interaction between, and relative importance of, individual disclosures within the description.
- The wording used to make the required disclosures. For example, the wording chosen does not omit or distort the disclosures presented.
- Whether the characteristics of the presentation are appropriate, given that the description criteria allow for variations in presentation.

---

[5] If the description has been prepared to meet the informational needs of a specific subset of such SOC 2 report users (and the report is restricted to those specific users), management considers the possible effect of misstatements (including omissions) that may be relevant to that specific subset of report users.

- The extent to which identified deficiencies in the suitability of design or the operating effectiveness of controls contradict the disclosures about controls included in the description.
- The effect of the misstatement or potential misstatement on the description as a whole.
- The seriousness of the consequences of the misstatement to noncompliance with laws or regulations. As an example, assume a service organization claimed that its controls were effective to meet system requirements that support its compliance with certain laws and regulations over privacy. However, the service auditor's tests indicated that such controls were not effective, and service organization management refused to revise the description. When considering whether the misstatement is material, the service auditor may consider the consequences of the failure to comply with such laws and regulations, which could involve both loss of reputation and monetary fines, when concluding that the description misstatement is material.
- Whether the misstatement was intentional or unintentional.
- Whether the misstatement relates to the relationship between the responsible party and, if different, the engaging party or its relationship with other parties.

3.87 The following are some examples related to materiality with respect to the description of the service organization's system:

- *Example 1.* Example Service Organization uses a subservice organization to perform its back-office functions; management elects to use the carve-out method. The description includes information about the nature of the services provided by the subservice organization and describes the monitoring and other controls performed at the service organization with respect to the processing performed by the subservice organization. However, it does not describe the types of controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization and that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved (CSOCs). Because the service auditor believes that understanding how the subservice organization's processes and controls may affect the achievement of the service organization's service commitment and system requirements is likely to be important to report users, the service auditor concludes that a description misstatement in such information would be material to the description of the service organization's system.
- *Example 2.* A service auditor is reporting on Example Service Organization's security controls. The service organization mirrors data to a data center located in another city and creates tapes of the data as a secondary backup. These tapes are stored at a third location. Data written to the backup tapes is encrypted. The service organization has identified the encryption of the tapes as a control, but it has not identified physical security controls over the tape storage location as a control because management believes

that the likelihood of destruction of both backups simultaneously is remote, and the encryption of the data on the tapes is sufficient. In this example, the omission of controls over physical access is not likely to be relevant to report users because controls over the encryption of the tapes prevent unauthorized access to the information and compensate for the omission of controls over physical access to the facility. Therefore, the omission of that information from the description would not be considered material.

- *Example 3.* A service auditor is reporting on controls related to security, availability, and confidentiality of Example Service Organization, which provides business users with a web-based customer relationship management system. The service auditor identifies certain deficiencies in the design of controls that protect customer data from unauthorized access. Because business users of the system are interested in maintaining the confidentiality of their customer relationships, the service auditor concluded that deficiencies in such controls are likely to be considered significant to such users. Therefore, the omission of such deficiencies from the description would be considered material.
- *Example 4.* Management of Example Service Organization makes certain claims within the description about the service organization's compliance with published privacy practices. Through examination procedures, the service auditor identified the practice of sharing the email addresses of certain user entity customers with a related party for use when marketing the related party's products. Because the violation was both intentional and involved a related-party relationship, the service auditor concludes that the omission of the identified control deficiency is a material misstatement in the description.

3.88 Once description misstatements have been identified, paragraph .46 of AT-C section 205 states that the service auditor should accumulate description misstatements identified during the engagement, other than those that are clearly trivial, to evaluate whether, individually or in the aggregate, those misstatements are material when forming the service auditor's opinion.

3.89 The service auditor would generally also consider the potential effect on the description of identified deficiencies or deviations that relate to the suitability of the design or operating effectiveness of controls. If the service auditor determines that the effects of identified description misstatements, individually or in the aggregate, are material with respect to the description, based on consideration of materiality as discussed beginning in paragraph 3.84, and therefore the subject matter is not in accordance with the criteria, the service auditor should modify the opinion on the description in accordance with paragraph .70 of AT-C section 205. When modifying the opinion, the service auditor's understanding of the nature and cause of the description misstatements and deficiencies enables the service auditor to determine how to appropriately modify the opinion. Chapter 4 discusses modifications of the service auditor's report.

3.90 Paragraph .18 of AT-C section 205 indicates that the service auditor should reconsider materiality if the service auditor becomes aware of information during the engagement that would have caused the service auditor to have initially determined a different materiality.

Obtaining Evidence About the Suitability of the Design of Controls

3.91 Suitably designed controls, if implemented and operating effectively, provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria. Suitably designed controls operate as designed by persons who have the necessary authority and competence to perform the controls. Service organization management is responsible for designing and implementing controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, identifying the risks that threaten the achievement of the service commitments and system requirements, modifying the controls as necessary based on new and evolving risks, and evaluating the linkage between the controls and the evolving risks and threats to the achievement of the service commitments and system requirements.

3.92 In accordance with paragraph .15 of AT-C section 205, the service auditor's understanding of the controls within a system includes an evaluation of the design of controls and whether the controls have been implemented. Evaluating the suitability of the design of controls involves assessing whether the controls stated in the description adequately address the risks that threaten the achievement of the service commitments and system requirements. This assessment is a two-step process:

- Obtaining an understanding of and assessing the service organization's risk assessment process to identify, design, and implement effective controls
- Evaluating whether the controls identified, designed, and implemented by service organization management are suitably designed

3.93 When evaluating service organization management's risk assessment process, the service auditor ordinarily obtains an understanding of the process through performance of the following:

- Considering how service organization management
  - identifies the service organization's service commitments and system requirements;
  - identifies information used by the system to provide the service to user entities and business partners and determines the threats to the security of that information;
  - identifies the threats to the achievement of the service organization's service commitments and system requirements and the vulnerabilities of the system components;
  - assesses the intersection of threats and vulnerabilities (that is, realization of the risks) and evaluates the likelihood and potential magnitude of the realization of the risks and the entity's tolerance for the identified risks;
  - incorporates information from its monitoring activities, including new threats and exploits, system events, and circumstances previously not considered; and

  - identifies whether a subservice organization has identified in its contract or in other communications with the service organization any user entity responsibilities or CUECs that should be in place at the service organization, when the carve-out method is used

- Evaluating evidence about the operating effectiveness of controls caused by a deficiency in the design of the controls
- Evaluating the frequency with which service organization management updates the risk assessment and supporting processes and controls
- Considering whether service organization management uses an appropriate security framework for managing its system processes and controls (for example, the NIST CSF or International Organization for Standardization and International Electrotechnical Commission [ISO/IEC] Standards 27001 and 27002) as part of its assessment and management process
- Considering whether management considers the risk of fraud, such as management override of identified controls, misappropriation of assets by service organization personnel, creation by service organization personnel of false or misleading documents or records, and inappropriate physical and logical access controls to information and the underlying infrastructure through social engineering attacks or similar measures

3.94 Effective risk assessment is critical to the design of controls. Failure to identify a significant threat or a vulnerability to a system component can cause the service organization to overlook a control that is necessary to achieve one or more service commitments and system requirements. In evaluating the service organization's risk assessment process, the service auditor considers the completeness, accuracy, and timeliness of threat identification and the completeness and accuracy of vulnerability identification and management, including, if necessary, regularly monitoring external sources for new vulnerabilities.

3.95 If the inclusive method is used to present the services and controls performed by a subservice organization, the service auditor also makes an assessment with respect to the controls at the subservice organization.

3.96 If the service organization uses a subservice organization, and the controls of the subservice organization are carved out of the description, the service auditor determines whether the subservice organization has identified in its contract or in other communications with the service organization any user entity responsibilities or CUECs that should be implemented by the service organization. If the subservice organization has identified such responsibilities or CUECs, the service auditor would ordinarily evaluate whether service organization management has considered these responsibilities or CUECs in its risk assessment.

3.97 When evaluating whether controls are suitably designed, the service auditor would generally evaluate the controls identified by management in comparison with the risks identified by management as part of it risk assessment process and the service auditor's own engagement risk assessment. The service auditor may also consider the following:

a. The frequency or timing of the occurrence or performance of the control

b. The authority and competence of the individual responsible for performing the control (for example, the level of the individual performing the control, the individual's role in the organization, and conflicting duties)

c. The tasks within the control being performed and the precision and sensitivity of those tasks (for example, the results of reviews and related follow-up activities)

d. Evidence that contradicts the assertion that the control is functioning as designed, such as the rate of system incidents identified related to the control

e. Whether the control, when considered with other controls, addresses each of the risks that threaten the achievement of the service commitments and system requirements based on the trust services criteria to which it relates

f. Whether the applicable control or set of controls, if operated effectively, would protect the information used by the system from system events that could compromise the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria

g. Whether the information used in the operation of the controls is reliable (For example, the operation of a control may rely on configuration parameters of the comparison of the data to another set of data that is expected to be complete and accurate.)

h. Whether the applicable control or set of controls is adequately changing, adapting, and evolving, from a threat-monitoring perspective, as new threats and exploits are identified and become able to be defended against

3.98 Some controls at the service organization may involve sampling (for example, reviewing a sample of data entered into the system as part of a quality assurance review or reviewing a sample of configuration settings for propriety). When evaluating the design of a control that monitors the appropriateness of system operations that uses sampling, the service auditor would need to also consider the service organization's sampling methodology, including the following:

- Whether sampling is an appropriate testing approach. (The considerations are similar to those that the service auditor would take into account when determining whether sampling is an appropriate strategy for testing controls as discussed in paragraph 3.157.)
- Whether management's assumptions, including the expected accuracy rate, are appropriate in the circumstances.
- Whether the control evaluates attributes of the system relative to the achievement of the service organization's service commitments and system requirements.
- Whether the sample size is sufficient to determine the accuracy rate within the population.
- Whether the sample of items is representative of the full population.

- Whether a sufficient process is in place to review results and make corrective actions in a timely manner for errors identified and any instances where results fall below expected accuracy rates. For example, errors may be due to inaccuracies in attributes important to service organization management but not related to the service commitments and system requirements and, therefore, may be evaluated separately.

3.99 The likelihood and magnitude of the realization of a risk will also affect the service auditor's judgment about the suitability of the design of controls and the appropriateness of management's risk assessment. For example, a service organization may permit just a user ID and password when authenticating access to an external informational website. The service auditor may assess the increased risk associated with single-factor authentication in this instance to be low and conclude that the control is suitably designed. However, if single-factor authentication were used for system administration account access, the service auditor would likely conclude that the authentication risk is a control deficiency that results in the failure to mitigate the risks.

3.100 Factors such as the size and complexity of the service organization are also important considerations when evaluating the suitability of the design of controls. A smaller, less complex service organization may be able to address risks that threaten the achievement of its service commitments and system requirements by using a different set of controls than a larger, more complex service organization. For example, a smaller, less complex service organization may

- have controls, including policies and procedures, that are less formal and detailed but sufficient to address the assessed risks;
- have fewer levels of management, which may result in more direct oversight of the operation of key controls; and
- make greater use of manual controls versus automated controls.

3.101 In addition, a small, less complex organization may have different policies and procedures for structuring its board of directors than a larger, more complex organization. Although the latter may have policies and procedures that require the board members be independent from management and to exercise oversight over the development and performance of internal control, a less complex service organization may find it costly and unnecessary to attract independent board members. In those organizations, the responsibility for overseeing the strategic direction of the service organization and the obligations related to the accountability of the service organization may be held by various parties, including the owner of a small business. If the oversight of an owner-manager is adequate to mitigate risks arising from the lack of segregation of duties that often exists in smaller, less complex service organizations, the service organization's policies and procedures may be appropriate to address the assessed risk even without an independent board of directors. On the other hand, if the owner-manager does not have the knowledge or competence to effectively perform the oversight role, the lack of independent oversight by board members may cause a breakdown in internal controls and increase the risk of fraud. In such cases, the lack of policies and procedures requiring independent board members to perform the oversight role may be considered a deficiency in the design of controls.

Additional Considerations for Subservice Organizations

3.102 Identifying and assessing risks and addressing such risks through effective internal control is one of the critical roles of management. When a service organization outsources tasks or functions to a subservice organization, it shifts some of the risks associated with performing those tasks or functions internally to risks associated with outsourcing. Even when a task or function is outsourced, service organization management retains the ultimate responsibility for managing these risks. That is why service organizations need to monitor the services provided by the subservice organization.

3.103 Because service organization management is responsible for monitoring the suitability of design and operating effectiveness of controls at a subservice organization, the description needs to disclose the processes and controls the service organization uses to monitor the services provided by the subservice organization. Controls that a service organization may implement to monitor the services provided and controls performed by a subservice organization are discussed further beginning at paragraph 3.67. In addition, considerations when evaluating the suitability of design and the operating effectiveness of controls used to monitor the controls at the subservice organization are discussed beginning at paragraph 3.168.

3.104 As part of its monitoring activities, service organization management may obtain a copy of a type 1 or type 2 report from the subservice organization if one is available. If the subservice organization's type 1 or type 2 report identifies the need for CUECs at the service organization, the description should describe the processes and controls the service organization has implemented to address the CUECs identified in the subservice organization's description of its system. In addition to describing the services provided by the subservice organization, management may indicate in its description whether the subservice organization's report is a type 1 or type 2 report.

3.105 As an example, assume that a service organization outsources aspects of its technology infrastructure to a subservice organization. The subservice organization's description includes the following CUEC:

> User entities should have controls in place to restrict access to system resources to appropriate user entity personnel.

3.106 To address the CUEC included in the subservice organization's description, service organization management would include controls such as the following in its description of the service organization's system:

- Access control software and rule sets are used to restrict logical access to information assets, including hardware, data (at rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components.
- Persons, infrastructure, and software are identified and authenticated prior to accessing information assets, whether locally or remotely.
- Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.

- Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.

Multiple Controls Are Necessary to Address All Aspects of an Applicable Trust Services Criterion

3.107 The service organization may have multiple controls in place to address the risks that threaten the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria. In this case, the service auditor may need to consider the suitability of each of those controls when determining whether controls have been suitably designed to address each of the risks associated with a particular criterion.[6] For example, trust services criterion A1.2, *The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives*, addresses, among other things, the risk that a server will not be able to support system availability in the event of a distributed denial-of-service attack. The service organization can address one aspect of this risk (and thus one element of that criterion) by designing and implementing a control that provides redundant load-balanced infrastructure protected by mechanisms for detecting and dropping access attempts. In this situation, when evaluating suitability of design, the service auditor would also have to consider other controls the service organization has designed and implemented to achieve the other aspects of that criterion.

3.108 The service auditor may conclude that there are no controls in place to support one or more aspects of an applicable trust services criterion. For example, for the trust services criterion PI1.2, *The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives*, user entities may submit transaction processing requests by telephone or electronically. Although the service organization has identified in its description controls that address the processing of electronic transaction requests received from user entities, it has not identified controls that address transaction requests received via telephone. In this situation, the service auditor would generally conclude that controls were not suitably designed to process transaction requests received via telephone.

Multiple Controls to Address a Particular Assessed Risk

3.109 The service organization may have designed and implemented multiple (redundant) controls to address a particular risk that threatens the achievement of its service commitments and system requirements. If the service auditor evaluated the suitability of design of one control and determined that it was ineffective, the service auditor may consider whether one or more of the other controls was suitably designed to address the risk. That control may then be tested to obtain evidence about operating effectiveness. In addition, the service auditor would ordinarily ask management to revise the description to

---

[6] TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, presents the 2017 trust services criteria. The trust services criteria are used by service organization management and by the service auditor when evaluating whether the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

exclude the control that is not suitably designed and include the control or controls that are suitably designed based on the applicable trust services criterion.

Procedures to Obtain Evidence About the Suitability of Design of Controls

3.110 The service auditor evaluates the suitability of the design of controls by using evidence and other information gathered when

- obtaining an understanding of the service organization's system and the controls within that program and
- determining whether the description of the system presents the system that was designed and implemented in accordance with the description criteria (including evidence obtained from performing walk-throughs).

3.111 To supplement such evidence and other information, the service auditor generally performs a combination of the following procedures:

- Inquiry of service organization personnel about the design and operation of applicable controls and the types of system events that have occurred or that may occur
- Inspection of documents produced by the service organization
- Performing additional walk-throughs of control-activity-related policies and procedures
- Reading applicable and supporting system documentation
- Determining whether attacks and vulnerability exploitations, including those identified publicly by organizations such as the United States Computer Emergency Readiness Team, and emerging risks and threats have been adequately addressed

3.112 As discussed beginning in paragraph 2.63, service organization management may document controls in a variety of ways. The nature and extent of documentation usually varies, depending on the size and complexity of the service organization and its monitoring activities. In some cases, the service auditor may be able to obtain and inspect management's documentation of controls, including its identification of risks and evaluation of the linkage of controls to those risks. In that case, the service auditor may use the documentation as a starting point when evaluating the completeness, accuracy, relevance, and timeliness of management's risk assessment process and the suitability of design of the controls implemented to mitigate those risks.

Additional Considerations When the Carve-Out Method Is Used for a Subservice Organization

3.113 If the service organization uses the carve-out method for a subservice organization, the service auditor would also need to evaluate whether the types of controls expected to be implemented at the subservice organization would, if operating effectively in combination with the controls at the service organization, provide reasonable assurance that the service organization's service commitments and system requirements were achieved. The service auditor would also need to consider whether evidence exists that the service organization has communicated to the subservice organization the service organization's requirements with respect to the types of controls that are expected to be implemented and whether there is any evidence that deficiencies exist in

either the suitability of the design or, in a type 2 examination, the operating effectiveness of controls at the subservice organization.

3.114 Examples of procedures that may be performed to obtain such evidence include the following:

- Reading contracts and other communications with the subservice organization to determine whether they identify the types of controls expected to be implemented at the subservice organization
- Obtaining an understanding of the procedures in place at the service organization to evaluate and monitor the implementation, suitability of design, and in a type 2 examination, the operating effectiveness of the controls at the subservice organization (for example, evaluation of a service auditor's SOC 2 report on the subservice organization's system or testing performed at the subservice organization by service organization personnel)
- Obtaining and evaluating a SOC 2 report on the subservice organization's system. For example, if the service organization is responsible for developing, testing, and approving program changes but has outsourced the actual implementation of the changes to the subservice organization, the service auditor would conclude that controls at the subservice organization are necessary based on trust services criterion CC8.1, *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.*

Evaluating Deficiencies in the Suitability of Design of Controls

3.115 A deficiency in the design of a control occurs when a risk that threatens the achievement of one or more of the service organization's service commitments and system requirements is not sufficiently mitigated by one or more properly designed controls. In contrast, a deficiency in the operation of a control exists when a properly designed control does not operate as designed. A service organization may be able to correct a deficiency in the operation of a control, for example, by providing additional training to the employee who performs the control. However, if the design of the control is deficient, the control will not operate effectively regardless of who performs it. For that reason, the service auditor often would not test the operating effectiveness of a control that is not suitably designed. Instead, the service auditor generally would evaluate the design of other controls, if any, that address the same risks.

3.116 In some situations, two or more controls are suitably designed only when operating in conjunction with each other. In these situations, the service auditor evaluates the suitability of design and operating effectiveness of the controls together in order to reach a conclusion.

3.117 When identifying such deficiencies, the service auditor considers whether the controls have the ability, as designed, to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria if they operate effectively. The service auditor may also consider the potential effect of other factors that may affect the opinion on the suitability of the design of controls, such as description misstatements or deficiencies in the operating effectiveness of controls. Generally, if controls are not suitably designed and

implemented to provide reasonable assurance that one or more service commitments or system requirements were achieved based on the applicable trust services criteria, such deficiencies are considered material. Materiality considerations when evaluating the suitability of design of controls are discussed beginning in paragraph 3.187.

3.118 Once deficiencies in the design of controls have been identified, the service auditor should, in accordance with paragraph .46 of AT-C section 205, accumulate deficiencies identified during the engagement, other than those that are clearly trivial, to evaluate whether, individually or in the aggregate, those deficiencies are material when forming the service auditor's opinion.

3.119 Paragraphs 4.87–.89 present examples of separate paragraphs that would be added to the service auditor's report when the service auditor determines that controls are not suitably designed to provide reasonable assurance that one or more of the service organization's service commitments or system requirements were achieved based on the applicable trust services criteria.

Obtaining Evidence About the Operating Effectiveness of Controls in a Type 2 Examination

3.120 Suitably designed controls operate as designed by persons who have the necessary authority and competence to perform the controls. Controls that operate effectively provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria.

3.121 In a type 2 examination, the service auditor tests the operating effectiveness of the controls stated in the description. The service auditor performs procedures (commonly referred to as tests of controls) to obtain evidence about the operating effectiveness of controls. Evidence from tests of controls usually relates to how the controls were applied, the consistency with which they were applied, and by whom or in what manner they were applied. When a service organization uses the inclusive method to present the services and controls of a subservice organization, the service auditor also applies tests of controls to the controls at the subservice organization.

3.122 If the service auditor has identified design deficiencies, the service auditor generally would not test the operating effectiveness of those controls. However, in certain circumstances, report users may expect management to identify the control in the description and may expect the service auditor to perform tests of the control. In such situations, the service auditor may choose to perform such testing and include the results of the testing in the report.

Designing and Performing Tests of Controls

3.123 In accordance with paragraph .25 of AT-C section 205, the service auditor should design and perform tests of controls to obtain sufficient appropriate audit evidence about the effectiveness of controls stated in the description. By including those controls in the description, service organization management has identified them as part of the system the service organization has designed, implemented, and operated to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

3.124 The service auditor is responsible for determining the nature (how the controls are tested), timing (when the controls are tested and the frequency of the testing), and extent (the number of procedures performed or the size of the sample) of procedures necessary to obtain sufficient appropriate evidence about the operating effectiveness of controls throughout the period addressed by the examination.

3.125 The service organization's control environment, risk assessment, information and communications, and monitoring components may also affect the system used to provide services to user entities and business partners. Controls within each of those components may enhance the effectiveness of specific controls or mitigate deficiencies in other controls. When not operating effectively, controls within each of those components may also have a detrimental effect on the operation of other controls. If the service auditor determines that certain controls with the control environment or other components are not effective, the service auditor would generally design and perform further procedures whose nature, timing, and extent are based on, and responsive to, the assessed risks of material misstatement resulting from those controls that are not operating effectively. In some situations, the service auditor may conclude that controls are not operating effectively because of deficiencies in controls related to one or more of the components of internal control.

3.126 As the risk addressed by a control being tested increases, the sufficiency and appropriateness of evidence that the service auditor needs to support an opinion on control effectiveness also increases. Factors the service auditor may consider when determining nature, timing, and extent of tests of controls include the following:

- The nature and materiality of misstatements that the control is intended to prevent, or detect and correct
- Whether the control has a history of operating deficiencies
- The effectiveness of monitoring activities over that and other controls
- The nature of the control and the frequency with which it operates
- The degree to which other controls are dependent on the effectiveness of the control
- The competence of the personnel who perform the control or monitor its performance and whether there have been changes in key personnel who perform the control or monitor its performance
- Whether the control is manual (that is, relies on performance by an individual) or automated
- The complexity of the control and the significance of the judgments that would be made in connection with its operation

3.127 Generally, a conclusion that a control is not operating effectively can be supported by less evidence than is necessary to support a conclusion that a control is operating effectively.

Nature of Tests of Controls

3.128 The nature and objectives of tests to evaluate the operating effectiveness of controls are different from those performed to evaluate the suitability of the design of controls. When designing and performing tests of controls,

the service auditor would generally perform one or more of the following procedures:

a. Inquire of service organization personnel, perform inspection (for example, of documents, reports, or electronic files) and other procedures, observe the application of the control, or reperform the control to obtain evidence about the following:

i. How the control was executed (Was the control performed as designed?)

ii. The consistency with which the control was applied throughout the period

iii. By whom or by what means the control was applied (Is the control automated or manual? Has there been high turnover of the personnel in the position that performs the control, and is the control being performed by an inexperienced person?)

b. Determine whether the controls to be tested depend on the operating effectiveness of other controls and, if so, whether it is necessary to obtain evidence supporting the operating effectiveness of those controls.

c. Evaluate whether the information produced by the service organization is reliable when such information is integral to the performance of the control (as discussed beginning at paragraph 3.138).

d. Determine an effective method for selecting the items to be tested to meet the objectives of the tests of controls.

3.129 Inquiry alone does not provide sufficient appropriate evidence of the operating effectiveness of controls. Performing inquiry combined with inspection or reperformance ordinarily provides more convincing evidence than performing inquiry and observation. For example, a service auditor may inquire about and observe a service organization's physical building security during the initial walk-throughs. Because an observation is pertinent only at the point in time at which it is made, the service auditor would generally supplement the observation with other procedures to obtain sufficient appropriate evidence regarding the operating effectiveness of the physical security control throughout the period. For example, the service auditor may inspect the video tapes that monitor the entrance of the facility and select a sample of individuals who entered the building to determine whether their names were included on the list of authorized individuals during that period.

3.130 Because of the methods used to store and transmit data within the system, the service auditor may find the use of analytics to be a highly effective technique when performing tests of controls. The following procedures illustrate ways in which analytics may be used when evaluating the suitability of design and operating effectiveness of controls:

- Documentation of authorization of service organization management approvals may be stored in an online workflow system, permitting the records from the system to be extracted and analyzed.
- System logs may be scanned for unusual activity that may be indicative of failure in the design or operating effectiveness of controls.

- Server security configuration parameters may be scanned and analyzed for consistency with policy.
- Access control lists can be analyzed for appropriateness of access rules.

When using analytics, the service auditor would need to perform procedures to validate the completeness and accuracy of the information received from the entity, as discussed beginning in paragraph 3.138.

3.131 The type of control being tested may affect the nature, timing, and extent of the testing performed by the service auditor. Some controls provide more persuasive evidence of their operating effectiveness than others. For example, some controls may leave a document trail when they operate. The service auditor may inspect such documentation to obtain evidence about the operating effectiveness of those controls. Other controls, however, may not leave documented evidence of their operation; for those controls, the service auditor may need to plan to test those controls when they operate.

3.132 If control documentation has been lost, misplaced, or inadvertently deleted by the service organization, the service auditor may have to evaluate the types of evidence available and whether the operating effectiveness of the control can be tested through other procedures, such as observation, that would provide evidence of operating effectiveness throughout the period. However, depending on the controls being tested and their significance to the achievement of the service organization's service commitments and system requirements, observation alone may not provide sufficient appropriate evidence of operating effectiveness. If the service auditor is unable to obtain sufficient appropriate evidence in support of the operating effectiveness of such controls, the opinion on operating effectiveness should be modified (for a scope limitation) in accordance with paragraph .70 of AT-C section 205 if the possible effect of the matter is or may be material. In some circumstances, when determining whether a qualified opinion or disclaimer of opinion would be appropriate, the service auditor may consider qualitative factors such as whether the absence of sufficient appropriate evidence was a result of the failure of a control to operate effectively or the inadvertent destruction of evidence (for example, the destruction of the computer hard disk on which the evidence was stored).

3.133 In addition to performing procedures to directly test the operating effectiveness of a control, the service auditor may also perform procedures to indirectly obtain evidence about whether a control operated to prevent or detect errors and fraud. For example, when testing the operating effectiveness of vulnerability scanning controls, the service auditor may use the service auditor's firm's own vulnerability scanning tools to detect unidentified vulnerabilities in the service organization's system. By comparing the results of the service auditor's independent vulnerability scan to the results of the service organization's vulnerability scan, the service auditor obtains evidence about the effectiveness of such controls. As another example, the service auditor might obtain from management a listing of system incidents identified throughout the period and compare the vulnerabilities exploited to the controls implemented by the service organization. Identifying deficiencies in the design or operation of the controls implemented to address exploited vulnerabilities can assist the service auditor with the evaluation of the suitability of design and operating effectiveness of such controls.

3.134 If there have been significant changes made to the service organization's system during the examination period, and the superseded controls are relevant to the achievement of one or more service commitments or system requirements, the service auditor should, in accordance with paragraph .20 of AT-C section 205, obtain sufficient appropriate evidence regarding the suitability of design and operating effectiveness of both the superseded controls and the new controls to draw conclusions regarding the suitability of design and operating effectiveness of controls. In accordance with paragraph .48 of AT-C section 205, if the service auditor is unable to obtain sufficient appropriate evidence to conclude that the controls operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved throughout the period, the service auditor should apply the requirements of paragraphs .70–.86 of AT-C section 205 to determine the appropriate opinion to be issued or withdraw from the engagement.

Testing Review Controls

3.135 When designing tests of controls to evaluate the design of review controls, the service auditor needs to understand the following matters:

- How the control was performed, including the specific steps involved in executing the review
- What the control owner considered when performing the review
- The criteria or thresholds used to trigger further investigation or other follow-up actions
- The steps involved in investigating and resolving matters identified by the reviewer

3.136 When testing the effectiveness of review controls, the service auditor also needs to consider the precision with which the control needed to be performed to determine whether the control operated the same way each time. The service auditor may need to determine whether the evidence gathered through the tests performed demonstrates that the review control consistently identified appropriate items for follow-up and that matters identified for investigation were resolved in a timely manner. Without documented instances of the review control identifying appropriate items for follow-up, the service auditor may not have sufficient appropriate evidence that the review control operated as designed throughout the examination period. The service auditor may find it necessary to test review controls through reperformance of the control in addition to inspection of the control.

Evaluating the Reliability of Information Produced by the Service Organization or Management's Specialists

3.137 From the service auditor's perspective, there are three types of information produced by a service organization:

- Information provided to the service auditor in response to ad hoc requests from the service auditor (for example, a request for a population list, such as a population of application changes that the service auditor uses to select a sample of items for testing)
- Information used in the execution of a control (for example, a user access list used by service organization personnel in an access review control or a list of controls that did not operate during the examination period)

- Information prepared for user entities (for example, a report listing user entity employee access)

3.138 When using information produced by the service organization, in accordance with paragraph .36 of AT-C section 205, the service auditor should evaluate whether the information is sufficiently reliable for the service auditor's purposes, including, as necessary, the following:

a. Obtaining evidence about the accuracy and completeness of the information

b. Evaluating whether the information is sufficiently precise and detailed for the service auditor's purposes

3.139 A service organization may prepare information to be used in the execution of a control only once or on a recurring basis. The information may be created manually or generated from a system. Information may also be made available to users through a data warehouse, which permits user entities to generate their own reports. Each of these factors may affect the procedures the service auditor performs to evaluate the reliability of information to be used in the examination.

3.140 In most cases, the service auditor identifies the information produced by the service organization while performing procedures to obtain the understanding of the service organization's system and controls within the system as discussed beginning at paragraph 3.93. Questions a service auditor may ask about information produced by the service organization include the following:

- How is the information produced or generated? (For example, the service organization's applications or systems, other service organization sources such as manually produced reports, or vendors outside the service organization)
- What procedures were performed to determine whether information produced or generated by applications or tools developed by third parties is accurate and complete?
- How is the information used?
- What effect could the information have on user entities?
- Is the information located in a controlled IT environment or an ad hoc reporting database or data warehouse?
- Is the information highly structured and complex or relatively straightforward?
- Does the information originate from a system already subject to the service auditor's procedures or from a system beyond the scope of the service auditor's examination?
- What is the basis for the service organization's comfort with the reliability of the information?
- Were any classes or ranges of data excluded from the information provided by the service organization? If so, were those exclusions appropriate?

3.141 In addition to these matters, the service auditor would ordinarily assess the impact such information could have on the examination. The results of the service auditor's tests will not be reliable if the population from which the items have been selected for testing is incomplete or inaccurate. For example,

the results of tests over the effectiveness of a review of user access controls may be affected by the completeness and accuracy of the information used to prepare the user access reports. In this case, the service auditor may decide to inspect the scripts used to create the user access reports for accuracy of logic before performing the procedures.

3.142 Depending on the means by which the service auditor obtains the information, the service auditor develops a plan to assess the completeness and accuracy of such information. The following factors may be relevant when assessing the information used in the execution of controls:

- The importance of the control in mitigating risks that threaten the achievement of the service organization's service commitments and system requirements
- The risk that one or more service commitments or system requirements would not be achieved if the information produced by the service organization is not reliable
- The degree to which the effectiveness of the control depends on the completeness and accuracy of the information
- The degree to which the control depends on other controls
- The precision with which the control is performed (for example, precision of review controls)

3.143 Determining the nature and extent of evidence needed to assess the reliability of information produced by the service organization is a matter of professional judgment. The service auditor may obtain evidence about the reliability of such information when testing controls or may develop and perform specific procedures that address this information. For example, when information is produced by a software application or tool, the service auditor may consider obtaining either a SOC 2 report on processing integrity for that application or tool or a SOC for Supply Chain report on the processing integrity of the process used in developing the application or tool. Paragraph .23 of AT-C section 205 notes that the more important the information or the control, the more persuasive the evidence about the reliability of the information should be. Because a type 2 report covers a period of time, the reliability of the information produced by the service organization needs to be evaluated throughout the examination period.

3.144 Generally, testing only the IT general controls supporting the system is not a sufficient procedure to evaluate the reliability of information produced by the service organization. The following are examples of additional procedures the service auditor may perform when evaluating the reliability of various types of information produced by the service organization:

Example 1: Information provided by the service organization to the service auditor in response to an ad hoc request from the service auditor

The service organization provides the service auditor with a system-generated list of new accounts set up during the period. In evaluating the accuracy and completeness of the list of new accounts set up during the period, the service auditor may do the following:

a. Observe the generation of the list of new accounts set up during the period, confirm that the correct source was queried and that the date range and type of account parameters were accurately entered, and determine whether any exclusions are listed.

b. Inspect the list for any new accounts with a "created on" date that is outside the date range specified.

c. Test the IT general controls supporting the system.

Example 2: Information used in the execution of a control

The description of the service organization's system states that a list of terminated employees is automatically produced by the human resources management system (HRMS) application on a weekly basis and that access to supporting business applications by terminated employees is removed on the date of termination. In evaluating the accuracy and completeness of the termination report, the service auditor may do the following:

a. Observe the human resources manager enter the date range and termination parameter into the reporting tool within the production environment of the HRMS application.

b. Inspect the report for any termination dates outside the date range specified.

c. Test the IT general controls supporting the HRMS.

Example 3: Population of incidents

The incident management recordkeeping application generates a report of all incidents during a period. Before testing a sample of such incidents, the service auditor may inspect the query logic used to generate the report and perform a walk-through of the process used to record incidents in the application. The service auditor may also inspect the report for anomalous gaps in sequence or timing to determine completeness.

Example 4: Population of changes

The change management system is used to communicate changes ready for implementation. Before testing a sample of changes to application software, the service auditor may perform a walk-through of the process used to communicate changes ready for implementation in order to understand whether any alternate paths of communication exist. The service auditor would also assess the completeness of the population as well as the segregation of duties between those responsible for the development and testing of the changes and those responsible for migration of changes to the production environment. The service auditor would also consider the enforcement of the segregation of duties through logical access controls.

Example 5: Population of servers

All servers accessed by the system are included in vulnerability scans. Before testing the results of a sample of vulnerability scans, the service auditor would ascertain the process for performing the vulnerability scans (for example, subnet scanning, manually adding server names) and the configurations used to include the service organization's system. The service auditor would need to understand and consider how the server build-out process is conducted and how servers are migrated to the relevant environments to be included in the scanning.

3.145 As discussed beginning in paragraph 2.11, there may be situations in which management engages a management's specialist to leverage knowledge, technologies, experience, and expertise not resident within the service

organization. In some situations, service organization management engages a management's specialist to provide information about the operation of controls that will assist management in enhancing the effectiveness of the service organization's controls. In this situation, in addition to performing the procedures described in paragraph 3.144, the service auditor may also perform the following procedures to determine if such information is sufficiently reliable for the service auditor's purposes:

- Evaluating the competence, capabilities, and objectivity of the specialist
- Obtaining an understanding of the work of the specialist
- Evaluating the appropriateness of that specialist's work as evidence regarding the operation of the service organization's controls

Timing of Tests of Controls

3.146 The following factors may be relevant to the service auditor's determination of the timing of tests of controls:

- The period of time during which the information will be available. For example,
  - — electronic files may be overwritten after a period of time,
  - — procedures may occur only at certain times during the period, and
  - — certain procedures may need to be performed after the end of the period, such as reviewing reconciliations that are generated after the end of the period
- Whether the control leaves evidence of its operation and, if not, whether the control can be tested through observation of the performance of the control.
- The significance of the control being tested to the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria.

3.147 The service auditor may perform tests of controls at interim dates, at the end of the examination period, or after the examination period if the tests relate to controls that were in operation during the period but do not leave evidence until after the end of the period. Performing procedures at an interim date may assist the service auditor in identifying, at an early stage of the examination, any potential deficiencies in the design or the operating effectiveness of controls and, consequently, provide an opportunity for the service organization to resolve identified deficiencies prior to the end of the examination period, regardless of the service auditor's determination about whether they affect the service auditor's report. When the service auditor performs tests of the operating effectiveness of controls during an interim period, the service auditor should, in accordance with paragraph .47 of AT-C section 205, evaluate whether sufficient appropriate evidence has been obtained regarding the operating effectiveness of the controls throughout the period, and if necessary, obtain further evidence. Such further evidence may be obtained by performing inquiries, inspecting the results of monitoring activities, and performing additional testing for the remaining period.

3.148 Paragraph 4.87 contains an illustrative paragraph that would be added to the service auditor's report if controls were not suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on an applicable trust services criterion for a portion of the period under examination.

Extent of Tests of Controls

3.149 The *extent* of the service auditor's testing refers to the size of the sample tested or the number of observations of a control activity. The extent of testing is based on the service auditor's professional judgment after considering factors such as the following:

- The tolerable rate of deviation
- The expected rate of deviation
- The frequency with which the control operates
- The relevance and reliability of the evidence that can be obtained to support the conclusion that the controls are operating effectively
- The length of the testing period
- The significance of the control to the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria
- The extent to which audit evidence is obtained from tests of other controls that support the achievement of those service commitments and system requirements based on the applicable trust services criteria.

3.150 The service auditor expresses an opinion on the operating effectiveness of controls throughout the period covered by the examination; consequently, in accordance with paragraph .47 of AT-C section 205, the sufficiency of the evidence regarding the effectiveness of controls should support that opinion. For example, if a control operates daily, the service auditor would test the operation of the control for a sufficient number of days throughout the period covered by the examination to determine whether the control operated effectively throughout the entire period. The shorter the period over which the control is performed, the less likely the service auditor will be able to obtain sufficient appropriate evidence to express an opinion on the effectiveness of controls. For example, if a control operates only once annually, and that date is outside of the examination period, the service auditor would be unable to test the operating effectiveness of the control within the period.

3.151 Evidence about the satisfactory operation of controls in prior periods does not provide evidence of the operating effectiveness of controls during the current period. The service auditor expresses an opinion on the effectiveness of controls throughout each period; therefore, sufficient appropriate evidence about the operating effectiveness of controls throughout the current period is required for the service auditor to express an opinion for the current period.

3.152 The service auditor's knowledge of modifications to the service auditor's report or deviations observed in prior engagements may, however, be considered when assessing risk. Such knowledge may lead the service auditor to increase the extent of testing in the current period. For example, if the opinion in the prior year's report was qualified because of deviations in controls over

the authorization of user access, the service auditor may decide to increase the number of items tested in the current examination to determine whether the deficiency was effectively corrected.

3.153 Generally, IT processing is inherently consistent; therefore, the service auditor may be able to limit the testing to one or a few instances of a control's operation. An automated control usually functions consistently unless the program, including the tables, files, or other permanent data used by the program, is changed. Once the service auditor determines that an automated control is functioning as intended, which could be determined at the time the control is initially implemented or at some other date, the service auditor would generally perform tests to determine that the control continues to function effectively. Such tests ordinarily would include determining that changes to the program are not made without being subject to the appropriate program-change controls, that the authorized version of the program is used for processing transactions, and that other relevant IT general controls are effective. In instances in which the automated control is configurable, the service auditor would consider the effect of the configurable parameters on the operation of the control and, if necessary, perform procedures to obtain evidence regarding the operation of the control given the effect of the parameters. Such procedures may include obtaining an understanding of the configuration process, performing procedures to test the completeness and accuracy of the configuration parameters, and evaluating the controls over access to alter the configuration. If the control is tested in an environment other than the production environment, the service auditor may need to assess the risk that the operation of the control in the production environment differs from that in the nonproduction environment and perform procedures to determine that the environment being tested matches that of the production environment.

3.154 If effective IT general controls are present, automated application controls may be tested only once or a few times. In such situations, the service auditor considers whether changes to the control made after the testing, but prior to the end of the examination period, would change the service auditor's conclusion regarding the suitability of design or operating effectiveness of the control and performs additional testing as deemed necessary.

Testing Superseded Controls

3.155 As discussed in paragraph 3.134, If the service organization makes changes to controls during the period and the superseded controls are relevant to the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria, the service auditor should obtain sufficient appropriate evidence regarding the suitability of design and operating effectiveness of the controls before the change. For example, during the period June 1, 20X0, to May 31, 20X1, Example Service Organization decided to automate a control that was previously performed manually. The service organization automated the control on December 15, 20X0. The service auditor tests the manual control for the period from June 1, 20X0, to December 14, 20X0, considering the nature of the control and the frequency of its operation, and then tests the automated control for the period from December 15, 20X0, to May 31, 20X1, considering the nature of the control and the frequency of its operation.

3.156 If (*a*) the service auditor is unable to test the superseded control (for example, because the control does not leave evidence of its operation after

a period of time or because the service auditor was engaged after the control was superseded) and (*b*) the control is relevant to the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria, the service auditor should disclose that fact in the description of tests and results. The service auditor should also determine the effect on the service auditor's report in accordance with paragraph .60 of AT-C section 205. If the circumstances result in a scope limitation, the service auditor should modify the service auditor's opinion in accordance with paragraph .48 of AT-C section 205. (See the relevant paragraphs within paragraphs .70–.86 of AT-C section 205 for reporting requirements when the service auditor is unable to obtain sufficient appropriate evidence.) Paragraph 4.89 of this guide presents an example of a separate paragraph that would be added to the service auditor's report when a scope limitation related to the operating effectiveness of controls exists.

Using Sampling to Select Items to Be Tested

3.157 The service auditor may consider whether to use audit sampling to select items for testing the operating effectiveness of controls. When determining the extent of tests of controls and whether sampling is appropriate, consideration is given to (*a*) the characteristics of the population of the controls to be tested, including the nature of the controls; (*b*) whether the population is made up of homogenous items; (*c*) the frequency of the controls' application; and (*d*) the expected deviation rate. AICPA Audit Guide *Audit Sampling* may be useful to the service auditor when performing sampling.

3.158 Before deciding to use sampling in a SOC 2 engagement, the service auditor should consider whether sampling is responsive to the assessed risk of material misstatement in accordance with paragraph .22 of AT-C section 205. This consideration may include whether

a. due to the design of one or more systems, it may not be possible to give every item in the population a chance of being selected for the sample.

b. the service auditor may determine that testing every instance of a control's operation using data analytics would be more effective because even a one-time failure of the control could result in a material deficiency in the operating effectiveness of controls.

c. the service auditor may conclude that it is more efficient and effective to test 100% of the population of data evidencing the effective operation of the control than selecting and testing a sample.

3.159 In such circumstances, sampling may not be an effective approach to obtaining sufficient appropriate evidence to evaluate the effectiveness of the control. Consequently, in applying professional judgment regarding the extent of testing, the service auditor needs to consider whether the assumptions for sample-based testing have been met.

Selecting Items to Be Tested

3.160 For tests of controls using sampling, the service auditor determines the tolerable rate of deviation and uses that rate to determine the number of items to be selected for a particular sample.

3.161 In accordance with paragraph .32 of AT-C section 205, the service auditor's selection of sample items should be reasonably expected to be representative of the population covering the reporting period. Random selection of items represents one means of obtaining such samples.

Additional Considerations Related to Risks of Vendors and Business Partners

3.162 Business partners, vendors, and other third parties with access to the service organization's system may access confidential information through the system or transmit information between themselves and the system. For example, a service organization may obtain data used in calculations via an automated transmission of data initiated by the vendor accessing the service organization's system. The vendor's access results in vulnerabilities that could be exploited by others and risks that could threaten the achievement of one or more of the service organization's service commitments and system requirements.

3.163 In response, service organization management needs to understand the nature of those risks and assess the likelihood and magnitude of such risks.

3.164 Processes and controls the service organization may perform to address the risks associated with interactions with a vendor or business partner are outlined in trust services criterion CC9.2 and include all or a combination of the following:

- Establishing specific requirements for vendor and business partner arrangements that include scope of services and product specifications, roles and responsibilities, compliance requirements, and service levels.
- Identifying any vulnerabilities arising from vendor and business partner relationships, including third-party access to the entity's IT systems and connections with third-party networks.
- Inventorying, tiering, and assessing, on a periodic basis, threats arising from relationships with vendors and business partners (and those entities' vendors and business partners) and the vulnerability of the entity's objectives to those threats. Examples of risks may include
  - financial failure,
  - security vulnerabilities,
  - operational disruption, or
  - failure to meet business or regulatory requirements.
- Assigning responsibility and accountability for the management of risks and changes to services associated with vendors and business partners.
- Establishing communication and resolution protocols for service or product issues related to vendors and business partners.
- Establishing exception handling procedures for service or product issues related to vendors and business partners.

- Assessing the performance of vendors and business partners as frequently as warranted based on the risk associated with the vendors or business partners.
- Implementing procedures for addressing issues identified with vendor and business partner relationships.
- Implementing procedures for terminating vendor and business partner relationships based on predefined considerations. Those procedures may include safe return of data and its removal from the vendor or business partner system.

3.165 During the examination, the service auditor would also need to perform procedures to evaluate whether monitoring controls over vendors and business partners were suitably designed and, in a type 2 examination, operated effectively. Paragraph 2.61 discusses monitoring controls that may be implemented by the service organization.

Additional Considerations Related to CSOCs

3.166 When the service organization uses the carve-out method for the services and controls of a subservice organization, the service auditor evaluates whether the types of controls stated in the description and expected to be implemented at the subservice organization are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria (that is, whether the controls are CSOCs). For example, if the service organization is responsible for developing, testing, and approving program changes but has outsourced the actual implementation of the changes to a carved-out subservice organization, controls at the subservice organization would be necessary to achieve the service organization's service commitments and system requirements based on trust services criterion CC8.1, *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.* If there are CSOCs, consideration would be given to whether the CSOCs and the service organization's controls are suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, if such controls were operating effectively.

3.167 The service auditor may consider performing procedures to obtain evidence about (*a*) whether the service organization has communicated to the subservice organization the service organization's requirements with regard to the CSOCs and (*b*) whether there is any evidence of deficiencies in the suitability of the design or operating effectiveness of controls at the subservice organization. Note, however, that the service auditor has no responsibility to communicate, in the service auditor's report, any deficiencies identified in the SOC 2 report of a carved-out subservice organization.

3.168 Although a subservice organization may perform certain functions for a service organization, management of the service organization remains responsible to its user entities for performing the services it has agreed to provide, including the outsourced functions. As a result, management is responsible for performing monitoring activities over the subservice organization, and management would include in the description controls used to monitor the

effectiveness of controls at the subservice organization. Examples of such monitoring activities are described in paragraph 2.61.

SOC 2 Report From Carved-Out Subservice Organization Is Obtained

3.169 As discussed in paragraph 2.61, one way service organization management can monitor the controls of the subservice organization is by obtaining a SOC 2 report. When management has obtained such a report, management's monitoring procedures should adequately address any description misstatements or deviations identified in the subservice organization's type 2 report. For example, if the service organization has obtained a type 2 report from the subservice organization, such monitoring procedures should include a review of the report to assess (*a*) the relevance of the system description and CSOCs to the service organization's system, (*b*) any deviations requiring further evaluation and response by service organization management, and (*c*) the period of coverage of the subservice organization's type 2 report relative to the period covered by the current examination.

3.170 In the preceding example, a description misstatement or deviation identified in the subservice organization's SOC 2 report may lead service organization management to augment its system description or implement additional controls to compensate for the misstatements or deviations noted in the report. Alternatively, management's evaluation of the subservice organization's SOC 2 report could result in a conclusion that the identified deviations or exceptions in the subservice organization's SOC 2 report do not affect the service organization's description or the suitability of design or operating effectiveness of controls to achieve the relevant service commitments and system requirements.

3.171 In evaluating the suitability of design and operating effectiveness of controls based on trust services criterion CC9.2, *The entity assesses and manages risks associated with vendors and business partners*, management's monitoring of the subservice organization is likely to be relevant, regardless of whether the inclusive method or the carve-out method is used. When determining the nature, timing, and extent of testing to perform, the service auditor may consider the results of the service organization's monitoring of subservice organizations. This may be particularly important when the subservice organization's SOC 2 report identifies deviations or exceptions at the subservice organization that could affect the suitability of design or operating effectiveness of the CSOCs for which it is responsible. For example, a qualification in the subservice organization's SOC 2 report related to CSOCs over the complete and accurate creation and distribution of reports that were not identified, evaluated, and addressed as part of the service organization's monitoring of subservice organizations (either through existing controls or additional procedures performed), could result in the service auditor identifying a deficiency in the operating effectiveness of monitoring controls at the service organization.

3.172 Paragraph .49 of AT-C section 205 also states that the service auditor should make inquiries of management about subsequent events. In a SOC 2 examination, the service auditor would make inquiries about whether there have been events at the subservice organization that could have a significant effect on the description, the suitability of design, the operating effectiveness of controls, or management's assertion. Inquiries regarding subsequent events are described beginning at paragraph 3.245.

SOC 2 Report From Carved-Out Subservice Organization Is Not Available

3.173 If service organization management does not obtain a type 2 report from a subservice organization, its monitoring of subservice organizations may include tests performed at the subservice organization through the execution of a right-to-audit clause. In such situations, management generally will identify such testing as a control in the description. In any event, the service auditor should obtain sufficient appropriate evidence of the description of the CSOCs and management's monitoring activities over the subservice organization in accordance with paragraph .25 of AT-C section 205.

3.174 When there are CSOCs, the service auditor's report would be modified to refer to them. Appendix C-1, "Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination (Carved-Out Controls of a Subservice Organization and Complementary Subservice Organization Controls and Complementary User Entity Controls)," contains language that may be appropriate when there are CSOCs.

Considering Controls That Did Not Need to Operate During the Period Covered by the Examination

3.175 The description of the service organization's system usually includes controls expected to operate during the period covered by the examination. However, in certain circumstances, some of the service organization's controls may not operate during the examination period because the circumstances that warrant the operation of those controls did not occur during that period. For example, controls related to providing a new user with identification and authentication credentials may not have operated if no new users were added during the examination period. When management informs the service auditor that the circumstances requiring the operation of certain controls did not occur, the service auditor would perform procedures to corroborate management's statement and would describe, in the description of the results of testing, the nature of the procedures performed and the results of such procedures. In such situations, there is no need for the service auditor to modify the opinion on the operating effectiveness of the controls. This might be more common when most or all of the controls relevant to the achievement of the same service commitment or system requirement did not need to operate during the examination period.

Considering the Relevancy of Controls That Operated Prior to the Period Covered by the Examination

3.176 Certain types of controls, such as entity-level controls, may operate with limited frequency, such as on an annual or semiannual basis. When service organization management identifies such controls (referred to as *periodic controls* in this discussion) in the description of the system as relevant to the system and to the achievement of the service organization's service commitments and system requirements, management would typically identify an examination period in which those controls operated. For example, if management reviews the appropriateness of logical access policies and procedures annually in October, management would likely identify an examination date that

encompasses such controls. However, when the engagement period is less than one year, management may not be able to select an engagement period that includes the performance of all periodic controls. This would be the case, for example, when a service organization's annual performance review cycle closes in February, but the system under examination did not begin operation until March, and the service auditor has been engaged to perform the examination for the period April 1 through December 31. In situations such as this, management would need to determine the relevance and significance of the performance review controls performed in February to the service organization's achievement of its service commitments and system requirements during the examination period (April through December).

3.177 If management determines periodic controls are relevant to the achievement of service commitments and system requirements for the current examination period, management would include in the description information about the design of the periodic controls and may also include the most recent history of the controls' operating effectiveness. Management may consider factors such as the following when determining whether a periodic control is relevant:

- Whether the periodic control affects the operation of other controls during the period (For example, approval of an organizational structure change before the period may affect the performance of controls during the period.)
- The length of time between the operation of the control and the examination period (For example, a control that operated one month prior to the start of the examination period is more likely to have an effect on the performance of controls during the examination period than one performed nine months prior to the examination period.)
- The importance of the periodic control to the service organization's efforts to mitigate one or more risks to the achievement of the service commitments and system requirements

When management has described the relevant periodic controls in the description, these same factors may inform the service auditor's evaluation of the description, including whether the controls discussed in the description are suitably designed and implemented.

3.178 In some cases, relevant periodic controls may be so important to the achievement of the service organization's service commitments and system requirements during the current examination period that the service auditor may determine that the lack of sufficient appropriate evidence about the design and operating effectiveness of the periodic controls in the current period would affect the service auditor's ability to issue an unmodified opinion. Examples of such situations include the following:

- The majority of the activities identified by management as addressing trust services criterion CC4.1, *The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning,* operated prior to the start of the examination period.
- A number of periodic control activities intended to mitigate logical and physical access risks, such as scanning to detect points of access, identifying new information assets, and reviewing

credentials of automated processes and vulnerability scanning, were performed prior to the start of the examination period.

3.179 When the service auditor determines that sufficient appropriate evidence cannot be obtained, the service auditor may (*a*) discuss with management the need to extend the current examination period to cover the period during which the periodic controls operated or (*b*) consider the effect of the lack of sufficient evidence about the design and operation of periodic controls on the service auditor's opinion.

3.180 For other relevant periodic controls, the service auditor would consider the nature, timing, and extent of procedures to be performed to obtain evidence about the suitability of their design and operating effectiveness in the current period.[7] For example, assume the service organization had a policy requiring the annual review of the list of personnel authorized to access a colocation facility. Because there were only a few personnel with authorized access, the service auditor may have determined that performing that control on an annual basis was suitable; the control was most recently performed two months prior to the beginning of the current examination period. To conclude that the control is suitably designed and operating effectively during the current period, the service auditor obtained the list of authorized personnel from the colocation facility as of a date during the examination period and determined whether any changes were made to the list during the current period. Because changes were made to the list of authorized personnel, the service auditor reviewed approvals related to such changes to determine that the review control, in conjunction with controls over the approval of changes to the list, result in the control continuing to be suitably designed in the current period. When determining the nature, timing and extent of evidence needed, the service auditor may consider factors such as the following:

- The service auditor's understanding of the nature of changes to the service organization's system, if any, and the assessed risk and the design and implementation of related controls that may reduce the effectiveness of the design or operation of the periodic control in the current period under examination (For example, management may have changed one or more of its monitoring activities to address significant turnover in personnel who operated controls during the examination period; in this case the service auditor would likely determine that it is necessary to test these additional controls.)
- Whether the control is sensitive to other business factors that may have changed (For example, annual vulnerability scanning of information system components may not continue to be appropriate due to the discovery of a new operating system vulnerability identified during the examination period.)
- Whether the nature and frequency with which the periodic control operates is sufficient to provide reasonable assurance that the

[7] When the service auditor is issuing both SOC 1 and SOC 2 reports for the same system and for the same examination period, the service auditor is responsible for complying with the requirement in paragraph .28 of AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, when performing the SOC 1 examination. This paragraph states that evidence obtained in prior engagements about the satisfactory operation of controls in prior periods does not provide a basis for a reduction in testing, even if it is supplemented with evidence obtained during the current period.

service organization's service commitments and system requirements would be achieved

3.181 To reduce the risk that the SOC 2 report is misleading, the description of the service auditor's tests and results of tests would generally include disclosure of the period of time during which the periodic control operated and the results of the tests performed on the operating effectiveness of those controls, as well as a description of the additional procedures performed related to the continued operation and effectiveness of the control during the current examination period and the results of those procedures.

Identifying and Evaluating Deviations in the Operating Effectiveness of Controls

3.182 In accordance with paragraph .46 of AT-C section 205, the service auditor should accumulate and evaluate identified deviations to determine whether the deviations are indicative of a control deficiency. Once that determination is made, the service auditor considers the significance of the deficiency on the effectiveness of the controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. In addition to considering the effect of the deficiency on the opinion on control effectiveness, the service auditor also considers the potential impact of other matters, such as description misstatements.

3.183 When a control deficiency is identified, it is usually helpful to the service organization for the service auditor to discuss it with service organization management in a timely manner. If the control deficiency was identified during interim testing, service organization management may be able to remediate the deficiency for the remainder of the period. In that case, when assessing whether the deficiency is material, the service auditor would be able to consider the effect of the deficiency during the first part of the period on the operating effectiveness of controls to provide reasonable assurance of achieving the service organization's service commitments and system requirements. In other situations, service organization management may be unable to correct the deficiency (for example, in instances in which the operation of the control has already occurred). In such circumstances, timely notification permits service organization management to remediate the deficiency on a go-forward basis.

3.184 If the service auditor becomes aware that any identified deviations have resulted from fraud, suspected fraud, or noncompliance or suspected noncompliance with laws or regulations, paragraph .34 of AT-C section 205 indicates that the service auditor should respond appropriately. In a SOC 2 examination, the service auditor would ordinarily reassess the risk that the description does not present the system that was designed and implemented in accordance with the description criteria, the controls are not suitably designed, and in a type 2 examination, the controls are not operating effectively. Responses that might be appropriate if revision to the risk assessment is necessary are discussed in paragraph 3.222.

3.185 In performing procedures, the service auditor may become aware of a system incident that has affected a system of the service organization that is not the system under examination. For example, the service organization may experience a breach in an IT system that is not a component of the system

under examination. In such situations, the service auditor needs to understand the nature and cause of the breach in case it occurred as a result of ineffective controls shared between all of the service organization's systems. If so, the service auditor would also consider whether there are controls in place to prevent a similar breach in the system under examination (for example, network segmentation). If shared controls are ineffective or there are no additional controls to prevent a similar breach in the system under examination, the service auditor should reconsider the assessment of the risk of material misstatement in accordance with paragraph .35 of AT-C section 205. Additionally, if the system incident is related to a security breach, the service auditor may need to consider whether the inherent risks of the environment connected to the system are significantly different than what was originally assessed or whether controls within the system may have been compromised by an advanced persistent threat that had not previously been detected. As a result of the reassessment of risk, the service auditor may determine that additional procedures are necessary or that management needs to identify additional controls that address the reassessed risks.

3.186 Throughout the course of the examination, the service auditor may perform procedures other than direct tests of operating effectiveness (for example, reviewing results from internal audit reports or other control reports issued by the service organization, or reading other information received from user entities). Such procedures may identify matters that indicate control deviations or deficiencies (such as system incidents arising from the use of a subservice organization) that may be relevant to the SOC 2 examination. In such situations, service organization management and the service auditor would generally separately evaluate and respond appropriately to the issue or event. For example, the service auditor may consider information about an issue or event when determining whether adjustments are needed to the planned nature, timing, or extent of procedures to address any new risks identified. In addition, both management and the service auditor would consider the effect on the SOC report, including whether disclosure of the issue or event in management's description of the service organization's system, management's assertion, and the service auditor's report is necessary to prevent the SOC 2 report from being misleading.

Materiality Considerations When Evaluating the Suitability of Design and Operating Effectiveness of Controls

3.187 The service auditor considers materiality when evaluating whether the effects of identified control deficiencies, individually or in the aggregate, are material with respect to the opinion on control effectiveness. As discussed in chapter 1, "Introduction and Background," the service auditor does this by considering the effect of identified control deficiencies on the service organization's ability to provide reasonable assurance of achieving the service commitments and system requirements based on the applicable trust services criteria. If the service auditor concludes that the effects of identified deficiencies are likely to be material to the achievement of the service commitments and system requirements, the service auditor would modify the opinion on control effectiveness.

3.188 There may be situations in which the service auditor determines that the same control deficiency identified during the SOC 2 examinations of two different service organizations is material for one service organization but

not for the other. When a control deficiency is identified, the service auditor is responsible for evaluating the effect of the deficiency by considering the effect on the system's ability to achieve the service commitments and system requirements that management established based on the trust services criteria. Although the same identified control deficiency may have resulted from the evaluation of a particular trust services criterion, the effect of the deficiency on the overall effectiveness of the system and related controls (that is, whether controls provide reasonable assurance of achieving the service organization's service commitments and system requirements) may be different at each organization.

3.189 Decisions about the effect of control deficiencies identified during the examination are very complex and involve a high degree of professional judgment. Consequently, the same deficiency may result in a different conclusion based on the particular facts and circumstances. For example, assume that service organizations A and B provide cloud infrastructure-as-a-service to commercial entities. Both organizations provide failover processing through load balancing across geographically diverse data centers. The service auditor's testing reveals that in both organizations the design of the failover processing results in a likelihood that processing capacity will be 50% of peak load for the first day of failover due to system resource limitations and the process for reallocating resources. Company A's target market is software-as-a-service (SaaS) entities that provide storage and retrieval of services, and its service commitment around availability is based on monthly total capacity available. Company B's target market is companies that provide financial instrument trading platforms, and its service commitment around availability is based on peak transaction-processing volume. In this example, a service auditor for the two organizations is likely to reach different conclusions when evaluating the effect of the deficiency on the achievement of the organizations' availability commitments.

3.190 The materiality of a control deficiency is considered in the context of qualitative factors and, when applicable, quantitative factors. Qualitative factors the service auditor considers include the following:

- *Relevance of a control to the achievement of a specific service commitment or system requirement based on the applicable trust services criteria.* Not all controls that have been implemented may need to be considered if the risk the control addresses is mitigated through the application of other controls. As an example, assume a service organization mirrors data to a data center located in another city and creates tapes of the data as a secondary backup. These tapes are stored at a third location. Data written to the backup tapes is encrypted. The service organization has identified the encryption of the tape as a control; however, service organization management has not identified physical security controls over the tape storage location in its description because of the following:
    - — The risk that both the primary data center and the mirror site are destroyed simultaneously is remote.
    - — Encryption of the data on the tapes, in conjunction with effective controls over the encryption process and key management, is sufficient.

In this example, physical access controls over the tape storage location are unlikely to be material or relevant because controls over the encryption of the tapes prevent unauthorized access. Accordingly, a deficiency in physical access controls is likely to be immaterial to the service auditor's conclusions about whether backup controls are suitably designed and operating effectively.

- *Alignment between the processes and controls stated in the description and the underlying system controls implemented by the service organization.* If the description includes a particular control, it is likely that report users will assume the control is material for the purposes of the SOC 2 examination. Similarly, report users are likely to expect that such controls, individually or in combination with other controls, operated effectively. For this reason, report users would ordinarily expect the service auditor to test and evaluate those controls as part of the evaluation of suitability of design and operating effectiveness, and deficiencies noted would likely be considered material.
- *The service auditor's understanding of previous communications made to report users about the security, availability, or information processing of the system and the confidentiality or privacy of the information it uses, based on the trust services category or categories included within the scope of the SOC 2 examination.* For example, if the service auditor becomes aware that the service organization has made representations to report users about security (for instance, through a presentation on the service organization's website that indicates that all client data is kept encrypted at all times), the service auditor is more likely to consider those representations important (and thus material) to report users.
- *Relevance to compliance with laws and regulations.* If the service organization is subject to requirements specified by laws or regulations related to security and other trust services categories included within the scope of the SOC 2 examination, identified deficiencies and deviations related to compliance are likely to be significant because they may have additional consequences to the organization. For example, if the service organization is required to meet the requirements of certain laws and regulations that have a direct effect on the services provided by the system being examined (for example, laws protecting sensitive personal information), management may establish service commitments and system requirements about compliance with such laws and regulations. Other laws and regulations (for example, regulations over the physical storage of biohazard materials, when the materials are stored in a warehouse with access secured by an electronic badging system) may be less directly linked to security or other trust services categories. In evaluating the service organization's system requirements, the service auditor may conclude such laws and regulations are relevant to the SOC 2 examination.
- *Interactions with third parties.* Materiality considerations are based on factors such as the likelihood and magnitude of risks arising from interactions with user entities, business partners, subservice organizations, vendors, or others (referred to collectively as *third parties*) with access to the service organization's

system, the degree to which those risks are relevant to the system, and the extent to which the service organization monitors controls performed by those third parties. In some cases, those third parties operate controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that one or more of the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. The more necessary those controls are to the service organization's achievement of its service commitments and system requirements based on the applicable trust services criteria, the more material such interactions with third parties are likely to be.

- *Performance indicators related to event occurrence, detection, and remediation.* The service organization's performance indicators about a system event (such as the mean time from first occurrence to detection and the mean time from detection to remediation) may be indicative of challenges in the design or operating effectiveness of system controls; accordingly, such factors may affect materiality judgments.
- *Degree to which controls are designed to identify and address threats and vulnerabilities that are currently unknown.* Certain controls may have the ability to detect and address unknown threats and vulnerabilities. An example of such a control is a data loss prevention (DLP) control that monitors and restricts outbound information, regardless of what caused the attempt to send the information externally. For that reason, deficiencies in those controls may be considered more significant (material) to the SOC 2 examination.
- *Threats related to prior periods.* An identified threat or vulnerability in a prior period may affect the service auditor's conclusion about the suitability of design and operating effectiveness of controls for the current period.
- *Effect of deviations.* Identified deviations may affect the service organization's ability to mitigate threats or vulnerabilities to the system. For example, the service auditor may question service organization management's assertion that a control is operating effectively when procedures performed resulted in observed deviations in the operation of that control.
- *Intentional acts.* A deficiency or deviation may be the result of an intentional or an unintentional act. An intentional act, particularly one perpetrated by service organization management or senior management, is likely to be considered more material than an unintentional act.
- *Effect of a control deficiency on third parties.* A deficiency in controls may relate to the relationship between the service organization and its user entities or business partners. A deficiency in controls at the service organization that could also result in a deficiency in controls at a user entity or business partner is more likely to be considered material.

3.191 Quantitative factors to be considered in a SOC 2 examination relate to matters such as the tolerable rate of deviation and the observed rate of

deviation. (In this guide, the tolerable rate of deviation is the maximum rate of deviation in the operation of the control that the service auditor is willing to accept without modifying the opinion on any of the subject matters in the examination.) Quantitative factors are less likely to apply when evaluating the design of controls. However, when evaluating the operating effectiveness of the controls, the service auditor should consider the effect of identified deviations, both individually and in combination with other identified deviations, in accordance with paragraph .60 of AT-C section 205.

3.192 Paragraph .18 of AT-C section 205 indicates that the service auditor should reconsider materiality if the service auditor becomes aware of information during the examination that would have caused a different materiality to have been determined initially.

The Service Auditor's Responsibility Regarding Compliance With Laws and Regulations

3.193 In a SOC 2 examination, the service auditor does not opine directly on whether the service organization complied with the requirements of relevant laws and regulations. Instead, the examination addresses whether controls were suitably designed and, in a type 2 examination, operated effectively to provide reasonable assurance of achieving the service commitments or system requirements that management has established related to such laws and regulations. In most cases, management would identify system requirements that are necessary to support compliance with laws and regulations with which the service organization is required to comply. When system requirements are identified, the service auditor would test the suitability of design and, in a type 2 report, the operating effectiveness of controls related to those system requirements.

3.194 Even in situations in which management has not identified specific service commitments or system requirements regarding compliance with laws and regulations, AT-C section 205 notes certain procedures that should be performed regarding compliance with laws and regulations, similar to procedures required related to fraud.

3.195 In accordance with paragraph .33 of AT-C section 205, the service auditor should (*a*) consider whether risk assessment procedures and other procedures related to understanding the service organization's system and related controls indicate a risk of material misstatements due to fraud or noncompliance with laws or regulations (as discussed in chapter 2); (*b*) inquire of appropriate parties to determine whether they have knowledge of any actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the service organization's system and related controls; (*c*) evaluate whether there are unusual or unexpected relationships within the service organization's system and related controls, or between the service organization's system and related controls and other related information, that indicate risks of material misstatement due to fraud or noncompliance with laws or regulations; and (*d*) evaluate whether other information obtained indicates a risk of material misstatement due to fraud or noncompliance with laws or regulations. Paragraph .A33 of AT-C section 205 and paragraph 3.223 of this guide discuss steps that the service auditor may take to appropriately respond to noncompliance or suspected noncompliance with laws or regulations that is identified during the engagement.

3.196 Although a SOC 2 report does not provide an opinion on whether the service organization complied with relevant laws or regulations, there may be situations in which management may want an opinion on compliance with relevant laws or regulations. In that situation, management may engage a practitioner to examine and report on compliance with requirements of specified laws and regulations in accordance with AT-C section 315, *Compliance Attestation*.

Using the Work of the Internal Audit Function

3.197 Chapter 2 discusses a service auditor's considerations with respect to understanding the nature of the internal audit function's responsibilities, and the activities it performs, to determine whether to use the work of internal audit during the SOC 2 examination. For situations in which the service auditor decides to use the work of the internal audit function in the SOC 2 examination, chapter 2 also addresses the need to obtain written acknowledgment from service organization management, as the responsible party, that internal auditors providing direct assistance will be allowed to follow the service auditor's instructions without management's interference, the evaluation of the objectivity and technical competence of members of the internal audit function, and the coordination of procedures with them, among other matters. This section discusses the service auditor's responsibility to test the work of the internal audit function to determine whether it is adequate for the examination.

3.198 When using the work of the internal audit function, paragraph .41 of AT-C section 205 states that the service auditor should perform sufficient procedures, including reperformance, on the body of work of the internal audit function that the service auditor plans to use in order to evaluate whether such work is adequate for the service auditor's purposes.

3.199 The nature, timing, and extent of procedures the service auditor performs in evaluating the adequacy of that work depends on the service auditor's assessment of the significance of that work to the service auditor's conclusions (for example, the significance of the risks that the controls are intended to mitigate). Such procedures usually consist of one or more of the following:

- Independent testing of items tested by the internal audit function (reperformance)
- Independent selection of items from the population tested by internal audit and the performance of tests of a similar nature to those performed by internal audit to independently evaluate internal audit's conclusion

3.200 Some relevant factors in determining whether to use the work of the internal audit function to obtain evidence about the operating effectiveness of controls include the pervasiveness of the control, the potential for management override of the control, and the degree of judgment and subjectivity required to evaluate the effectiveness of the control. As the significance of these factors increases, so does the need for the service auditor, rather than the internal audit function, to perform the procedures, and conversely, as these factors decrease in significance, the need for the service auditor to perform the tests decreases.

3.201 The service auditor uses professional judgment in performing procedures to evaluate the work performed by the members of the entity's internal audit function. As discussed in chapter 2, the service auditor is responsible for determining the work to be performed and obtaining sufficient appropriate

evidence for the opinion. The service auditor has sole responsibility for the opinion expressed in the service auditor's report, and that responsibility is not reduced by the service auditor's use of the work of the internal audit function.

3.202 If the service auditor finds that the quality and extent of the work performed by the members of the entity's internal audit function are not equivalent to the quality and extent of work the service auditor would have performed, the service auditor generally performs additional procedures and considers the extent to which the work of the internal audit function may be used to obtain evidence.

3.203 In reviewing internal audit reports, the service auditor evaluates exceptions identified by the members of the entity's internal audit function to determine whether those exceptions require the service auditor to alter the nature, timing, and extent of the service auditor's procedures. The service auditor ordinarily corroborates exceptions identified by the members of the internal audit function and considers the extent of the exceptions, their nature and underlying causes, and whether additional procedures by the service auditor are necessary.

3.204 Another relevant factor in evaluating the adequacy of the work of the internal audit function is the adequacy of the sampling procedures used and whether the sampling procedures were appropriate and free from bias (that is, whether all items in the population have the same opportunity to be selected). AICPA Audit Guide *Audit Sampling* provides additional guidance that may be useful to a service auditor who has decided to use audit sampling in performing procedures.

3.205 If the size of the sample used by the members of the entity's internal audit function is less than the sample size the service auditor would have used, the service auditor generally would select additional items to achieve the required sample size. For example, if internal audit has selected a sample of 25 items for testing, the service auditor may determine that an additional 15 items need to be tested.

3.206 The responsibility to report on the description of the system, the suitability of design of controls, and in a type 2 examination, the operating effectiveness of controls rests solely with the service auditor and cannot be shared with the internal audit function. Therefore, the judgments about the significance of deviations in the effectiveness of controls, the sufficiency of procedures performed, the evaluation of identified deficiencies, and other matters that affect the service auditor's opinion are those of the service auditor. In making judgments about the extent of the effect of the work of the internal audit function on the service auditor's procedures, the service auditor may determine, based on the risk associated with the controls and the significance of the judgments relating to them, that the service auditor will perform the work relating to some or all of the controls, rather than using the work performed by the internal audit function.

3.207 When using internal auditors to provide direct assistance, paragraph .43 of AT-C section 205 states that the service auditor should direct, supervise, and review the work of the internal auditors. The service auditor fulfills that responsibility by (*a*) informing the internal auditors of their responsibilities, the objectives of the procedures they are to perform, and matters that may affect the nature, timing, and extent of their procedures and by

(*b*) supervising and reviewing the work performed by internal auditors in a manner similar to the review of work performed by the firm's own staff.

3.208 Paragraph .45 of AT-C section 205 states that the service auditor should, before the completion of the engagement, evaluate whether the use of the work of the internal audit function or the use of internal auditors to provide direct assistance results in the service auditor still being sufficiently involved in the examination, given the service auditor's sole responsibility for the opinion expressed.

Using the Work of a Service Auditor's Specialist

3.209 Chapter 2 discusses the service auditor's responsibilities when a service auditor's specialist will be used in the SOC 2 examination. Those responsibilities include (*a*) evaluating the specialist's competence, capabilities, and objectivity; (*b*) obtaining an understanding of the specialist's field of expertise to enable the service auditor to determine the nature, scope, and objectives of the specialist's work and to evaluate the adequacy of that work; and (*c*) agreeing with the specialist on the terms of the engagement and other matters. In addition to those responsibilities, paragraph .37 of AT-C section 205 states that the service auditor should evaluate the adequacy of the work of the service auditor's specialist for the service auditor's purposes.

3.210 According to paragraph .37*d* of AT-C section 205, evaluating the adequacy of the work of the service auditor's specialist involves consideration of the following:

a. The relevance and reasonableness of the findings and conclusions of the specialist and their consistency with other evidence

b. If the work of the service auditor's specialist involves the use of significant assumptions and methods,

  i. obtaining an understanding of those assumptions and methods and

  ii. evaluating the relevance and reasonableness of those assumptions and methods in the circumstances, giving consideration to the rationale and support provided by the service auditor's specialist, and in relation to the service auditor's other findings and conclusions

c. If the work of the service auditor's specialist involves the use of source data that is significant to the work of the service auditor's specialist, the relevance, completeness, and accuracy of that source data

3.211 If the service auditor determines that the work of the service auditor's specialist is not adequate, paragraph .38 of AT-C section 205 states that the service auditor should

a. agree with the service auditor's specialist on the nature and extent of further work to be performed by the service auditor's specialist or

b. perform additional procedures considered appropriate in the circumstances.

Revising the Risk Assessment

3.212 Paragraph .35 of AT-C section 205 states that the service auditor's assessment of the risks of material misstatement may change during the course of the examination as additional evidence is obtained. If the service auditor obtains evidence from performing further procedures, or if new information is obtained (for example, the identification of a security breach that could affect the system under examination as discussed in paragraph 3.185), either of which is inconsistent with the evidence on which the service auditor originally based the assessment, the service auditor should revise the assessment and modify the planned procedures accordingly. Such further procedures may include asking service organization management to modify the description, as necessary.

Evaluating the Sufficiency and Appropriateness of Evidence

3.213 Sufficient appropriate evidence is necessary to support the service auditor's opinion and report. Such evidence is cumulative in nature and may come from sources inside or outside of the service organization. Evidence comprises both information that supports and corroborates aspects of the subject matter and any information that contradicts aspects of the subject matter. In addition, in some cases, the absence of information (for example, refusal by the responsible party to provide a requested representation) also constitutes evidence.

3.214 According to paragraph .47 of AT-C section 205, the service auditor should evaluate the sufficiency and appropriateness of the evidence obtained in the context of the engagement and, if necessary, attempt to obtain further evidence. Concluding on the sufficiency and appropriateness of evidence is discussed beginning in paragraph 4.08. As discussed in paragraphs .47–.48 of AT-C section 205, if the service auditor is unable to obtain sufficient appropriate evidence, a scope limitation exists and the service auditor should express a qualified opinion, disclaim an opinion, or withdraw from the engagement, when withdrawal is possible under applicable law or regulation. The service auditor should apply the requirements in paragraphs .70–.86 of AT-C section 205 when a scope limitation exists and the service auditor is determining the type of opinion to be issued.

Evaluating the Results of Procedures

3.215 In accordance with paragraph .46 of AT-C section 205, the service auditor should accumulate description misstatements and deficiencies related to the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls for use in forming the service auditor's opinion. Misstatements or deficiencies related to a specific subject matter in the service auditor's opinion (for example, the description of the service organization's system) may affect the other subject matters in the opinion (the suitability of the design or operating effectiveness of controls). For example, a description misstatement resulting from the inclusion of controls that have not been implemented may also affect the suitability of the design of controls and the operating effectiveness of the controls because the service organization has not implemented those controls. Chapter 4 discusses the effect that the service auditor's opinion modification on one subject matter may have on the other subject matters.

3.216 In accordance with paragraph .47 of AT-C section 205, the service auditor should consider all relevant evidence, which may include conducting both a quantitative analysis (for example, rates of deviations in testing a control using a sample-based testing strategy) and qualitative analysis of identified description misstatements and control deficiencies. That consideration is used to determine whether such misstatements and deficiencies are material; if so, the service auditor's opinions on the description, the suitability of design of controls, and in a type 2 examination, the operating effectiveness of controls might be affected. As an example, assume that, when investigating the follow-up and resolution of two identified system incidents, the service auditor determined that the resolution took longer to complete than the management-prescribed resolution requirement but that the difference was not material (for example, final resolution took two days longer than prescribed). In that situation, the service auditor concluded that the identified deficiencies were not material. However, if the service auditor's testing had indicated that entity personnel failed to follow up at all for either of the two instances, the service auditor might have concluded that the controls were not effective in achieving one or more service commitments or system requirements based on the applicable trust services criteria. (As discussed in paragraph 4.19, the service auditor would disclose all identified deficiencies in the description of the service auditor's tests and results, regardless of the service auditor's conclusion about operating effectiveness.)

3.217 Evaluating the results of procedures involves investigating the nature and cause of any identified description misstatements and deficiencies or deviations in the design or effectiveness of controls and determining the following:

- Whether the identified description misstatements result in either the failure to meet one or more of the description criteria or in a presentation that could be misleading to users if the service auditor's opinion were not modified to reflect the identified description misstatements
- Whether identified deviations are within the expected rate of deviation and are acceptable or whether they constitute a deficiency
- If deviations are within the expected rate of deviation, whether the procedures performed provide an appropriate basis for concluding that the control operated effectively throughout the specified period
- Whether identified deficiencies are likely to have, in the service auditor's judgment, a pervasive effect on the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria
- Whether
  - another tested control (or combination of controls), often referred to as compensating controls, provides sufficient appropriate evidence about whether controls operated effectively or
  - additional testing of the control or other controls is necessary to determine whether the controls were effective throughout the period (If the service auditor is unable to apply additional procedures to the selected items, the service auditor would consider the reasons for this limitation

and conclude on whether those selected items are deviations from the prescribed policy or result in a limitation of the scope of the examination.)

- The significance of the effect of such deficiencies on the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria

Considering Whether the Description Is Misstated or Otherwise Misleading

3.218 In accordance with paragraph .61 of AT-C section 205, the service auditor should evaluate whether the description is misleading within the context of the engagement based on the evidence obtained. Paragraph .A79 of AT-C section 205 states that, when making this evaluation, the service auditor may consider whether additional disclosures are necessary to supplement the description. Additional disclosures may include, for example,

- significant interpretations made in applying the criteria in the engagement circumstances (for example, what constitutes a system event or a system incident) and
- subsequent events,[8] depending on their nature and significance.

3.219 Such additional disclosures may be presented in the description (in which case they are subject to the service auditor's examination procedures) or as other information. The service auditor's responsibility for other information presented in a SOC 2 report is discussed beginning at paragraph 4.101.

3.220 Although the description should be presented in accordance with the description criteria, paragraph .61 of AT-C section 205 does not require the service auditor to determine whether the description discloses every matter related to the service organization's system. That is because the description is intended to meet the common informational needs of the broad range of SOC 2 report users; accordingly, the description is unlikely to contain disclosures considered useful by every report user. For example, a description may omit certain information related to aspects of the service organization's system when those aspects are unlikely to be significant (in other words, they are immaterial) to report users' decisions.

Responding to and Communicating Known and Suspected Fraud, Noncompliance With Laws or Regulations, Uncorrected Misstatements, and Deficiencies in the Design or Operating Effectiveness of Controls

Known or Suspected Fraud or Noncompliance With Laws or Regulations

3.221 As discussed in chapter 2, the service auditor has a responsibility to consider known or suspected incidents of fraud[9] and noncompliance with laws

---

[8] Subsequent events are discussed beginning in paragraph 3.243.

[9] Paragraph .12 of AT-C section 105, *Concepts Common to All Attestation Engagements*, defines *fraud* as an intentional act involving the use of deception that results in a misstatement in the subject matter or the assertion.

or regulations relevant to the examination. Such incidents may include, for example, the intentional bypassing of controls and the intentional misstatement of one or more aspects of the description. As discussed in paragraph 3.190, when a deficiency or deviation is the result of an intentional act, it is likely to be considered more material than a deficiency or deviation caused by an unintentional act, particularly if the intentional act was perpetrated by a member of senior management. The service auditor determines the effect of such incidents on the description; the suitability of design of controls; in a type 2 examination, the operating effectiveness of controls; and the service auditor's report. Additionally, the service auditor communicates such information to appropriate parties.

3.222 When incidents of fraud or suspected fraud are identified during the examination, the service auditor is expected to respond appropriately. For example, unless prohibited by law, regulation, or ethics standards, appropriate responses may include the following:

- Discussing the matter with service organization senior management (and the engaging party, if different) and other appropriate parties, unless senior management is suspected to have committed the fraud
- If the service auditor suspects fraud involving senior management, communicating those suspicions to those charged with governance and discussing with them the nature, timing, and extent of procedures necessary to complete the examination
- Requesting that senior management (and the engaging party, if different) consult with an appropriately qualified third party, such as the service organization's legal counsel or a regulator
- Considering the implications of the matter in relation to other aspects of the engagement, including the service auditor's risk assessment and the reliability of written representations from service organization management (and the engaging party, if different)
- Obtaining legal advice about the consequences of different courses of action
- Communicating with third parties (such as a regulator)
- Withdrawing from the engagement

3.223 The actions noted in the preceding paragraph may also be appropriate in response to noncompliance or suspected noncompliance with laws or regulations identified during the engagement. In addition, the service auditor may decide to describe the matter in a separate paragraph in the service auditor's report, unless the following apply:

a. The service auditor is precluded by service organization management (or the engaging party, if different) from obtaining sufficient appropriate evidence to evaluate whether noncompliance that may be material to the conclusion about the suitability of design of controls or, in a type 2 examination, the operating effectiveness of controls has, or is likely to have, occurred. In this situation, there is a scope limitation that precludes the service auditor from expressing an opinion on the suitability of design or the operating effectiveness of controls; accordingly, the service auditor would disclaim an opinion.

b. The service auditor concludes that the noncompliance results in the failure of the service organization's controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. In this situation, the service auditor expresses a modified opinion.

Communicating Incidents of Known or Suspected Fraud, Noncompliance With Laws or Regulations, Uncorrected Misstatements, or Internal Control Deficiencies

3.224 In addition to responding to known and suspected fraud and noncompliance with laws or regulations, the service auditor should communicate information regarding those matters, along with information regarding any uncorrected description misstatements or material deficiencies, to the appropriate levels of management (and to the engaging party, if different) in accordance with paragraph .87 of AT-C section 205. The service auditor may also consider whether to communicate other matters.

3.225 In accordance with paragraph .88 of AT-C section 205, if the service auditor encounters known or suspected fraud or noncompliance with laws or regulations, the service auditor should consider responsibilities under the AICPA Code of Professional Conduct and applicable law prior to communicating such information to management (and the engaging party, if different).

3.226 The service auditor may be precluded from reporting such incidents to parties outside the service organization because of the service auditor's professional duty to maintain the confidentiality of client information. Paragraph .A125 of AT-C section 205 reminds the service auditor that disclosure of confidential information, as defined in the Code of Professional Conduct, requires explicit consent of service organization management.

3.227 In circumstances in which such matters are identified, the service auditor may consider discussing with legal counsel or others prior to communicating or taking further action.

Obtaining Written Representations

3.228 During the SOC 2 examination, service organization management makes many oral and written representations to the service auditor in response to specific inquiries or through the presentation of the description and management's assertion. Such representations from management are part of the evidence the service auditor obtains. However, they cannot replace other evidence the service auditor could reasonably expect to be available, nor do they provide sufficient appropriate evidence on their own about any of the matters with which they deal. Furthermore, the fact that the service auditor has received reliable written representations does not affect the nature or extent of other evidence that the service auditor obtains.

3.229 It is up to the service auditor to determine the appropriate person or persons within the service organization's management or governance structure with whom to interact, including considering which person or persons have the appropriate responsibilities for and knowledge of the matters concerned. In addition, in certain circumstances, the service auditor may obtain written

representations from parties in addition to service organization management, such as those charged with governance.

3.230 In some cases, the party making the assertion may be indirectly responsible for and knowledgeable about specified matters covered in the representations. For example, the chief information officer (CIO) of the service organization may be knowledgeable about certain matters through personal experience and about other matters through employees who report to the CIO. The service auditor may request that individuals who are directly or indirectly responsible for and knowledgeable about matters covered in the written representations provide their own representations.

3.231 Written representations ordinarily confirm representations explicitly or implicitly given to the service auditor, indicate and document the continuing appropriateness of such representations, and reduce the possibility of a misunderstanding concerning the matters that are the subject of the representations.

3.232 Paragraph .51 of AT-C section 205 indicates that, in an examination, a service auditor should request written representations in the form of a letter from the responsible party. In accordance with that paragraph, the following representations should be included in the representation letter:

a. Management's assertion about the subject matters[10] based on the criteria[11]

b. A statement that all relevant matters are reflected in the measurement or evaluation of the subject matters or assertion

c. A statement that all known matters contradicting the subject matters or assertion and any communication from regulatory agencies or others affecting the subject matters or assertion have been disclosed to the service auditor, including communications received between the end of the period addressed in the written assertion and the date of the service auditor's report (In a SOC 2 engagement, this would generally include information about misstatements in the description, instances in which controls were not suitably designed and implemented, instances in which controls did not operate effectively or as described, and communications from regulatory agencies, user entities, or others affecting the presentation of the description or the suitability of the design or operating effectiveness of controls, including communications received between the end of the period addressed in the description and the date of the report.)

d. Acknowledgement of management's responsibility for

i. the description; suitability of design of controls; in a type 2 examination, operating effectiveness of controls; and management's assertion;

---

[10] Within this section of the guide, the term *subject matters* refers to the subject matters in the SOC 2 examination: (*a*) the description, (*b*) the suitability of design of controls, and (*c*) in a type 2 examination, the operating effectiveness of controls.

[11] Within this section of the guide, the term *criteria* refers to both the description criteria and the trust services criteria.

ii. selecting the criteria (in a SOC 2 engagement, this would generally also include management's responsibility for selecting the trust services category or categories to be included within the scope of the examination and stating the applicable trust services criteria and related controls in the description); and

iii. determining that such criteria are suitable, will be available to the intended users, and are appropriate for the purpose of the engagement

e. A statement that management has disclosed to the service auditor

i. all deficiencies in internal control relevant to the SOC 2 examination of which it is aware, including uncorrected misstatements;

ii. its knowledge of any actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the description, the suitability of design of controls, and the operating effectiveness of controls;

iii. identified system incidents that resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements as of the date of the description (for a type 1 examination) or during the period of time covered by the description (for a type 2 examination); and

iv. other matters the service auditor deems appropriate (in a SOC 2 engagement, this would generally include any changes in the controls that are likely to be relevant to report users)

f. A statement that any known events subsequent to the period (or point in time) of the subject matters being reported on that would have a material effect on the subject matters or assertion have been disclosed to the service auditor

g. A statement that management has provided the service auditor with all relevant information and access, as agreed upon in the terms of the engagement

h. If applicable, a statement that management believes the effects of uncorrected misstatements (description misstatements and deficiencies) are immaterial, individually and in the aggregate, to the subject matters

3.233 Other matters about which the service auditor may request representations generally depend on the facts and circumstances of the engagement. For instance, if changes to the service organization's controls have been made during the period covered by the examination, the service auditor may decide to request certain representations that address the period before the change and the period after the change.

3.234 The required written representations are separate from, and in addition to, management's written assertions. They are usually made in the form of a representation letter addressed to the service auditor, dated as of the date of the service auditor's report, and address the subject matters and periods referred to in the service auditor's opinion.

3.235 When written representations are directly related to matters that are material to the subject matter, paragraph .54 of AT-C section 205 states that the service auditor should

a. evaluate their reasonableness and consistency with other evidence obtained, including other representations (oral or written) made by service organization management, and

b. consider whether those making the representations can be expected to be well informed on the particular matters.

3.236 If a service organization uses a subservice organization, and service organization management has elected to use the inclusive method to present the services and controls at the subservice organization, the service auditor would also request many of the same representations listed in paragraph 3.232 from subservice organization management. Obtaining written representations from subservice organization management when the inclusive method is used is discussed beginning in paragraph 2.105.

3.237 Illustrative representation letters that may be appropriate for use in a type 1 and type 2 examination are available on the AICPA website.

3.238 In certain situations, the service auditor may become aware of information that causes the service auditor to reconsider some of the conclusions reached to that point. For example, when obtaining the written representations from management, the service auditor may learn about a previously unknown security incident or a suspected fraud. The discovery of such information at this point in the examination would lead the service auditor to consider the effect of the matter on the risk assessment and other conclusions that the service auditor has reached. In some cases, the service auditor may conclude that reassessment of the risks of material misstatement is necessary, which may lead to the need to perform further procedures. Depending on the circumstances, the service auditor may also consider the guidance in the next section with respect to other actions that may be appropriate.

Requested Written Representations Not Provided or Not Reliable

3.239 Paragraph .56 of AT-C section 205 provides guidance to the service auditor when

- service organization management has not provided one or more of the requested representations;
- the service auditor concludes that there is sufficient doubt about the competence, integrity, ethical values, or diligence of those providing the written representations; or
- the service auditor concludes that the written representations are otherwise not reliable.

3.240 In such circumstances, that paragraph states that the service auditor should

- discuss the matter with the appropriate party,
- reevaluate the integrity of those from whom the representations were requested or received and evaluate the effect that this may have on the reliability of representations and evidence in general, and

- if any of the matters are not resolved to the service auditor's satisfaction, take appropriate action, including determining the possible effect on the opinions in the service auditor's report.

Engaging Party Is Not the Responsible Party

3.241 Paragraph .52 of AT-C section 205 provides the option of obtaining oral (rather than written) representations from the responsible party (service organization management) in an examination engagement in which the engaging party is not the responsible party and the responsible party refuses to provide the required written representations. However, in the examination discussed in this guide, service organization management's refusal to furnish evidence in the form of written representations constitutes a limitation on the scope of the examination sufficient to preclude an unmodified opinion on either the description or the effectiveness of controls. Usually, the scope limitation is sufficient to cause the service auditor to disclaim an opinion on the description and the effectiveness of controls or to withdraw from the engagement. The alternative provided in paragraph .52 of AT-C section 205 of obtaining oral representations is not permitted in this examination.

Representations From the Engaging Party When Not the Responsible Party

3.242 When the engaging party is not the responsible party, paragraph .53 of AT-C section 205 states that the service auditor should request written representations from the engaging party, in addition to those requested from the responsible party, in the form of a letter addressed to the service auditor. In accordance with that paragraph, written representations should include the following:

a. An acknowledgment that the responsible party is responsible for the subject matter being in accordance with the criteria and for its assertion

b. An acknowledgement of the engaging party's responsibility for selecting the criteria

c. An acknowledgement of the engaging party's responsibility for determining that such criteria are suitable, will be available to the intended users, and are appropriate for the purposes of the engagement

d. A statement that the engaging party is not aware of any material misstatements in the description, suitability of design of controls, and in a type 2 examination, operating effectiveness of controls or assertion

e. A statement that the engaging party has disclosed to the service auditor all known events subsequent to the period (or point in time) of the subject matter being reported on that would have a material effect on the subject matter or assertion

f. Other matters that the service auditor deems appropriate

Subsequent Events and Subsequently Discovered Facts

3.243 Events or transactions may occur after the period of time covered by the examination, but prior to the date of the service auditor's report, that could

have a significant effect on the description, the suitability of design of controls, and in a type 2 examination, the operating effectiveness of controls. In such circumstances, disclosure of those events and transactions in the description or in management's assertion may be necessary to prevent report users from being misled.

3.244 The following are examples of events that could affect the description of the service organization's system or management's assertion:

- After the period covered by the examination, service organization management discovered that, during the last quarter of that period, the IT security director provided all the programmers with access to the production data files, enabling them to modify data.
- After the period covered by the examination, service organization management discovered that a confidentiality breach occurred during the period covered by the service auditor's report.

3.245 In accordance with paragraph .49 of AT-C section 205, the service auditor should inquire of management (and if different, the engaging party) about whether it is aware of any such events. If such events exist, the service auditor should apply appropriate procedures to obtain evidence regarding the events. For example, the service auditor may obtain evidence by inquiring about and considering information about the operating effectiveness of controls by inspecting the following:

- Relevant internal auditors' reports issued during the subsequent period
- Other practitioners' reports issued during the subsequent period
- Relevant regulatory agencies' reports issued during the subsequent period
- Reports on other professional engagements for that entity

3.246 Paragraph .49 of AT-C section 205 does not require the service auditor to perform any procedures regarding the description, the suitability of design of controls, or the operating effectiveness of controls after the date of the service auditor's report. However, paragraph .50 of AT-C section 205 clarifies that the service auditor is responsible for responding appropriately to facts that become known after the date of the report that, had they been known as of the report date, may have caused the service auditor to revise the report.

3.247 After obtaining information about an event, the service auditor determines whether the facts existed at the date of the report and, if so, whether persons who would attach importance to these facts are currently using, or likely to use, the SOC 2 report (which includes the description, management's assertion, and the service auditor's report). The service auditor may do this through discussions with management and other appropriate parties and through the performance of additional procedures that the service auditor considers necessary to determine whether the description, assertion, and service auditor's report need revision or whether the previously issued report continues to be appropriate.

3.248 Specific actions to be taken at that point depend on a number of factors, including the time elapsed since the date of the service auditor's report and whether issuance of a subsequent report is imminent. Depending on the circumstances, the service auditor may determine that notification of persons

currently using or likely to use the service auditor's report is necessary. This may be the case, for example, when

- the SOC 2 report is not to be relied upon because
  - — the description, management's assertion, or the service auditor's report needs revision or
  - — the service auditor is unable to determine whether revision is necessary and
- issuance of a subsequent service auditor's report is not imminent.

3.249 In accordance with paragraph .49 of AT-C section 205, if the service auditor believes the event is of such a nature and significance that its disclosure is necessary to prevent report users from being misled, the service auditor should determine whether information about the event is adequately disclosed in the description or in management's assertion. For example, assume that, after the period covered by the examination but prior to the date of the service auditor's report, service organization management learns of a system incident involving the loss of customers' personal information. After investigation, management determines that the incident stemmed from an otherwise unknown vulnerability in its system; furthermore, that vulnerability existed during the examination period. In this example, the service auditor ordinarily would conclude that the matter should be disclosed in the description and assertion. If it is not, the service auditor's course of action depends on the service auditor's legal and ethical rights and obligations. Therefore, the service auditor may consider seeking legal advice before deciding on a course of action. Appropriate actions may include

a. disclosing the event (including a description of the nature of the event and its effect on the description, assertion, or report) in the service auditor's report and modifying the related service auditor's opinion and

b. withdrawing from the engagement.

Subsequent Events Unlikely to Have an Effect on the Service Auditor's Report

3.250 The service auditor may have determined that the event discovered subsequent to the period covered by the examination would likely have had no effect on the description, the suitability of design of controls, or in a type 2 examination, the operating effectiveness of controls because the underlying situation did not exist until after the period covered by the SOC 2 report. However, the matter may be sufficiently important to warrant disclosure by management in its description and, potentially, emphasis by the service auditor in the service auditor's report. The following are examples of such events:

- The service organization was acquired by another entity.
- The service organization experienced a significant operating disruption or other extraordinary event such as an event caused by weather or other natural disasters.
- A data center hosting service organization that provides applications and technology to enable user entities to perform essential business functions made significant changes to its information systems, including a system conversion or significant outsourcing of operations, after the date of the SOC 2 report.

Documentation

3.251 Paragraphs .37–.44 of AT-C section 105, *Concepts Common to All Attestation Engagements*, provide requirements regarding the documentation that should be prepared for an attestation engagement. Those paragraphs address matters such as the timeliness of the documentation, how to make necessary changes to the documentation after the original preparation date, retention of engagement documentation, confidentiality of documentation, and the need to document situations in which the service auditor judges it necessary to depart from a relevant presumptively mandatory requirement.

3.252 Additionally, paragraphs .89–.90 of AT-C section 205 discuss the service auditor's responsibilities for preparing and maintaining documentation that is appropriate to an examination. The service auditor's documentation in a SOC 2 examination is the principal record of attestation procedures applied, information obtained, and conclusions or findings reached by the service auditor. The quantity, type, and content of documentation are matters of the service auditor's professional judgment. However, the documentation should be sufficient to determine the following:

a. The nature, timing, and extent of the procedures performed to comply with AT-C section 205 and applicable legal and regulatory requirements, including the following:
   i. The identifying characteristics of the specific items or matters tested
   ii. Who performed the engagement work and the date such work was completed
   iii. The discussions with management or others about findings or issues that, in the service auditor's professional judgment, are significant, including the nature of the significant findings or issues discussed and when and with whom the discussions took place
   iv. When management will not provide one or more of the requested written representations or the service auditor concludes that there is sufficient doubt about the competence, integrity, ethical values, or diligence of those providing the written representations or that the written representations are otherwise not reliable, the matters in paragraph .56 of AT-C section 205 (see discussion beginning in paragraph 3.239)
   v. Who reviewed the engagement work performed and the date and extent of such review
   vi. If the service auditor has identified information that is inconsistent with the service auditor's final opinion regarding a significant matter, how the service auditor addressed the inconsistency

b. The results of the procedures performed and the evidence obtained

3.253 If, after the date of the report, the service auditor becomes aware of facts that may have caused the service auditor to revise the report had they been known at the time of the report, paragraph .90 of AT-C section 205 indicates that documentation in the SOC 2 examination should include the following in addition to the items in paragraph 3.252:

- The circumstances encountered
- Any new or additional procedures performed, evidence obtained, and conclusions reached and their effect on the report
- When and by whom the resulting changes to the documentation were made and reviewed

3.254 As in other attestation engagements, documentation in the SOC 2 examination would ordinarily also include a record of the following:

- Issues identified with respect to compliance with relevant ethical requirements and how they were resolved
- Conclusions on compliance with independence requirements that apply to the engagement and any relevant discussions with the firm that support these conclusions
- Conclusions reached regarding the acceptance and continuance of client relationships and attestation engagements
- The nature and scope of, and conclusions resulting from, consultations undertaken during the course of the engagement
- If the service auditor uses the work of the internal audit function, other practitioners, or the service auditor's specialists, documentation of conclusions reached by the service auditor regarding the evaluation of the adequacy of the work and the procedures performed on that work

3.255 Paragraphs .A127–.A130 of AT-C section 205 provide additional application guidance that might be helpful to a service auditor when deciding what to document in the SOC 2 examination.

Considering Whether Service Organization Management Should Modify Its Assertion

3.256 As discussed in chapter 2, service organization management provides the service auditor with a written assertion about whether the description presents the system that was designed and implemented in accordance with the description criteria and whether the controls within the program were effective. Management's written assertion is generally expected to align with the service auditor's opinion by reflecting the same modifications.

3.257 The following is an example of modifications (indicated with bold text) that might be made to management's assertion when there is a description misstatement that results in a description that does not present the system that was designed and implemented in accordance with the description criteria:

[*Assertion paragraph*]

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

a. **except for the effects of the matter described in the following paragraph,** the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and

system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria.

The description states that XYZ has physical access controls that incorporate biometric devices and individual PINs. Although such controls have been implemented throughout XYZ's main facility, they have not been consistently implemented in the other three facilities.

3.258 The following is an example of modifications (indicated with bold text) that might be made to management's assertion when there are deficiencies in the suitability of design and operating effectiveness of controls:

[*Assertion paragraph*]

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

a. the description presents XYZ's transportation management system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. **except for the effects of the matter described in the following paragraph,** the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria.

c. **except for the effects of the matter described in the following paragraph,** the controls stated in the description did operate effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria.

The description states on page XX that application changes are tested prior to their implementation; however, the testing procedures do not include a requirement for scanning application code for known vulnerabilities prior to placing a change into operation. The failure to detect such vulnerabilities may result in the implementation of such vulnerabilities into production. As a result, XYZ's controls were not suitably designed or operating effectively to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on trust services criterion CC8.1, *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.*

3.259 If service organization management is unwilling to modify its assertion to align with the service auditor's opinion, this may have implications for the service auditor's opinion. For example, the service auditor needs to consider whether report users are likely to misunderstand a SOC 2 report that includes management's assertion and the service auditor's opinion when management

and the service auditor have reached and expressed in the same document different conclusions with respect to the description, the suitability of design of controls, or in a type 2 examination, the operating effectiveness of controls. If the service auditor believes it is likely that such a report will be misunderstood by report users, the service auditor may decide to withdraw from the engagement.

Meeting the Requirements of a Process or Control Framework

3.260 When management has included disclosures about how the system components, including processes and controls, addressed requirements of a process or control framework and how the implemented controls met these requirements, the service auditor would consider the adequacy of those disclosures based on DC3 and DC5, respectively. This consideration would be part of the service auditor's evaluation of whether the description is presented in accordance with the description criteria. In addition, the service auditor would consider whether the presentation is misleading within the context of the engagement. For example, if management indicates that a particular control met a requirement of a process or control framework, and the service auditor determined that the control did not meet that requirement, the service auditor would consider whether this misstatement is material.

3.261 Because the process or control framework would likely constitute a portion of the service commitments and system requirements, the service auditor would consider that commitment or requirement in the evaluation of the suitability of design and operating effectiveness of controls.

3.262 If the service organization has not implemented one or more controls required by the process or control framework, the service auditor needs to consider the effect of that exception in evaluating whether there is a deficiency in the design of controls. There may be situations in which the failure to implement one or more controls would have no effect on the service auditor's opinion. The following are situations in which an exception may or may not result in a deficiency in the design of controls:

- If the required control is not relevant to the services provided by the service organization or its system, the exception is unlikely to result in a deficiency in the design of controls.
- If the service auditor determines that the exception is not material to the requirements of the process or control framework or to the achievement of the service organization's service commitments or system requirements, the exception is unlikely to result in a deficiency in the design of controls. For example, if the service organization has received approval from the sponsoring organization to substitute another control for the required control, the exception is unlikely to result in a deficiency in the design of controls.
- If the service auditor determines that the exception is a deficiency in the design of controls, the service auditor should consider the effect of the deficiency on the opinion in accordance with paragraph .60 of AT-C section 205.

SOC 2 Examination That Addresses Additional Criteria (SOC 2+)

3.263 As discussed earlier, when management includes disclosures about how the system components, including processes and controls, addressed requirements of the process or control framework and how the implemented controls met these requirements, these disclosures are considered in the service auditor's evaluation of whether the description is presented in accordance with the description criteria. Procedures to evaluate the disclosures may include the following:

- Comparison of the requirements of the process or control framework with management's description of the processes and controls
- Performance of walk-throughs and other tests of the implementation of the required controls not otherwise covered by the service auditor's procedures
- Inquiries of management about their implementation and monitoring of processes or controls required by the framework
- Inspection of internal audit and third-party reports evaluating the implementation of the process or control framework

3.264 If management has not included such disclosures and the service auditor concludes that the omission of such disclosures results in a material misstatement of the description based on the description criteria, the service auditor should modify the opinion on the description in accordance with paragraph .70 of AT-C section 205. In addition, in accordance with paragraph .61 of AT-C section 205, the service auditor should evaluate, based on the evidence obtained, whether the presentation of the subject matter or assertion is misleading within the context of the engagement. Paragraph .A79 of AT-C section 205 goes on to state that the service auditor may consider whether additional disclosures are necessary to describe the subject matter, assertion, or criteria. In evaluating the description, the service auditor may conclude that disclosures about how system components, including processes and controls, addressed requirements of the process or control framework and how the implemented controls met these requirements are necessary to provide intended users of the report with the information necessary to enable them to understand the system description, management's assertion, or the service auditor's opinion. If so, the service auditor would modify the opinion on the description.

3.265 The service auditor designs and performs procedures to obtain sufficient and appropriate evidence to form an opinion on whether the controls were implemented to meet the requirements of the process or control framework. In most situations, the controls identified by management in the description will include the controls required by the framework. In such situations, no additional procedures may be necessary.

3.266 If the service organization has not implemented one or more controls required by the process or control framework, the service auditor needs to consider the effect of that exception on the service auditor's opinion on whether controls were implemented to meet the requirements of the process or control framework. However, there may be situations in which the failure to implement one or more controls would have no effect on the service auditor's opinion. The following are situations in which an exception may or may not affect the service auditor's opinion:

a. If a required control is not relevant to the services provided by the service organization or its system, the exception is unlikely to be material.

b. If the service auditor determines that the exception is not material to the requirements of the process or control framework, the exception would have no effect on the opinion. For example, if the service organization has received approval from the sponsoring organization to substitute another control for the required control, the exception would be unlikely to be material.

c. If the service auditor determines that the exception is material to the requirements of the process or control framework, the service auditor should consider the effect of the exception on the opinion about whether controls were implemented to meet the requirements of the process or control framework in accordance with paragraph .60 of AT-C section 205.

d. If the service auditor has identified a material deficiency in the suitability of the design of the controls to achieve the service organization's service commitments and system requirements, the service auditor should modify the opinion on the design of controls based on the trust services criteria in accordance with paragraph .70 of AT-C section 205.

3.267 As discussed in paragraph 3.232, the service auditor should request written representations in the form of a letter from the responsible party. Because a SOC 2+ engagement includes additional matters (as discussed in paragraph 1.70) and additional assertions (as discussed in paragraph 2.189), additional representations may be appropriate. For example, in addition to asserting that management has disclosed to the service auditor all deficiencies in internal control relevant to the SOC 2 examination of which it is aware, the service auditor may determine that it is appropriate for management to assert that it has disclosed to the service auditor any failure of the controls required by the process or control framework to operate as required.

Chapter 4

Forming the Opinion and Preparing the Service Auditor's Report

This chapter describes the service auditor's responsibilities for forming an opinion and preparing a SOC 2 report. The chapter primarily focuses on the reporting elements of a service auditor's type 2 report and modifications of that report that may be necessary in certain circumstances. It also describes situations in which a SOC 3 report may be appropriate and provides guidance for preparing a SOC 3 report.

Responsibilities of the Service Auditor

4.01 The service auditor's responsibilities in a SOC 2 examination include forming an opinion and issuing a report expressing that opinion. A type 2 report includes the service auditor's opinion about whether (*a*) the description presents the system that was designed and implemented throughout the period in accordance with the description criteria, (*b*) the controls were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and (*c*) the controls operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

4.02 As discussed in chapter 1, "Introduction and Background," the service auditor may express an unmodified opinion on the description only if evidence obtained supports a conclusion that the description is free from material misstatement. When considering the materiality of identified description misstatements, if any, on the description, the service auditor considers the common information needs of intended users whose decisions are based on the subject matter taken as a whole. Accordingly, it is reasonable for the service auditor to consider whether the description, taken as a whole, is presented in accordance with the description criteria when forming the service auditor's opinion. Although an identified description misstatement that results in the failure to meet one or more description criteria may be indicative of a material misstatement, ultimately the service auditor's opinion focuses on the effect of the misstatement on the description of the system (that is, whether the misstatement could affect decisions made by intended users based on the subject matter taken as a whole).

4.03 The service auditor may issue an unmodified opinion on controls only if evidence obtained supports a conclusion that controls are suitably designed and, in a type 2 examination, operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. Although one or more control deficiencies may be identified during tests of controls, ultimately, the service auditor's opinion on controls focuses on the effect of the control deficiencies on the system's ability to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria.

4.04 Issuing the service auditor's type 2 report involves preparing the following:

- A written description of the tests of controls performed by the service auditor and the results of those tests
- The service auditor's report, including each of the reporting elements for a type 2 report identified in paragraph 4.35, and any modifications to the report that the service auditor determines are necessary in the circumstances

4.05 This chapter focuses on forming an opinion and preparing a type 2 report. Although this chapter does not provide detailed guidance for preparing a type 1 report, paragraphs 4.110–.111 briefly discuss differences between a type 1 report and a type 2 report. Appendix D, "Illustrative Management Assertion and Service Auditor's Report for a Type 1 Examination," presents an illustrative type 1 report.

Forming the Service Auditor's Opinion

4.06 When forming an opinion in accordance with paragraph .60 of AT-C section 205, *Assertion-Based Examination Engagements*,[1] the service auditor should evaluate

a. the service auditor's conclusion about the sufficiency and appropriateness of evidence and

b. whether uncorrected description misstatements are material, individually or in the aggregate.

4.07 Chapter 3, "Performing the SOC 2 Examination," discusses determining whether uncorrected misstatements are material, individually or in the aggregate.

Concluding on the Sufficiency and Appropriateness of Evidence

4.08 Sufficient appropriate evidence is primarily obtained from procedures performed during the engagement. It may, however, also include information obtained from other sources, such as previous engagements (provided the service auditor has determined whether changes have occurred since the previous engagement that may affect the relevance of information obtained from the previous engagement to the current engagement) or a firm's quality control procedures for client acceptance and continuance. Rates of error in testing may be used in assessing the risks of material misstatement and determining the extent of testing.

4.09 The sufficiency and appropriateness of evidence are interrelated. Sufficiency of evidence is the measure of the quantity of evidence. The quantity of the evidence needed is affected by the risks of material misstatement and by the quality of such evidence.

4.10 Appropriateness of evidence is the measure of the quality of evidence, that is, its relevance and reliability in providing support for the service auditor's opinions. The reliability of evidence is influenced by its source and nature and is dependent on the individual circumstances under which it is obtained. Generalizations about the reliability of various kinds of evidence can be made; however,

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

such generalizations are subject to important exceptions. Even when evidence is obtained from sources external to the responsible party, circumstances may exist that could affect its reliability. For example, evidence obtained from an independent external source may not be reliable if the source is not knowledgeable. Recognizing that exceptions may exist, the following generalizations about the reliability of evidence may be useful:

- Evidence is more reliable when it is obtained from independent sources outside the appropriate party (or parties).
- Evidence that is generated internally is more reliable when the related controls are effective.
- Evidence obtained directly by the service auditor (for example, observation of the application of a control) is more reliable than evidence obtained indirectly or by inference (for example, inquiry about the application of a control).
- Evidence is more reliable when it exists in documentary form, whether paper, electronic, or other media (for example, a contemporaneously written record of a meeting is ordinarily more reliable than a subsequent oral representation of what was discussed).
- Evidence provided by original documents is more reliable than evidence provided by photocopies, facsimiles, or documents that have been filmed, digitized, or otherwise transformed into electronic form, the reliability of which may depend on the controls over their preparation and maintenance.

4.11 Evidence obtained from multiple sources or from sources of a different nature ordinarily provides more assurance than evidence from items considered individually. In addition, obtaining evidence from different sources or of a different nature may indicate that an individual item of evidence is not reliable. For example, corroborating information obtained from a source that is independent of the responsible party may increase the assurance the service auditor obtains from a representation from the responsible party. Conversely, when evidence obtained from one source is inconsistent with that obtained from another, the service auditor should determine what additional procedures are necessary to resolve the inconsistency in accordance with paragraph .24 of AT-C section 205.

4.12 Whether sufficient appropriate evidence has been obtained on which to base the service auditor's opinion is a matter of professional judgment. The service auditor's professional judgment regarding what constitutes appropriate sufficient evidence is influenced by factors such as the following:

- The significance of a potential description misstatement or deficiency and the likelihood that it will have a material effect, individually or when aggregated with other potential description misstatements and deficiencies, on the presentation of the description of the service organization's system, on the suitability of design of controls, or on the effectiveness of controls
- The effectiveness of management's responses to address the known risks
- The experience gained during previous consulting or examination engagements with respect to similar potential description misstatements and deficiencies

- The results of procedures performed, including whether such procedures identified specific description misstatements and deficiencies
- The source and reliability of the available information
- The persuasiveness of the evidence
- The service auditor's understanding of the service organization (and any subservice organizations, when the inclusive method is used) and its environment

Considering Uncorrected Description Misstatements and Control Deficiencies

4.13 A SOC 2 examination is a cumulative and iterative process. As the service auditor performs planned procedures, evidence obtained may cause the service auditor to alter the nature, timing, or extent of other planned procedures, as discussed in the following list:

- The nature and number of identified description misstatements and control deficiencies may change the service auditor's professional judgment about the reliability of sources of information. For example, the service auditor may have discovered that management was unaware that detection tools were not implemented over a server that was a component of the system under examination. In response, the service auditor considered the need for additional testing to evaluate whether controls over the server were effective and whether detection measures over other system components were effective to mitigate the risk or detect incidents related to the server.
- Identified discrepancies in relevant information, or conflicting or missing evidence, may cause the service auditor to determine additional procedures are necessary to resolve the discrepancies.
- Procedures performed toward the end of the engagement may indicate a previously unrecognized risk of material misstatement, which may cause the service auditor to reevaluate planned procedures. As an example, assume that, while testing management's procedures to mitigate security incidents, a service auditor becomes aware of a deficiency in the design of a control that prevents unauthorized access. The service auditor may determine that additional testing is needed to evaluate whether there are other suitably designed controls that operated effectively to mitigate the risk of unauthorized access addressed by the deficient control. In such circumstances, the service auditor may need to reevaluate the planned procedures.

4.14 The service auditor also evaluates the effect of uncorrected description misstatements or control deficiencies on the engagement and on the opinion. The service auditor may conclude that additional appropriate evidence is required to form a conclusion about the description, suitability of design of controls, or control effectiveness. In that case, the service auditor should design and perform additional procedures to obtain sufficient appropriate evidence in accordance with paragraph .47 of AT-C section 205.

4.15 If the service auditor concludes, based on the evidence obtained, that the description is not presented in accordance with the description criteria or

that the controls were not suitably designed or operating effectively, the opinion should be modified to express a qualified or adverse opinion in accordance with paragraph .70 of AT-C section 205. Reporting when the service auditor decides to modify the opinion is discussed beginning in paragraph 4.47.

Expressing an Opinion on Each of the Subject Matters in the SOC 2 Examination

4.16 As discussed in paragraph 4.01, the service auditor expresses an opinion on three distinct but complementary subject matters in a SOC 2 examination: (1) whether the description of the system is presented in accordance with the description criteria;[2] (2) whether controls were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and (3) in a type 2 examination, whether controls operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Depending on the circumstances, the service auditor's opinion may be different for each subject matter.

4.17 When the service auditor concludes that an opinion modification on one of the subject matters is appropriate, a relevant consideration is the effect of that conclusion on the opinion on the other subject matters. Consider the following examples:

- A service auditor determines that an adverse opinion on the description is appropriate because the description discloses that certain controls have been implemented, but such controls were not implemented and management refuses to amend the description to correct the misstatement. Because such controls are necessary for the service organization's controls to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria, an adverse opinion on the suitability of the design and operating effectiveness of the controls is also appropriate.
- A service auditor expresses a qualified opinion on the description because management failed to disclose one or more principal service commitments. The service auditor may conclude that, even though the service commitments were not disclosed, the controls were suitably designed and operating effectively during the period covered by the examination and a qualification of the opinion on the suitability of design and operating effectiveness of controls is not necessary.
- A service auditor expresses a qualified opinion on the suitability of the design of the controls because, as designed, controls do not provide reasonable assurance that the service organization would achieve its service commitments and system requirements based

[2] The description criteria presented in this document (the 2018 description criteria) have been designed to be used in conjunction with the 2017 trust services criteria set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, in AICPA *Trust Services Criteria* in a SOC 2 report. The 2018 description criteria are codified in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022),* in AICPA *Description Criteria* and include points of focus that were revised in 2022.

on the applicable trust services criteria, even if the controls operated effectively. The service auditor would also conclude that the qualification applies to the operating effectiveness of the controls.

- A service auditor disclaims an opinion on the description because of a lack of sufficient appropriate evidence about whether controls were implemented during the specified period. In this situation, the lack of evidence also leads the service auditor to disclaim an opinion on the suitability of the design and operating effectiveness of controls.

Describing Tests of Controls and the Results of Tests in a Type 2 Report

4.18 The service auditor's report for a type 2 examination, as discussed in this guide, contains a reference to a description of the service auditor's tests of controls and results thereof. Such information is necessary to enable users to better understand the effects of identified deviations and deficiencies on users' systems and controls. It also enables users to better understand the service auditor's opinion on the suitability of design and the effectiveness of controls. Table 4-1 summarizes the information to be included in the SOC 2 report when describing the service auditor's tests of controls and results.

Table 4-1

Information to Be Included When Describing Tests of Controls and Results

Information to Be Described	*If No Deviations Were Identified*	*If Deviations Were Identified*
The controls that were tested	Yes	Yes
Whether the items tested represent all or a selection of the items in the population (that is, clarify whether a sample or the full population was selected)	Yes	Yes
The nature of the tests performed in sufficient detail to enable report users to determine the effect of such tests on their risk assessments	Yes	Yes
The number of items tested	No	Yes
The number and nature of the deviations	N/A	Yes
Causative factors	N/A	Optional
A description of the internal auditor's work and of the service auditor's procedures with respect to that work, if the work of the internal audit function has been used in tests of controls to obtain evidence (see paragraph 4.26)	Optional	Optional

4.19 Because the service auditor does not have the ability to determine whether a deviation will have significance to an individual report user, the concept of materiality would generally not be applied when determining whether a testing exception is a deviation to be reported in the results of tests of controls. Consequently, the service auditor's description of the tests of controls and results would include all identified deviations. If the service auditor has not identified any deviations, the service auditor may document those results with a phrase such as "No exceptions noted" or "No deviations noted." An example of a description of tests of controls in which no deviations have been identified can be found in the illustrative description on the AICPA website.

4.20 The description of tests of controls need not be a duplication of the service auditor's detailed audit program, which might make the report too voluminous for report users and provide more than the required level of detail. The description of tests of controls is intended to provide report users with sufficient detail about the nature and extent of the service auditor's procedures to enable users to understand the effect of the tests on users' risk assessments. In table 4-2, "Relevant Information When Describing Tests of Controls," the first column identifies in some detail the information to be included in the service auditor's description of tests of controls and results, and the second column provides an example of the disclosure.

Table 4-2

Relevant Information When Describing Tests of Controls

Relevant Information When Describing a Test of Controls	*Example*
The nature of the tests performed (inquiry, observation, inspection, or reperformance) included in sufficient detail to enable report users to determine the effect on their risk assessments	Observed the existence of signage in the facility lobby directing personnel to contact the Ethics Help Line to report...
The document or electronic file to which the service auditor referred to obtain evidence	Inspected the Information Security Office Charter to determine that • the roles and responsibilities of members of the Information Security Office are defined. • the reporting relationship of the Chief Information Security Officer to service organization leadership is defined.

(continued)

Relevant Information When Describing Tests of Controls — *continued*

Relevant Information When Describing a Test of Controls	*Example*
The extent of testing, including whether the items tested represent all or a selection of the items in the population	*Example 1:* For a sample of new access requests selected from the system-generated HR listing of newly hired employees, inspected ticket and system access evidence to determine if access was granted or denied based on the service organization's access criteria. *Example 2:* For the full population of employees terminated during the examination period, inspected the related active directory account to determine that it was deactivated within 24 hours of the termination date.
The title and role of service organization personnel to whom inquiries were directed	Inquired of the Data Center Security Officer responsible for ensuring that all visitors are signed in based on government-issued credentials and escorted throughout the facility regarding procedures for visitors...
The documents, files, or other sources from which the tested items were selected	Inspected a sample of terminated employees from a list generated by the human resources system and compared the termination date per the listing to the access card deactivation dates for each terminated employee per the access system...
Any testing performed on information produced by the service organization	Inspected one daily termination report that was generated automatically from the human resources management system and automatically emailed to the facilities manager. Inspected the system script used to generate and email the report to determine whether terminations were accurately and completely included in the report and whether the listing routed automatically to the facilities manager after generation was correct. (This example assumes that underlying IT general controls operated effectively throughout the period and that no changes were made to the associated script or configurations throughout the period.)

Relevant Information When Describing Tests of Controls — *continued*

Relevant Information When Describing a Test of Controls	*Example*
Procedures performed by the service auditor when the design of management's control allows for a tolerable rate of deviation.	Reperformed a sample of new customer setup quality assurance reviews to determine whether management accurately performed the customer setup review.[3] Inspected the monthly quality assurance review results for new customer setup to determine if the results were reviewed each month to verify that accuracy rates were within the tolerable error threshold[4] and that corrective actions were taken, documented, and approved for instances in which the tolerable threshold was exceeded.

If deviations were identified, users are likely to expect disclosures about the number of items tested and the number and nature of the deviations identified even if, based on tests performed, the service auditor concludes that the controls necessary to provide reasonable assurance that the service organization achieved its service commitments and system requirements were effective based on the applicable trust services criteria. In addition, when sampling is used and deviations identified, disclosure of both the sample size and population size are likely to be helpful to users.

4.21 When deviations have been identified, report users may also find it helpful for management to disclose, to the extent known, the causative factors for the deviations, the controls that mitigate the effect of the deviations, corrective actions taken, and other qualitative factors that would assist users in understanding the effects of the deviations on the service organization's ability to achieve its service commitments and system requirements. Such information may be included in the description of the service organization's system or in a separate section of the SOC 2 report to distinguish it from the description. Such a section may be entitled, for example, "Other Information Provided by the Service Organization." Information in such a section is not covered by the service auditor's report (see paragraph 4.101).

4.22 If management's responses to identified deviations are included in the description, they are usually included in the section of the description that

[3] Even if management reports an overall accuracy rate within the tolerable threshold, a deviation identified in the testing of management's quality assurance review would be included in the service auditor's description of tests and results as it relates to the operating effectiveness of this control. Accuracy of the quality assurance information is necessary in determining whether the error rate in the population is within the tolerable threshold.

[4] Exceptions noted by management as part of its monthly quality assurance review would not need to be included in the service auditor's description of tests of controls and results if they were reviewed by management and determined to be within the expected deviation rate based on the design of the control. If the deviation rate is outside of management's expected deviation rate based on the design of the control, this may result in an exception that would be included the service auditor's description of tests of controls and results and require further analysis by management and the service auditor.

lists the applicable control and related criteria. In these circumstances, management's response would be considered part of the description; therefore, a misstatement in management's response may be material to the service auditor's opinion. As a result, the service auditor would generally include management's responses in the evaluation of the description and would perform procedures, if necessary to obtain sufficient appropriate evidence in support of the service auditor's conclusions. Such procedures may include making inquiries of management and others and inspecting documentation. In addition, the service auditor may decide to describe those procedures and results in the description. If the response includes forward-looking information, such as future plans to implement controls or to address deviations, such information ordinarily would be included in the section "Other Information Provided by the Service Organization." Other information that is not covered by the service auditor's report is discussed beginning at paragraph 4.101.

4.23 The following example illustrates the description of tests of controls when deviations have been identified:

> *Trust services criterion CC6.4.* The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
>
> *Example service organization's controls.* Daily, a list of terminated employees is automatically generated from the human resources system and routed to the facilities manager. The facilities manager compares the list of terminated employees to the lists of individuals authorized to enter the building and off-site data storage facilities, deletes the access card accounts for any terminated employees, and logs the completion of this process in the ticketing system.
>
> *Service auditor's tests of controls.* Selected a sample of terminated employees from a list generated by the human resources system and compared the termination date per the list to the date the access card was deactivated for each employee. Obtained one daily termination report that was generated automatically from the human resources management system and automatically emailed to the facilities manager. Obtained the system script used to generate and email the report to determine if terminations are appropriately included in the report and the listing is routed automatically to the facilities manager after generation.
>
> *Results of tests of controls.* For one terminated employee in an initial sample of 25 selected from a population of 451, the employee's physical access security card was not deactivated until 91 days after the employee's last day of work. Subsequently tested an additional sample of 15 terminated employees and found no additional deviations.

Describing Tests and Results When Controls Did Not Operate During the Period

4.24 As discussed in paragraph 3.175, in certain circumstances, the description of the service organization's system may include controls that ordinarily operate during the period covered by the examination but did not operate during that period because the circumstances that warrant the operation of those controls did not occur. For example, an identified security event involving the unauthorized access of confidential information by an entity employee

would not always trigger the operation of all recovery processes and controls (such as restoring systems and data from clean backups and replacing compromised files), particularly if the event did not result in a data loss. In these circumstances, service organization management and the service auditor would do the following:

- Service organization management would continue to include the processes in its description and may indicate that the controls did not operate during the period covered by the examination.
- The service auditor would indicate in the service auditor's description of tests of controls and results that the circumstances that warrant the operation of the controls did not occur during the period covered by the examination and, therefore, no testing was performed.
- The service auditor would also indicate what testing procedures were performed to determine that the circumstances that warrant the operation of the control did not occur.

Describing Tests of Controls and Results When Using the Internal Audit Function

4.25 The service auditor has sole responsibility for the opinion expressed in the service auditor's report, and accordingly, that responsibility is not reduced by the service auditor's use of the work of the internal audit function. Therefore, the service auditor would not refer to the work of the internal audit function in the service auditor's opinion.

4.26 If the work of the internal audit function has been used in tests of controls to obtain evidence, the service auditor may elect to identify which testing procedures presented in the tests of controls section were performed by the internal audit function and describe the service auditor's procedures with respect to that work. (The work of the internal audit function referred to in the previous sentence does not include procedures performed by internal auditors as direct assistance. Such tests are designed by the service auditor and performed under the direction, supervision, and review of the service auditor; therefore, they receive the same scrutiny as if they were performed by the engagement team. In this case, the description of tests of controls and results need not distinguish between procedures performed by members of the internal audit function and procedures performed by the service auditor.)

4.27 When the work of the internal audit function has been used in performing tests of controls, the service auditor's description of that work and of the service auditor's procedures with respect to that work may be presented in several ways. For example, it may be presented by including introductory material in the description of tests of controls that indicates that certain work of the internal audit function was used in performing tests of controls and that describes the service auditor's procedures on that work. Conversely, it may be presented by attributing individual tests to internal audit and describing the service auditor's procedures with respect that work.

4.28 The following are examples of introductory material that may be included in the description of tests of controls and results when the service auditor elects to inform report users that the service auditor has used the work of the internal audit function:

- Throughout the examination period, members of Example Service Organization's internal audit function performed tests of controls related to trust services criterion CC6.1, *The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.* Members of the internal audit function observed the controls being performed by employees, inspected documentation of the performance of the control, and reperformed a sample of control activities. The tests performed by the members of the internal audit function and the results of those tests are presented under the captions "Tests Performed" and "Results of Tests." We reperformed selected tests that had been performed by members of the internal audit function and found no exceptions.
- Members of Example Service Organization's internal audit function performed tests of controls for trust services criterion CC6.1, *The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.* The tests performed by members of the internal audit function included inquiry of employees who performed the control activities, observation of the control being performed at different times during the examination period, reperformance, and examination of the documentation for a sample of requests for system access and a sample of requests for reports. The tests performed by the members of the internal audit function and the results of those tests are presented under the captions "Tests Performed" and "Results of Tests." We tested the work of members of the internal audit function through a combination of independent testing and reperformance and noted no exceptions.

4.29 The following are examples of descriptions of tests of controls and results that identify the tests performed by the internal audit function and attribute that work to them:

Example 1

When withdrawal requests are received, the processing clerk compares the name of the individual requesting the withdrawal to a client-provided list of individuals authorized to make such requests. The processing clerk who performs this control initials the request form to indicate that the comparison has been performed. Requests from individuals whose names are not on the client-provided list are rejected and sent back to the client.

Tests Performed by the Internal Audit Function

- Inquired of the processing clerk responsible for performing the control regarding the procedures performed when a withdrawal request is received.
- Observed the employee performing the control on multiple occasions throughout the examination period.
- For a sample of withdrawals made during the examination period that were selected from the payments register, compared the name on the withdrawal request to the client-provided list of individuals authorized to make such

requests, and determined that the request had been initialed by the processing clerk.

Tests Performed by the Service Auditor

- Inquired of the processing clerk responsible for performing the control regarding the procedures performed when a withdrawal request is received.
- For a sample of items tested by members of the internal audit function, reperformed the test.
- For an additional sample of withdrawals made during the examination period that were selected from the payments register, compared the name on the withdrawal request to the client-provided list of employees authorized to make such requests, and determined that the request had been initialed by the processing clerk.

Results of Tests

- No exceptions noted.

Example 2

When withdrawal requests are received, the processing clerk compares the name of the individual requesting the withdrawal to a client-provided list of employees authorized to make such requests. The clerk performing this control initials the request form or electronic request to indicate that the comparison has been performed. Requests from individuals who are not on the client-provided list are rejected and sent back to the client.

Tests Performed

- Members of the internal audit function inquired of the clerk responsible for performing the control regarding the procedures followed when withdrawal requests are received.
- Members of the internal audit function made multiple observations throughout the examination period of the clerk performing the control.
- For a sample of withdrawals during the examination period that were selected from the payments register, the members of the internal audit function and the service auditor compared the name on the withdrawal request form or electronic request to the client-provided list of individuals authorized to make such requests and determined that the request had been initialed by the processing clerk.
- The service auditor reperformed the testing for a sample of items tested by members of the internal audit function.

Results of Tests

- No exceptions noted.

Describing Tests of the Reliability of Information Produced by the Service Organization

4.30 As discussed in paragraph 3.138, the service auditor should evaluate whether information produced by the service organization is sufficiently reliable for the service auditor's purposes. The service auditor's procedures to

assess the reliability of such information would generally be included in the description of tests of controls and results. The service auditor may

- provide this information in summary form in the description of tests of controls and results.
- identify the individual procedures performed on a control-by-control basis.
- present this information using both of these methods, depending on the nature of the information produced by the service organization (that is, information provided to user entities, information used in the execution of a control, or information provided in response to ad hoc requests from the service auditor).

4.31 One presentation method may be more appropriate than another depending on the circumstances. For example, when the service auditor performs procedures to assess the reliability of information used in the examination or information prepared for use in the operation of a control, including a description of the detailed procedures performed by the service auditor on a control-by-control basis may be more useful than information provided in summary form.

4.32 When the service auditor decides to present the information in summary form, language such as the following may be added as a lead-in to the description of tests of controls and results:

> **Information Produced by the Entity**
>
> For tests of controls requiring the use of information produced by the entity (IPE), including electronic information (for example, controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible — based on the nature of the IPE — to address the completeness, accuracy, and data integrity of the data or reports used:
>
> - Inspected the source of the IPE
> - Inspected the query, script, or parameters used to generate the IPE
> - Tied data between the IPE and the source
> - Inspected the IPE for anomalous gaps in sequence or timing to determine that the data is complete, accurate, and maintains its integrity
>
> For tests of controls requiring management's use of IPE in the execution of the controls (for example, management's monitoring of alerts generated by its intrusion prevention system [IPS]), we performed additional procedures including, but not limited to, inspecting evidence of authorization for users with access to administer and modify IPS configurations, a selection of changes to configurations, and updates applied to the IPS during the examination period. We inspected evidence of management's procedures, as applicable, to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

4.33 When the service auditor decides to provide details about the procedures performed and results thereof, language such as the following may be included in the description of tests of controls and results:

> Observation and inspection procedures were performed related to [*system-generated reports, queries, and listings*] to assess the accuracy and completeness (reliability) of the information [*used in the*

performance of our testing of the controls or used by the service organization in the execution of controls].

Obtained a system-generated listing of terminated employees from the human resources management system and inspected the queries used to generate the listing to determine whether it included the appropriate date-selection criteria and record types for terminated employees.

Preparing the Service Auditor's SOC 2 Report

Elements of the Service Auditor's SOC 2 Report

4.34 AT-C section 205 identifies the elements to be included in a service auditor's examination report. It also provides requirements for adding a paragraph to the report to restrict its use in certain circumstances. Table 4-3, "Elements of a Service Auditor's Type 2 Report," identifies the requirements in paragraphs .63–.65 of AT-C section 205 on which each element of a SOC 2 report is based. Appendix C-1, "Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination (Carved-Out Controls of a Subservice Organization and Complementary Subservice Organization Controls and Complementary User Entity Controls)," presents an illustrative service auditor's type 2 report.

4.35 The "Illustrative Service Auditor's Type 2 Report Language" column of the table illustrates language that would be used in a type 2 report[5] for a service organization that outsources certain aspects of its system to a subservice organization and elects to use the carve-out method for the subservice organization. In addition, the language in that column assumes that complementary user entity controls (CUECs) and complementary subservice organization controls (CSOCs) are required. Language shown in ***boldface italics*** is only included when the service organization uses one or more subservice organizations and there are CUECs and CSOCs.

Table 4-3

Elements of a Service Auditor's Type 2 Report

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
par. .63*a*	A title that includes the word *independent*	The service auditor's report should include a title that includes the word *independent*.	Independent Service Auditor's Report

(continued)

[5] Although the table presents the reporting requirements of a type 2 report, many of the requirements would also apply to a type 1 report. Appendix D, "Illustrative Management Assertion and Service Auditor's Report for a Type 1 Examination," presents an illustrative type 1 report.

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
par. .63*b*	An appropriate addressee as required by the circumstances of the engagement	An appropriate addressee is determined by the circumstances of the engagement. (In most cases, the service auditor is engaged by the service organization and would address the service auditor's report to management of the service organization. However, the service auditor may be engaged by one or more user entities or the board of directors of the service organization and, in such cases, would address and provide the report to the party that engaged the service auditor.)	To: Management of XYZ Service Organization
par. .63*c*	An identification or description of the subject matter or assertion being reported on, including the point in time or period of time to which the measurement or evaluation of the subject matter or assertion relates	AT-C section 205, *Assertion-Based Examination Engagements*, permits a service auditor to report on either management's assertion or directly on the subject matter. In a SOC 2 engagement described in this guide, however, the service auditor reports directly on the subject matters. The report should identify the subject matters of a SOC 2 examination, which generally include the following:	*Scope* We have examined XYZ Service Organization's accompanying description of its [*type or name*] system titled [*insert title of management's description*] throughout the period [*date*] to [*date*] (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System*

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		1. A description of the service organization's system, the function performed by the system, and the period to which the description relates 2. The description criteria used to evaluate the description 3. The applicable trust services criteria used to evaluate whether the controls stated in the description were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved	*in a SOC 2®Report*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period [*date*] to [*date*] to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*.

(continued)

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		If the service organization uses a subservice organization and service organization management has determined that complementary controls at the subservice organization that are suitably designed and operating effectively are necessary, along with controls at the service organization, to achieve the service organization's service commitments or system requirements based on the applicable trust services criteria, the report will generally include the following: 1. A statement that the service organization uses a subservice organization 2. An identification of the types of services or functions provided by the subservice organization	***XYZ uses a subservice organization to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of XYZ's controls. The description does not***

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		3. An indication of whether the controls at the subservice organization are included in the description and in the service auditor's examination[6] 4. If management elects to carve out the subservice organization's controls from the description and from the service auditor's examination, a statement that *a.* the description indicates that complementary subservice organization controls (CSOCs) that are suitably designed and operating effectively are necessary, along with controls at the service organization, to achieve the service	***disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.*** ***The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the***

(continued)

[6] Column 4 illustrates only the service auditor's report language when the subservice organization's controls have been "carved-out" of the description and the service auditor's examination. If service organization management has elected to include such controls in the description and within the scope of the service auditor's examination, the subservice organization is also a responsible party, and additional language should be added to the service auditor's report to refer to its responsibilities. Appendix C-2, "Illustrative Service Organization and Subservice Organization Management Assertions and Service Auditor's Report for a Type 2 Examination (Subservice Organization Presented Using the Inclusive Method and Complementary User Entity Controls)," illustrates a service auditor's report on a type 2 examination in which the inclusive method is used.

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		organization's service commitments and system requirements based on the applicable trust services criteria; *b.* the description presents the types of CSOCs assumed in the design of XYZ's controls;[7] and *c.* the description does not disclose the actual controls at the subservice organization The service auditor is likely to also include a statement that the examination did not include the services provided by the subservice organization and that the service auditor has not evaluated the suitability of the design or operating effectiveness of the CSOCs.	***applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.***

[7] As noted in later portions of columns 3 and 4, the service auditor's opinion is also modified when there are complementary subservice organization controls (CSOCs) and complementary user entity controls (CUECs).

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		5. If service organization management has determined that complementary user entity controls (CUECs) that are suitably designed and operating effectively are necessary, along with controls at the service organization, to achieve one or more of the service organization's service commitments or system requirements based on the applicable trust services criteria, the report will generally include a statement that *a.* the description indicates that CUECs that are suitably designed and operating effectively are necessary, along with controls at the service organization, to achieve the service	

(continued)

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		organization's service commitments and system requirements based on the applicable trust services criteria; *b.* the description presents the service organization's controls, the applicable trust services criteria, and the CUECs assumed in the design of the service organization's controls; *c.* the examination did not include such CUECs and the service auditor has not evaluated the suitability of the design or operating effectiveness of such controls[8]	

[8] As noted in later portions of columns 3 and 4, the service auditor's opinion is also modified when there are CSOCS and CUECs.

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
par. .63*d*	An identification of the criteria against which the subject matter was measured or evaluated	In a SOC 2 examination, the description is evaluated against the *description criteria* and the suitability of design and operating effectiveness of controls are evaluated against the trust services criteria relevant to the categories addressed by the examination (*applicable trust services criteria*). A reference to both sets of criteria should be included in the scope paragraph of the service auditor's report.	[*See scope paragraph of report*]
par. .63*e*	A statement that identifies the responsible party and its responsibility for the subject matter being in accordance with (or based on) the criteria or for its assertion	The report should include an identification of the responsible party[9] and its responsibilities, which generally include statements that service organization management is responsible for the following:	*Service Organization's Responsibilities* XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide

(continued)

[9] As discussed in the preceding footnote, if controls at the subservice organization are included in the description and within the scope of the service auditor's examination, the subservice organization is also a responsible party, and additional language should be added to the service auditor's report to refer to its responsibilities. Appendix C-2 illustrates a service auditor's report on a type 2 examination in which the inclusive method is used.

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		1. The service organization's service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service organization's service commitments and system requirements were achieved 2. Providing the assertion about the description and the suitability of design and operating effectiveness of controls stated therein 3. Preparing the description of the service organization's system and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion 4. Providing the services covered by the description	reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion, titled [*insert the title of the attached management assertion*] (assertion), about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		5. Selecting the applicable trust services criteria addressed by the examination and stating the related controls in the description of the service organization's system 6. Identifying the risks that threaten the achievement of the service organization's service commitments and system requirements	
par. .63*f*	A statement that the practitioner's responsibility is to express an opinion on the subject matter or assertion, based on the practitioner's examination	As noted previously, in a SOC 2 engagement, the service auditor reports directly on the subject matters, not on management's assertion. The report should include a statement that the service auditor is responsible for expressing an opinion on the description and on the suitability and design of controls stated in the description, based on the service auditor's examination.	*Service Auditor's Responsibilities* Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination.

(continued)

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
par. .63*g*	A statement that i. the practitioner's examination was conducted in accordance with attestation standards established by the AICPA ii. those standards require that the practitioner plan and perform the examination to obtain reasonable assurance about whether (1) the subject matter is in accordance with (or based on) the criteria, in all material respects (or equivalent language regarding the subject matter	As noted previously, in a SOC 2 engagement, the service auditor reports directly on the subject matters, not on management's assertion. In applying these requirements, the service auditor generally includes in the report the following statements: 1. The examination was conducted in accordance with attestation standards established by the AICPA. 2. Those standards require that the service auditor plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description presents the system that was designed and implemented throughout the period in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance	Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
	and criteria, such as the language used in the examples in paragraph .A90 of AT-C section 205) or (2) the responsible party's assertion is fairly stated, in all material respects ii. the practitioner believes the evidence the practitioner obtained is sufficient and appropriate to provide a reasonable basis for the practitioner's opinion	that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 3. The service auditor believes the evidence obtained is sufficient and appropriate to provide a reasonable basis for the opinion.	

(continued)

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
par. .63*h*	A description of the nature of an assertion-based examination engagement	In describing the nature of a SOC 2 examination, the service auditor generally indicates that a SOC 2 examination includes the following: 1. Obtaining an understanding of the system and the service organization's service commitments and system requirements 2. Assessing the risks that the description of the service organization's system is not presented in accordance with the description criteria and that the controls were not suitably designed or did not operate effectively 3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria 4. Performing procedures to obtain evidence about whether the controls stated in the description were suitably designed to provide reasonable	An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following: • Obtaining an understanding of the system and the service organization's service commitments and system requirements • Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively • Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria • Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria 5. Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria 6. Evaluating the overall presentation of the description In addition, the service auditor may indicate that the examination also included performing other procedures the service auditor considered necessary in the circumstances.	achieved its service commitments and system requirements based on the applicable trust services criteria • Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria • Evaluating the overall presentation of the description Our examination also included performing such other procedures as we considered necessary in the circumstances.

(continued)

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
par. .63*i*	A statement that the practitioner is required to be independent and to meet the practitioner's other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement	The service auditor's report should include a statement that the service auditor is required to be independent and to meet the service auditor's other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement.	We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.
par. .63*j*	A statement that describes significant inherent limitations, if any, associated with the measurement or evaluation of the subject matter against the criteria	Because controls can only provide reasonable assurance that service commitments and system requirements are achieved, the service auditor should consider including in the report statements such as the following: • A description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.	*Inherent Limitations* The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		• There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. • Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.	Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

(continued)

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
par. .A93	A practitioner may be requested to provide, in a separate section of the practitioner's report, a description of the procedures performed and the results thereof in support of the practitioner's opinion. The addition of procedures performed and the results thereof in a separate section of an assertion-based examination report may increase the potential for the report to be misunderstood when taken out of the context of the knowledge of the requesting parties. This potential for an increase in the risk of misunderstanding may lead the practitioner to add a restricted-use paragraph to the practitioner's report.	The SOC 2 report described in this guide includes a description of the procedures performed and the results of those procedures in the report. For that reason, as discussed beginning in paragraph 4.36, the SOC 2 report is restricted to parties who are likely to understand the report. The elements of the service auditor's description of procedures performed and results thereof are discussed beginning in paragraph 4.18. [*Not illustrated in the right-hand column*]	*Description of Tests of Controls* The specific controls we tested and the nature, timing, and results of those tests are listed in section XX.[10]

[10] The illustrative description on the AICPA website includes additional language that may be useful.

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	***AT-C Section 205 Requirements and Relevant Application Guidance***	***SOC 2 Reporting Elements and Additional Guidance***	***Illustrative Service Auditor's Type 2 Report Language***
par. .63*k*	The practitioner's opinion about whether the subject matter is in accordance with (or based on) the criteria, in all material respects	The service auditor's opinion should be expressed in a statement about whether, in all material respects, 1. the description of the service organization's system presents the system that was designed and implemented throughout the specified period in accordance with the description criteria. 2. the controls stated in the description were suitably designed throughout the specified period to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria if the controls operated effectively throughout the specified period.	*Opinion* In our opinion, in all material respects, *a.* the description presents XYZ's [*name or type*] system that was designed and implemented throughout the period [*date*] to [*date*] in accordance with the description criteria. *b.* the controls stated in the description were suitably designed throughout the period [*date*] to [*date*] to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period ***and if the subservice organization and user entities applied the***

(continued)

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		3. the controls stated in the description operated effectively throughout the specified period to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria. If the application of CUECs or CSOCs is necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, the service auditor should include a statement to that effect in the report to prevent report users from misunderstanding the limitations of the service auditor's opinion. See the discussion of CSOCs beginning in paragraph 2.20 and the discussion of CUECs beginning in paragraph 2.23.	***complementary controls assumed in the design of XYZ's controls throughout that period.*** *c.* the controls stated in the description operated effectively throughout the period [*date*] to [*date*] to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria ***if complementary subservice organization controls and complementary user entity controls assumed in the design of XYZ's controls operated effectively throughout that period.***

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
par. .64*a* par. .65	The practitioner's report should include an alert, in a separate paragraph, that restricts the use of the report if the practitioner determines that the criteria used to evaluate the subject matter are appropriate only for a limited number of parties who either participated in their establishment or can be presumed to have an adequate understanding of the criteria. The alert should *a.* state that the practitioner's report is intended solely for the information and use of the specified parties,	The service auditor's report is usually restricted to those parties who have sufficient knowledge and understanding of particular matters relevant to the service organization and service auditor's examination. Accordingly, the report should include an alert that does the following: 1. States that the service auditor's report, including the description of tests of controls and results, is intended solely for the information and use of the specified parties. 2. Identifies the specified parties for whom use is intended. Often the specified parties will be prospective user entities and business partners of the service organization and practitioners engaged by a user entity or business partner when the SOC 2 report is	*Restricted Use* This report, including the description of tests of controls and results thereof in section XX, is intended solely for the information and use of XYZ, user entities of XYZ's [*type or name*] system during some or all of the period [*date*] to [*date*], business partners of XYZ subject to risks arising from interactions with the [*type or name*] system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following: *a.* The nature of the service provided by the service organization *b.* How the service organization's system interacts with user entities, business partners, subservice

(continued)

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
	b. identify the specified parties for whom use is intended, and *c.* state that the report is not intended to be and should not be used by anyone other than the specified parties.	intended to provide evidence to the practitioner regarding controls operated by the service organization. 3. When others, such as regulators, are intended users, their use of the report is likely to be appropriate only when they have sufficient knowledge and understanding of the following: *a.* The nature of the service provided by the service organization *b.* How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties *c.* Internal control and its limitations *d.* User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services	organizations, and other parties *c.* Internal control and its limitations *d.* ***Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements*** *e.* User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services *f.* The applicable trust services criteria *g.* The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks This report is not intended to be, and

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		e. The applicable trust services criteria *f.* The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks When there are CUECs and CSOCs, the following additional bullet may also be added to this list: *g.* CUECs and CSOCs and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements	should not be, used by anyone other than these specified parties.

(continued)

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		At the service auditor's discretion, the specified parties may be specifically identified in the report. The intended users of a SOC 2 report are discussed beginning in paragraph 1.07. In addition, the report should include a statement that the report is not intended to be and should not be used by anyone other than the specified parties.	
par. .63*l*	The manual or printed signature of the practitioner's firm	The service auditor's report should include the manual or printed signature of the service auditor's firm.	*Service auditor's signature*
par. .63*m*	The city and state where the practitioner's report is issued	The service auditor's report should include the city and state where the service auditor's report is issued.	*City and state where the report is issued*
par. .63*n*	The date of the report (The report should be dated no earlier than the date on which the practitioner has obtained sufficient appropriate evidence on which to base the practitioner's opinion, including evidence that *a.* the attestation documentation has been reviewed;	The service auditor should date the report no earlier than the date on which the service auditor has obtained sufficient appropriate evidence to support the opinion, including evidence that 1. the attestation documentation has been reviewed, 2. the description of the service organization's system has been prepared, and 3. service organization management has provided a written assertion.	*Date of the service auditor's report*

Elements of a Service Auditor's Type 2 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 2 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 2 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
	b. if applicable, the written presentation of the subject matter has been prepared; and *c.* the responsible party has provided a written assertion or, in the circumstances described in paragraph .A72 of AT-C section 205, an oral assertion.)		

Requirement to Restrict the Use of the SOC 2 Report

4.36 A SOC 2 report, as described in this guide, is intended to include a description of the procedures performed by the service auditor and the results of those procedures. According to paragraph .A93 of AT-C section 205, the addition of procedures performed and the results thereof in a separate section of an examination report may increase the potential for that report to be misunderstood when taken out of the context of the knowledge of the requesting parties. For that reason, the service auditor's report includes an alert restricting it to those intended users who are likely to understand it. As discussed in chapter 1, the SOC 2 report has been designed to meet the common information needs of the broad range of potential SOC 2 users. (Table 4-3 also identifies the broad range of specified parties to whom the service auditor's report is ordinarily restricted.) However, nothing precludes the service auditor from restricting the use of the service auditor's report to a smaller group of users.

4.37 Table 4-3 presents the requirements for an alert paragraph from paragraph .65 of AT-C section 205. The service auditor's report should include each of those elements in the alert paragraph.

Reporting When the Service Organization's Design of Controls Assumes Complementary User Entity Controls

4.38 AT-C section 205 does not address the need for additional language in certain situations unique to a SOC 2 examination that may affect report users' understanding of the subject matter and the examination. One of those situations occurs when service organization management assumes, during the

design of the service organization's system controls, that user entities would apply certain controls. Such controls, known as CUECs, must be suitably designed and operating effectively for the service organization to achieve its service commitments and system requirements.

4.39 If there are CUECs, description criterion DC6 requires that fact be disclosed in the description of the service organization's system. Because the service auditor does not examine the controls implemented at user entities, disclosure of that information in the service auditor's report is necessary to inform report users about that limitation on the examination. In addition, the service auditor's report would generally include a statement that the service auditor has not evaluated the suitability of the design or operating effectiveness of CUECs and that the service organization can achieve its service commitments and system requirements based on the applicable trust services criteria stated in the description only if CUECs are suitably designed and operating effectively, along with the related controls at the service organization. Furthermore, the service auditor may wish to include in the restricted-use paragraph the need for specified users to have sufficient knowledge and understanding of the CUECs and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements. Illustrative language related to CUECs is shown in boldface italics in table 4-3.

4.40 Service organization management would also modify its assertion to reflect the modifications to the service auditor's report discussed in the preceding paragraph. The illustrative report in appendix C-1 contains language that may be useful.

Reporting When the Service Organization Carves Out the Controls at a Subservice Organization

4.41 Another situation that affects the subject matter of the SOC 2 examination occurs when a service organization uses a subservice organization and service organization management assumes, in the design of the service organization's system, that the subservice organization would apply certain controls. Such controls, known as CSOCs, must be suitably designed and operating effectively for the service organization to achieve its service commitments and system requirements.

4.42 When using the carve-out method, description criterion DC7 requires service organization management to include in the description certain disclosures about the use of a subservice organization, including the services provided by the subservice organization and the types of CSOCs it is expected to perform. DC7 also requires disclosure of the types of complementary controls that are assumed to be suitably designed and operated effectively at the subservice organization. The description also needs to disclose controls designed to provide reasonable assurance that the service organization's service commitments and system requirements are achieved, which include controls that the service organization uses to monitor the services provided by the subservice organization.

4.43 To inform report users about the potential effect of CSOCs, the service auditor's report would generally contain similar disclosures as those described in the preceding paragraph. In addition, it would generally contain a statement that the service auditor has not evaluated the suitability of the

design or operating effectiveness of CSOCs and that the service organization can achieve its service commitments and system requirements based on the applicable trust services criteria stated in the description only if CSOCs are suitably designed and operating effectively, along with the related controls at the service organization. Furthermore, the service auditor may wish to include in the restricted-use paragraph the need for specified users to have sufficient knowledge and understanding of the CSOCs and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements. Illustrative language related to CSOCs is shown in boldface italics in table 4-3. The illustrative report on the AICPA website contains language that may be useful.

4.44 There may be circumstances in which more detailed information about the specific controls at the subservice organization is necessary to meet the needs of individual users. For example, additional information may be necessary if a service organization has outsourced all of its IT infrastructure to a cloud service provider. To inform users that this information may be available in a SOC 2 report of the subservice organization, the service auditor may consider adding additional language, such as the following, to the inherent limitations paragraph of the service auditor's report:

> The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. ***If individual users determine that detailed information about the actual controls at the subservice organization is necessary to meet those needs, they may request from service organization management the subservice organization's SOC 2 report, if available.***

Expanded Reporting

4.45 Paragraph .A83 of AT-C section 205 notes that the service auditor may choose to issue a report that contains only the required reporting elements described in table 4-3 or may issue a report that expands on or supplements those elements. A description of procedures performed and results of those procedures, described as *additional reporting elements* in paragraph .A83 of AT-C section 205, are expected disclosures in a SOC 2 service auditor's report. The report may also contain information or explanations that are not intended to affect the service auditor's opinion but that may be helpful to users' understanding of the SOC examination. Examples of such explanations include additional details about the terms of the engagement, details of the qualifications and experience of the service auditor and others involved with the engagement, or recommendations to management. In accordance with paragraph .82 of AT-C section 205, such information should be clearly separated from the service auditor's opinion and phrased in a manner that makes clear that it is not intended to detract from the opinion.

Reporting When the Service Auditor Assumes Responsibility for the Work of an Other Practitioner

4.46 When the service auditor assumes responsibility for the work of an other practitioner, the description of tests of controls and results prepared by the other practitioner would be included in the section of the service auditor's

report that includes such information. However, because the service auditor takes responsibility for the work of the other practitioner, the service auditor does not refer to the other practitioner in the service auditor's report.

Modifications to the Service Auditor's Report

4.47 In accordance with paragraph .70 of AT-C section 205, the service auditor should modify the opinion when either of the following circumstances exist and, in the service auditor's professional judgment, the effect of the matter is or may be material:

a. The service auditor is unable to obtain sufficient appropriate evidence to conclude that the subject matter is presented in accordance with (or based on) the criteria, in all material respects.

b. The service auditor concludes, based on evidence obtained, that the subject matter is not presented in accordance with (or based on) the criteria, in all material respects.

4.48 In applying paragraphs .70–.71 of AT-C section 205 to the SOC 2 examination, the service auditor's opinion should be modified and the service auditor's report should include a description of the matters giving rise to the modification if any of the following apply:

a. The service auditor concludes that the description does not present the system designed and implemented throughout the period in accordance with the description criteria, in all material respects.

b. The service auditor concludes that the controls are not suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively, in all material respects.

c. The service auditor concludes that the controls did not operate effectively throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, in all material respects.

d. The service auditor is unable to obtain sufficient appropriate evidence.

4.49 The objective of including a description of each of the matters giving rise to the modification is to enable report users to consider the effects of identified description misstatements, deficiencies, and deviations when making their own risk assessments. Materiality considerations related to the description are discussed beginning in paragraph 3.84, and considerations related to the suitability of design and operating effectiveness of controls are discussed beginning in paragraph 3.186.

4.50 If a modified opinion is appropriate, the service auditor determines whether to issue a qualified opinion, an adverse opinion, or a disclaimer of opinion. As indicated in paragraph .A113 of AT-C section 205, the decision regarding which type of modified opinion is appropriate depends on the following:

a. The nature of the matter giving rise to the modification (that is, whether the subject matter of the engagement is presented in accordance with [or based on] the criteria, in all material respects, or

in the case of an inability to obtain sufficient appropriate evidence, may be materially misstated)

b. The service auditor's professional judgment about the pervasiveness of the effects or possible effects of the matter on the subject matter of the engagement

4.51 When determining the type of modified opinion to be issued, the service auditor evaluates whether identified (*a*) description misstatements (including omissions) or (*b*) deviations in the suitability of the design and operating effectiveness of the controls are material.

4.52 Table 4-4 identifies the type of modified opinion to be issued based on the nature of the matter giving rise to the modification and the service auditor's professional judgment about the materiality and pervasiveness of its effects (or possible effects) on the opinion on the description, the suitability of design of controls, and the operating effectiveness of controls.

Table 4-4

Types of Opinion Modifications

Nature of Matter Giving Rise to the Modification	***Service Auditor's Professional Judgment About the Pervasiveness of the Effects (or Possible Effects) on the Opinion on the Description, on the Suitability of the Design of Controls, and on the Operating Effectiveness of Controls***	
	Material but Not Pervasive	***Material and Pervasive***
Scope limitation. An inability to obtain sufficient appropriate evidence.	Qualified opinion	Disclaimer of opinion
Material misstatements • The description is materially misstated. or • The controls are not suitably designed to provide reasonable assurance that one or more of the service organization's service commitments or system requirements were achieved based on the applicable trust services criteria. or • The controls are not operating effectively to provide reasonable assurance that one or more of the service organization's service commitments or system requirements were achieved based on the applicable trust services criteria.	Qualified opinion	Adverse opinion

4.53 In accordance with paragraph .71 of AT-C section 205, when the service auditor modifies the opinion, a separate paragraph should be included in the service auditor's report that provides a description of the matters giving

rise to the modification. Examples of separate paragraphs that describe the matters giving rise to a modification are provided beginning in paragraph 4.75.

4.54 When determining whether to modify the service auditor's report, the service auditor considers the effect of identified misstatements, individually and in the aggregate, on the description of the service organization's system taken as a whole. The service auditor also considers the effect of identified deficiencies on the suitability of the design and operating effectiveness of the controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria throughout the specified period. Chapter 3 discusses materiality, including the quantitative and qualitative factors the service auditor considers, in further detail.

Qualified Opinion

4.55 The service auditor expresses a qualified opinion in the following circumstances:

- The service auditor, having obtained sufficient appropriate evidence, concludes that description misstatements, either individually or in the aggregate, are material but not pervasive or deficiencies in the design or operation of controls are material but not pervasive.
- The service auditor is unable to obtain sufficient appropriate evidence on which to base the opinion but the service auditor has concluded that the possible effects on the subject matter of undetected description misstatements or deficiencies, if any, could be material but not pervasive to the subject matter.

This section discusses qualifications because of material description misstatements. The section beginning in paragraph 4.63 discusses qualifications because of scope limitations.

4.56 When the service auditor has determined that a qualified opinion is appropriate because of material description misstatements or deficiencies, the service auditor's report would be modified by doing the following:

- Including, in a separate paragraph before the opinion paragraph, a clear explanation of the matters giving rise to the qualified opinion. When the modification is due to a deficiency in control effectiveness, the service auditor usually identifies the effect of the deficiency on the service organization's ability to achieve one or more service commitments and system requirements.
- Stating in the opinion paragraph that, *except for the effects of the matters giving rise to the modification*, the description is presented in accordance with the description criteria and the controls were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, in all material respects.
- Amending the service auditor's responsibility paragraph to state that the service auditor believes that the evidence the service auditor has obtained is sufficient and appropriate to provide a basis for the service auditor's *qualified* opinion.

Adverse Opinion

4.57 Paragraph .74 of AT-C section 205 indicates that a service auditor should issue an adverse opinion when the service auditor concludes that description misstatements, either individually or in the aggregate, are material and pervasive or deficiencies in the design or operation of controls are material and pervasive. Generally, the service auditor would express an adverse opinion in a SOC 2 examination if the description misstatements in the description of the service organization's system or deficiencies in the suitability of the design or operating effectiveness of the controls are material and pervasive throughout the description or prevent the achievement of all or most of the service organization's service commitments and system requirements based on the applicable trust services criteria.

4.58 When determining whether a material description misstatement or deficiency is likely to have a pervasive effect on the description based on the description criteria or on the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria, paragraph .A115 of AT-C section 205 notes that the term *pervasive* describes the effects on the subject matter of misstatements or the possible effects on the subject matter of misstatements, if any, that are undetected due to an inability to obtain sufficient appropriate evidence. Based on that guidance, pervasive effects in a SOC 2 examination are those that, in the service auditor's professional judgment, are

a. not confined to only specific aspects of the description or to the conclusion about the suitability of design and, in a type 2 examination, the operating effectiveness of controls;

b. if so confined, represent or could represent a substantial proportion of the description or conclusions about suitability of design and, in a type 2 examination, the operating effectiveness of controls; or

c. in relation to disclosures, are fundamental to the intended users' understanding of the description or conclusion about the suitability of design and, in a type 2 examination, the operating effectiveness of controls.

4.59 When determining whether a material description misstatement is pervasive, the service auditor may consider the significance of the description criteria that were not met as a result of the misstatement to the description taken as a whole. Such determination may assist the service auditor in evaluating whether the misstatement is isolated to a single aspect of the description or whether it affects a significant portion of the description. For example, management's omission of the use of a subservice organization may affect not only the disclosures required in DC7 regarding subservice organizations, but also disclosures related to the applicable trust services criteria and controls required by DC5. Because a significant portion of the description is affected, the service auditor may conclude that the material description misstatement is pervasive.

4.60 Similarly, when determining if a material deficiency is pervasive, the service auditor may consider the significance of the trust services criteria that were not met as a result of the deficiency to the achievement of the service commitments and system requirements taken as a whole. Such determination may assist the service auditor in evaluating whether the deficiency is isolated

to a single aspect of the system or if it affects multiple aspects. As an example, assume a service organization uses password vaulting to restrict access to accounts with system administrator authorities and to document the users who access those administrative accounts. When performing procedures in the SOC 2 engagement addressing security, confidentiality, and privacy, the service auditor identified the following control deviations:

- The vaulted administrative accounts were frequently accessed by someone using the user ID of a terminated employee.
- The user ID of the terminated employee was used to access administrative accounts frequently and for long periods of time. The use of the terminated employee account originated from outside the boundaries of the service organization's network.
- The administrative account was used to edit system logs to remove tracking of administrative account activities prior to returning administrative control to the vaulting software.
- The system logs did not include evidence of the tampering with the log.

After considering the effect of these deficiencies on the achievement of the service organization's service commitments related to logical access, change management, and other system requirements, the service auditor determined that the material deficiencies were pervasive because of their effect on IT infrastructure integrity, access to data, and change management controls, all of which are critical to the achievement of the service organization's service commitments and system requirements. Accordingly, the service auditor issued an adverse opinion on control effectiveness.

4.61 Other factors that the service auditor may consider when determining whether identified material deficiencies have a pervasive effect on the achievement of the service organization's service commitments and system requirements include the following:

- The effect that entity-level controls have on the operation of other controls. Deficiencies in entity-level controls often have a pervasive effect on the operation of other controls, which may affect the ability of controls to provide reasonable assurance of achieving the service organization's service commitments and system requirements.
- The extent of the use of segmentation across the service organization's networks and systems. The greater the use of segmentation, the less likely it is that deficiencies in the operation of controls in one system will have an effect on the operation of controls in another one.

4.62 When the service auditor determines that it is appropriate to expresses an adverse opinion on the description, the suitability of design, or the operating effectiveness of controls, it would not be appropriate to issue an opinion other than an adverse opinion on the other subject matters. When expressing an adverse opinion, the service auditor should add a separate paragraph to the service auditor's report in accordance with paragraph .71 of AT-C section 205 describing the matters giving rise to the modification and should modify the opinion paragraph of the service auditor's report in accordance with paragraph .75 of AT-C section 205. In the following example, changes to the opinion

paragraph of the service auditor's report are shown in ***boldface italics***; deleted text is shown in ~~strikethrough~~.

> In our opinion, ***because of the significance of the matter(s) referred to in the preceding paragraph,*** in all material respects,
>
> *a.* the description of the [*name or type*] system ***does not*** present the system that was designed and implemented throughout the period [*date*] *to* [*date*] in accordance with the description criteria.
>
> *b.* the controls stated in the description were ***not*** suitably designed throughout the period [*date*] to [*date*] to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria,
>
> *c.* the controls stated in the description ***did not*** operate effectively throughout the period [*date*] to [*date*] to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

In addition, the last sentence of the service auditor's report should be modified in accordance with paragraph .79 of AT-C section 205 to indicate that the evidence obtained is appropriate for the modified opinion expressed, as follows:

> We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our ***adverse*** opinion.

Scope Limitation

4.63 A service auditor may express an unmodified opinion only when the service auditor has conducted the examination in accordance with the attestation standards. If the service auditor has been unable to apply all the procedures considered necessary in the circumstances, the service auditor would not have complied with the attestation standards.

4.64 According to paragraph .A117 of AT-C section 205, a scope limitation may arise from any of the following:

a. Circumstances beyond the control of management. For example, documents that the service auditor considers necessary to inspect were in the custody of a vendor whose services are no longer in use and the documents no longer exist.

b. Circumstances relating to the nature or timing of the service auditor's work. For example, a physical process that the service auditor considers necessary to observe may have occurred before the service auditor's engagement or may not be performed regularly during the examination period. (However, an inability to perform a specific procedure does not constitute a scope limitation if the service auditor is able to obtain sufficient appropriate evidence by performing alternative procedures.)

c. Limitations imposed by management (or the engaging party, if different). For example, management may have imposed a limitation that prevents the service auditor from performing a procedure

that the service auditor considers necessary in the circumstances. Limitations of this kind may have other implications for the engagement, such as for the service auditor's consideration of risks of material misstatement and for engagement acceptance and continuance.

4.65 In accordance with paragraph .72 of AT-C section 205, when there is a scope limitation, the service auditor should modify the opinion appropriately based on the pervasiveness of the effects or possible effects on the description and on the suitability of design and operating effectiveness of controls. According to paragraph .72 of AT-C section 205, the service auditor should express a qualified opinion when the service auditor is unable to obtain sufficient appropriate evidence on which to base the opinion but the service auditor has concluded that the possible effects on the subject matter of undetected description misstatements or deficiencies, if any, could be material but not pervasive to the subject matter. (Disclaiming an opinion because of a scope limitation is discussed beginning in paragraph 4.68.)

4.66 When the service auditor has determined that a qualified opinion is appropriate because of a limitation in the scope of the examination, the service auditor's report would be modified by doing the following:

- Including, in a separate paragraph before the opinion paragraph, a clear explanation of the matters giving rise to the modification
- Stating, in the opinion paragraph, that *except for the possible effects of the matters giving rise to the modification*, the description is presented in accordance with the description criteria and the controls were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, in all material respects
- Amending the service auditor's responsibility paragraph to state that the service auditor believes that the evidence obtained is sufficient and appropriate to provide a basis for the service auditor's *qualified* opinion

4.67 If the service auditor expresses a qualified opinion because of a scope limitation, and also concludes there were material misstatements in the description or material deficiencies in the suitability of design or operating effectiveness of controls, the service auditor should include, in separate paragraphs of the report, a clear explanation of both the scope limitation and the matters that cause the description, suitability of design, or operating effectiveness of controls to be materially misstated in accordance with paragraph .71 of AT-C section 205.

Disclaimer of Opinion

4.68 In accordance with paragraph .77 of AT-C section 205, the service auditor should disclaim an opinion when the service auditor is unable to obtain sufficient appropriate evidence on which to base the opinion and the service auditor concludes that the possible effects on the subject matters of undetected description misstatements, if any, could be both material and pervasive. In such circumstances, the service auditor may also reach a mutual agreement with the engaging party to terminate the engagement or may withdraw from the engagement.

4.69 Paragraph .80 of AT-C section 205 notes the following modifications to the service auditor's report when disclaiming an opinion:

- The first sentence of the service auditor's report should be revised to state, "We were engaged to examine" rather than "We have examined."
- The standards under which the service auditor conducts an examination are identified at the end of the second sentence of the report, rather than in a separate sentence in the second paragraph of the report.
- A separate paragraph of the report should state that, because of the significance of the matters giving rise to the modification, the service auditor has been unable to obtain sufficient appropriate evidence to provide a basis for an opinion, and accordingly, the service auditor does not express an opinion.
- The report should omit statements
  - — indicating the requirements of AICPA standards for the service auditor.
  - — describing the nature of an examination engagement or identifying the procedures performed and the results of those procedures.

4.70 If the service auditor disclaims an opinion and, based on the limited procedures performed, has concluded that (*a*) certain aspects of the description do not present the system designed and implemented in accordance with the description criteria, (*b*) certain controls are not suitably designed, or (*c*) certain controls did not operate effectively, the service auditor should, in accordance with paragraph .81 of AT-C section 205, include in the service auditor's report a separate paragraph containing a clear description of the matters that led the service auditor to those conclusions.

4.71 Other situations in which the service auditor should disclaim an opinion include the following, as noted in paragraphs .85–.86 of AT-C section 205:

- Management refuses to provide a written assertion (after initially agreeing to do so), and law or regulation does not allow the service auditor to withdraw from the engagement (see paragraph 4.73).
- Management refuses to provide a representation reaffirming its written assertion included in or attached to its description or a representation stating that it has provided the service auditor with all relevant information and access agreed to.

4.72 Appendix C-3, "Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation," presents an illustrative report that may be used when the service auditor decides to disclaim an opinion because of a scope limitation due to management's refusal to provide one or more requested written representations.

Management Will Not Provide a Written Assertion but Law or Regulation Does Not Permit the Service Auditor to Withdraw From the Engagement

4.73 Paragraph .84 of AT-C section 205 states that, if service organization management is both the responsible party and the engaging party and refuses

to provide a written assertion, the service auditor is required to withdraw from the engagement. However, if the service auditor is required by law or regulation to accept or continue an engagement to report on controls at a service organization and management refuses to provide a written assertion, paragraph .85 of AT-C section 205 indicates that the service auditor may conduct the engagement and, ultimately, should disclaim an opinion.

4.74 The following is an example of a separate paragraph that might be added to the service auditor's report in that situation:

> Attestation standards established by the AICPA require that we request a written assertion from management of Example Service Organization that its description of its [*type of system*] throughout the period [*date*] to [*date*] is presented in accordance with the description criteria and that the controls stated in the description were suitability designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We requested that assertion, but Example Service Organization management did not provide such an assertion.

Report Paragraphs Describing the Matter Giving Rise to the Modification

Illustrative Separate Paragraphs When There Are Material Misstatements in the Description

4.75 Chapter 3 presents several situations in which the service auditor would generally determine that the description is not presented in accordance with the description criteria, in all material respects. In practice, if the service auditor makes such a determination, the service auditor works with service organization management to make the necessary changes to the description for it to be presented in accordance with the description criteria. If management refuses to amend the description, the service auditor may decide to withdraw from the engagement. In accordance with paragraph .70 of AT-C section 205, if the service auditor decides to continue with the engagement, the service auditor should modify the opinion paragraph of the report.

4.76 Examples of separate paragraphs that would be added to the service auditor's report if management is unwilling to amend a description that is not presented in accordance with the description criteria, in all material respects, are presented beginning at paragraph 4.77.

Description Includes Controls That Have Not Been Implemented

4.77 The following is an example of a separate paragraph that would be added to the service auditor's report when the description includes controls that have not been implemented:

> The accompanying description states that Example Service Organization's system is protected against unauthorized logical access through the use of operator identification numbers and passwords. Based on inquiries of staff personnel and observation of activities, we determined that operator identification numbers and passwords are used in applications A and B but not in application C.

Description Includes Information That Cannot Be Objectively Evaluated

4.78 The following is an example of a separate paragraph that would be added to the service auditor's report when the description of the service organization's system includes subjective information that is not measurable:

> On page XX of the accompanying description, Example Service Organization states that its data analytics system is "the industry's best system" and "is staffed by the most talented IT personnel." Because there are no criteria against which these attributes can be measured, these statements cannot be measured or objectively evaluated within the scope of this examination.

Description Omits Relevant Changes to Controls

4.79 The following is an example of a separate paragraph that would be added to the service auditor's report when the description does not address relevant changes to the service organization's controls:

> The accompanying description states that the information security group monitors and reviews user access to the data analytics application. Inquiries of staff personnel indicate that this control was first implemented on July 1, 20XX, three months after the beginning of the period addressed by this report. Description criterion 9 requires disclosure in the description of relevant details of significant changes to the system during that period.

Description Omits CUECs

4.80 The following is an example of a separate paragraph that would be added to the service auditor's report when the description omits CUECs:

> Example Service Organization has omitted from its description a statement indicating that user entities should have controls in place that limit access to user-defined indexes to authorized individuals. Description criterion 6 requires disclosure of complementary user entity controls when such controls are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Description Omits CSOCs

4.81 The following is an example of a separate paragraph that would be added to the service auditor's report when the description omits CSOCs:

> The description does not disclose that subservice organizations that provide services to Example Service Organization should have controls in place that limit access to user-defined tables to authorized individuals or that complementary subservice organization controls are necessary, in combination with controls at Example Service Organization, to provide reasonable assurance that Example Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Description criterion 7 requires disclosure of such information.

Description Does Not Disclose That Service Organization Uses a Subservice Organization

4.82 The following is an example of a separate paragraph that would be added to the service auditor's report when the service organization has not disclosed the existence of a subservice organization, the functions it performs, and other related matters:

> The description does not indicate that Example Service Organization uses a subservice organization for computer processing. Description criterion 7 requires disclosure of this and other information about the subservice organization when controls at the subservice organization are necessary, in combination with controls at Example Service Organization, to provide reasonable assurance that Example Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Description Includes Information Not Relevant to the Trust Services Category Addressed by the Engagement

4.83 The following is an example of a separate paragraph that would be added to the service auditor's report when the description includes information that is not relevant to the trust services category addressed by the engagement, and the service organization refuses to place the information in a separate section of the report identified as, for example, "Other Information Provided by Example Service Organization," or to exclude it from the description:

> The accompanying description includes the controls Example Service Organization performs when obtaining consent for new uses of personal information to achieve its privacy commitments and system requirements based on the applicable trust services criteria for privacy. Because our examination was limited to the system's controls to provide reasonable assurance that Example Service Organization's availability commitments and system requirements were achieved based on the applicable trust services criteria, we did not examine the suitability of design or operating effectiveness of controls to provide reasonable assurance that Example Service Organization's privacy commitments and system requirements were achieved based on the applicable trust services criteria for privacy. Therefore, such controls should not be included in the description of Example Service Organization's payroll system.

In these circumstances, because management refuses to remove the other information and place it in a separate section of the report, the service auditor may also disclaim an opinion on that information by adding the words "and, accordingly, we express no opinion on them" at the end of that separate paragraph.

Description Omits Applicable Trust Services Criteria

4.84 If service organization management inappropriately omits one or more applicable trust services criteria from the description of the service organization's system, the service auditor would generally request that management include the omitted criteria and related controls. If management refuses to do so, the service auditor should disclaim an opinion or withdraw from the engagement in accordance with paragraph .77 of AT-C section 205.

Other Information Provided by the Service Organization Is Materially Inconsistent With Information in the Description of the Service Organization's System

4.85 The following is an example of a separate paragraph that would be added to the service auditor's report when other information provided by the service organization is materially inconsistent with the information in the description of the service organization's system and the service organization refuses to correct it or remove it from the description:

> The information in section 5, "Other Information Provided by Example Service Organization," that describes the processing of dental claims by Example Service Organization is presented by management of Example Service Organization to provide additional information and is not a part of Example Service Organization's description of its medical claims processing system during the period June 1, 20X0, to May 31, 20X1. Information about Example Service Organization's dental claims processing has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it. However, we noted that information in section 5 indicating that Example Service Organization provides in-house dental claims processing is materially inconsistent with Example Service Organization's description of its medical claims processing system, which states that dental claims processing is outsourced to another organization.

Illustrative Separate Paragraphs: Material Deficiencies in the Suitability of Controls

4.86 Chapter 3 presents several situations in which the service auditor would generally determine that the controls are not suitably designed, in all material respects. Examples of separate paragraphs that should be added to the service auditor's reports in such situations in accordance with paragraph .75 of AT-C section 205 are presented beginning at paragraph 4.87.

Controls Are Not Suitably Designed

4.87 The following is an example of a separate paragraph that would be added to the service auditor's report preceding the opinion paragraph if the service auditor concludes that controls are not suitably designed:

> The accompanying description of ABC Service Organization's system states on page 8 that ABC Service Organization's system supervisor makes changes to the systems only if the changes are authorized, tested, and documented. The procedures, however, do not include a requirement for approval of the change before the change is placed into operation. As a result, controls were not suitably designed or operating effectively throughout the period [*date*] to [*date*] to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Controls Were Not Suitably Designed During a Portion of the Period

4.88 The following is an example of a separate paragraph that would be added to the service auditor's report preceding the opinion paragraph if the service auditor concludes that controls are not suitably designed for a portion of the period under examination:

> The accompanying description of ABC Service Organization's system states on page 8 that ABC Service Organization's system supervisor makes changes to the system only if the changes are authorized, tested, and documented. During the period January 1, 20XX, to March 31, 20XX, however, controls related to proper authorization, testing, and documentation of system changes were not consistently performed. On April 1, 20XX, ABC Service Organization implemented a procedure requiring that all changes be authorized, tested, and documented by the director of application development before being placed into operation. As a result, during the period January 1, 20XX, to March 31, 20XX, the controls were not suitably designed or operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based the applicable trust services criteria.

Scope Limitation Related to Suitability of Design of Controls

4.89 The following is an example of a separate paragraph that would be added to the service auditor's report when the service auditor is unable to obtain sufficient appropriate evidence about the suitability of design of controls:

> Page XX of the accompanying description states that Example Service Organization's [*identify the party who does this*] researches and resolves events logged by the intrusion detection software. Example Service Organization's logging software was replaced on July 15, 20X0, and sufficient appropriate evidence that independent research and resolution were performed prior to July 15, 20X0, was not available. As a result, we were unable to determine whether Example Service Organization's controls were suitably designed and operating effectively during the period January 1 to July 14, 20X0, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Illustrative Separate Paragraphs: Material Deficiencies in the Operating Effectiveness of Controls

4.90 Chapter 3 presents several situations in which the service auditor would determine that the controls are not operating effectively, in all material respects. Examples of separate paragraphs that should be added to the service auditor's reports in such situations, in accordance with paragraph .71 of AT-C section 205, are presented beginning at paragraph 4.92.

4.91 The service auditor may conclude that controls are suitably designed but are not operating effectively. The following is an example of a separate paragraph that should be added to the service auditor's report when the service auditor determines that controls are not operating effectively:

> ABC Service Organization states in the description of its system that the director of IT may approve emergency changes to the system without receiving a written request for such changes if the changes are documented within 48 hours after implementation into production. However, as noted on page 155 of the description of tests of controls and the results thereof, controls related to the authorization of emergency changes were not consistently performed and, therefore, were not operating effectively throughout the period [*date*] to [*date*]. As a result, controls did not provide reasonable

assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Controls Were Not Operating Effectively During a Portion of the Period to Achieve the Service Commitments and System Requirements

4.92 The following is an example of a separate paragraph that would be added to the service auditor's report when controls were not operating effectively to achieve one or more service commitments and system requirements for a portion of the report period (assumed to be January 1, 20X1, to March 31, 20X1, in this example):

> The accompanying description of ABC Service Organization's system states on page 8 that ABC Service Organization's system supervisor makes changes to the system only if the changes are authorized, tested, and documented. However, as noted in section 4, controls related to proper authorization of system changes were not consistently performed during the period January 1, 20X1, to March 31, 20X1. As a result, during the period January 1, 20X1, to March 31, 20X1, the controls were not operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based the applicable trust services criteria.

Scope Limitation Related to Operating Effectiveness of Controls

4.93 The following is an example of a separate paragraph that should be added to the service auditor's report if the service auditor is unable to obtain sufficient appropriate evidence regarding the operating effectiveness of controls:

> Example Service Organization states in its description of its [*type of system*] that it has automated controls in place to log and track security incidents for research and resolution. However, electronic records of the performance of this control for the period January 1, 20X1, to July 31, 20X1, were deleted because of a computer processing error, and therefore, tests of the operating effectiveness of this control could not be performed for that period. Consequently, we were unable to determine whether the service organization's controls operated effectively during the period January 1, 20X1, to July 31, 20X1, to provide reasonable assurance that its service commitments and system requirements were achieved based on trust services criterion CC6.1, *The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.*

Other Matters Related to the Service Auditor's Report

Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs

4.94 The service auditor may consider it necessary to draw users' attention to the following:

- A matter or matters appropriately presented or disclosed by management's description, assertion, or other information section that, in the service auditor's professional judgment, are of such

importance that they are fundamental to users' understanding of the system (emphasis-of-matter paragraph)

- A matter or matters other than those presented or disclosed by management that are relevant to users' understanding of a SOC 2 engagement, the service auditor's responsibilities, or the service auditor's report (other-matter paragraph)

4.95 The service auditor may draw users' attention to such matters by including an emphasis-of-matter paragraph or other-matter paragraph, as applicable, in the service auditor's report. Because paragraphs emphasizing matters such as those in the preceding paragraph are not intended to detract from the service auditor's opinion on the subject matter, paragraph .82 of AT-C section 205 indicates that emphasis-of-matter paragraphs should be segregated from paragraphs that relate to the service auditor's opinion on the subject matter or any other reporting responsibilities and should be worded in a way that makes it clear that the paragraph is not intended to detract from the opinion.

4.96 The service auditor may adapt and apply the guidance in AU-C section 706, *Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs in the Independent Auditor's Report*.[11] The following is an example of an emphasis-of-matter paragraph for a situation in which the service organization experienced a significant operating disruption after the examination period:

> As described on page X of "Other Information Provided by Example Service Organization," after the period covered by the examination, Example Service Organization's data center system was flooded and rendered inoperable for a period of two weeks by a severe storm in January, 20XX.

Distribution of the Report by Management

4.97 When engaged by the service organization, the service auditor provides the report to management of the service organization, and management distributes the report to the parties to whom use of the report is restricted. A service auditor is not responsible for controlling a client's distribution of a restricted-use report.

4.98 In some cases, however, service organization management may not be the engaging party (for example, if the service auditor is engaged by one or more user entities). In that case, the service auditor provides the report only to the party that engaged the service auditor.

4.99 When establishing the terms of the engagement, the service auditor's understanding with the engaging party may include the fact that the use of the SOC 2 report will be restricted to the parties identified in the report. In addition, it is good practice for the service auditor to inform the engaging party that restricted-use reports are not intended for distribution to unspecified parties. The service auditor may obtain from the engaging party an agreement that the engaging party and the specified parties will not distribute the report to parties other than those identified in the report.

---

[11] All AU-C sections can be found in AICPA *Professional Standards*.

Service Auditor's Recommendations for Improving Controls

4.100 Although it is not the objective of a service auditor's engagement, a service auditor may develop recommendations to improve a service organization's controls. The service auditor and service organization management agree on whether and how such recommendations will be communicated. Typically, the service auditor includes this information in a separate written communication provided only to service organization management.

Other Information Not Covered by the Service Auditor's Report

4.101 Service organization management may wish to communicate to report users information that is beyond the scope of the engagement. Such information may be prepared by service organization management or by another party. For example, service organization management may want to include other information, such as the following, in the SOC 2 report:

- 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
- Qualitative information, such as marketing claims, that may not be objectively measurable
- Responses from management to deviations identified by the service auditor, 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 that may be of interest to report users
- Information relating to compliance with a process or control framework, such as a mapping of controls to the framework, when management has not identified compliance with such a framework as a principal service commitment or system requirement. (Paragraph 4.113 discusses reporting on process or control frameworks when they have been identified as principal service commitments or system requirements).

4.102 Generally, such other information is presented in a separate section of the 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 the procedures outlined in paragraph 4.104 on the other information.

4.103 If service organization management wishes to include its responses to deviations in tests of controls in the description of the service organization's system rather than in the section of the report containing information that is not covered by the service auditor's report, such responses are usually included along with the description of the applicable control and related trust services criteria. In that case, the service auditor would determine through inquiries, in combination with other procedures, whether there is evidence supporting the action described by management in its response.

4.104 Paragraph .58 of AT-C section 205 states that the service auditor should read the other information to identify material inconsistencies, if any, with the subject matter, assertion, or report. If, upon reading the other information, the service auditor believes that either of the following applies, the service auditor should discuss the matter with service organization management and take further action as appropriate:

a. There are material inconsistencies between the other information and the description of the service organization's system, management's assertion, or the service auditor's report.

b. A material misstatement of fact exists in the other information, the description of the service organization's system, management's assertion, or the service auditor's report. (Other information may bring to light a material misstatement of fact in the description, assertion, or in the service auditor's report that the service auditor did not identify when evaluating whether

i. the description presents the system that was designed and implemented throughout the period in accordance with the description criteria,

ii. controls were suitably designed, or

iii. controls were operating effectively.)

4.105 If management refuses to correct or delete the other information containing a material inconsistency or a material misstatement of fact, paragraph .A73 of AT-C section 205 identifies the following examples of further actions the service auditor may take:

- Requesting that management consult with a qualified third party, such as the appropriate party's legal counsel
- Obtaining legal advice about the consequences of different courses of action
- If required or permissible, communicating with third parties (for example, a regulator)
- Describing the material inconsistency in the service auditor's report
- Withdrawing from the engagement when withdrawal is possible under applicable laws and regulations

4.106 The following is an example of a separate paragraph that would be added to the service auditor's report to identify other information provided by the service organization and to disclaim an opinion on it:

> The information attached to the description titled "Other Information Provided by Example Service Organization" is presented by Example Service Organization management to describe the service organization's medical billing system and is not a part of the service

organization's description of its medical records management system made available to user entities during the period June 1, 20X0, to May 31, 20X1. Information about Example Service Organization's medical billing system has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

4.107 Paragraph 4.85 presents an illustrative separate paragraph that would be added to the service auditor's report when the description includes information that is materially inconsistent with other information contained in the SOC 2 report and management refuses to remove it from the description.

Illustrative Type 2 Reports

4.108 Although this guide specifies the information to be included in a description of a service organization's system, it is not specific about the format for a SOC 2 report. Service organizations and service auditors may organize and present the required information in a variety of formats. An illustrative description of the system is available on the AICPA website and illustrative assertions and service auditor's reports are available in appendix C.

4.109 Appendix C contains the following illustrative type 2 reports:

- Appendix C-1, "Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination (Carved-Out Controls of a Subservice Organization and Complementary Subservice Organization Controls and Complementary User Entity Controls)"
- Appendix C-2, "Illustrative Service Organization and Subservice Organization Management Assertions and Service Auditor's Report for a Type 2 Examination (Subservice Organization Presented Using the Inclusive Method and Complementary User Entity Controls)"
- Appendix C-3, "Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation"

Headings in those illustrative reports are optional.

Preparing a Type 1 Report

4.110 When the service auditor has been engaged to perform a type 1 examination, certain of the elements in table 4-3 would be tailored to refer specifically to the subject matters addressed in that examination. For instance, among other things, all references to management's assertion and the service auditor's opinion would be revised to refer only to the following:

a. The description of the [*name or type*] system presents the system that was designed and implemented as of [*date*] in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of [*date*] to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively as of [*date*].

4.111 In a type 1 examination, the service auditor does not express an opinion about whether the controls operated effectively. Accordingly, the type 1

report would also not include a description of the service auditor's tests of controls and the results thereof.

4.112 Appendix D presents an illustrative type 1 report. Headings in that illustrative report are optional.

Meeting the Requirements of a Process or Control Framework

4.113 When the description includes information about how the service organization's controls met the requirements of a process or control framework, report users may make assumptions about the service auditor's responsibilities for that information. For that reason, the service auditor may decide to add an emphasis-of-matter paragraph to the service auditor's report drawing attention to the information about the process or control framework and clarifying the service auditor's responsibility for it. The following illustrates a paragraph that might be added, after the scope paragraph of the service auditor's report, to clarify the service auditor's responsibility for such information:

> Management has identified, in the system description, a principal service commitment and related system requirements to implement controls to address the requirements of ABC framework. Accordingly, management has also included in the description information about how XYZ Service Organization's implemented controls address the requirements of that framework. Management has not, however, engaged us to express an opinion on whether XYZ Service Organization implemented controls that met the requirements of ABC Framework and, accordingly, we express no such opinion.

SOC 2 Examination That Addresses Additional Criteria (SOC 2+)

4.114 In accordance with paragraph .63 of AT-C section 205, in a SOC 2+ examination, the service auditor should modify the scope and opinion paragraphs of the report to specifically address the controls implemented to meet the requirements of the process or control framework. The service auditor should also modify the management's responsibility and service auditor's responsibility paragraphs to address the additional controls.

4.115 In certain cases, the sponsoring organization that developed the process or control framework may also be an intended user. In such instances, the service auditor includes the sponsoring organization in the alert that restricts use of the report.

4.116 If the additional criteria are only appropriate for a particular subset of intended users of the SOC 2 report, the service auditor may conclude that the alert should restrict use of the report to that subset of users in accordance with paragraph .64 of AT-C section 205.

4.117 The service auditor may also consider whether to include an emphasis-of-matter paragraph to provide report users with additional information about the process or control framework.

4.118 Appendix E, "Illustrative Service Auditor's Report for a SOC 2+ Examination," presents an illustrative SOC 2+ service auditor's report.

Forming the Opinion and Preparing a SOC 3 Report

Elements of the SOC 3 Report

4.119 As discussed in chapter 1, the SOC 3 report was designed as a general-purpose report. Because the intended users of a SOC 3 report are different than the intended users of a SOC 2 report, there are some distinct differences between the contents of a SOC 3 report and a SOC 2 report.

4.120 The elements of a SOC 3 report are as follows:

a. An assertion by service organization management about whether the controls were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. As part of that assertion, management also describes the boundaries of the system and the service organization's principal service commitments and system requirements.

b. An opinion by the service auditor on management's assertion about whether controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

These elements are discussed further in the following paragraphs.

Management's Assertion

4.121 As discussed in the preceding paragraph, as part of its assertion, management describes the boundaries of the system and the principal service commitments and system requirements. The boundaries of the system addressed by the examination need to be clearly understood, defined, and communicated to report users. Report users need that information to enable them to understand the scope of the service auditor's examination. They also need information about the service organization's principal service commitments and system requirements to enable them to understand how the effectiveness of controls was evaluated based on the applicable trust services criteria.

4.122 Disclosures about the boundaries of the system would typically include matters such as the following:

- The use of CUECs and CSOCs, when those are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments or system requirements were achieved based on the applicable trust services criteria
- The use of subservice organizations, including whether management has elected to use the inclusive or carve-out method with respect to the services provided by subservice organizations
- Any other information that is likely to assist report users in understanding the limitations on the service auditor's examination and opinion

4.123 Disclosures about the boundaries of the system and the principal service commitments and system requirements ordinarily would be included in management's assertion or in an exhibit thereto. If management does not include those disclosures in its assertion (or in an exhibit thereto), the service

auditor would ordinarily conclude that the use of the service auditor's report would need to be restricted to intended users who have sufficient knowledge of the boundaries of the system and the service organization's principal service commitments and system requirements. In most situations, this would be limited to the service organization itself and its board of directors.

Service Auditor's Opinion

4.124 In a SOC 3 report, the service auditor expresses an opinion on management's assertion that the controls within the system were effective throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, in all material respects.[12]

Elements of the Service Auditor's Report

4.125 Similar to a SOC 2 report, the elements included in the service auditor's SOC 3 report are based on the requirements in AT-C section 205. Table 4-5 identifies the requirements in paragraphs .63–.64 of AT-C section 205 on which each element of a service auditor's SOC 3 report is based.

Table 4-5

Elements of a Service Auditor's SOC 3 Report

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
par. .63*a*	A title that includes the word *independent*	The service auditor's report should include a title that includes the word *independent.*	Independent Service Auditor's Report
par. .63*b*	An appropriate addressee as required by the circumstances of the engagement	An appropriate addressee is determined by the circumstances of the engagement. (In most cases, the service auditor is engaged by the service organization and would address the service auditor's report to management of the service organization. However, the service auditor may be engaged by one or more user	To: Management of XYZ Service Organization

[12] Although the service auditor expresses an opinion on the assertion in a SOC 3 examination, as described in this guide, paragraph .67 of AT-C section 205, *Assertion-Based Examination Engagements*, does permit a service auditor to express an opinion directly on the effectiveness of the controls within the system, if the service auditor so chooses.

Elements of a Service Auditor's SOC 3 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
		entities or the board of directors of the service organization and, in such cases, would address and provide the report to the party that engaged the service auditor.)	
par. .63*c*	An identification or description of the subject matter or assertion being reported on, including the point in time or period of time to which the measurement or evaluation of the subject matter or assertion relates	In a SOC 2 examination, the service auditor reports directly on the subject matter; however, in a SOC 3 examination, the service auditor reports on management's assertion. The report should identify management's assertion about whether the controls within the service organization's system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*	*Scope* We have examined XYZ Service Organization's (XYZ's) accompanying assertion, titled "Assertion of XYZ Service Organization Management" (assertion),[13] that the controls within XYZ's medical claims processing system (system) were effective throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022).*

(continued)

[13] As part of its assertion, management also describes the boundaries of the system and the service organization's principal service commitments and system requirements. Such information is ordinarily presented along with the assertion. If it is not presented, the service auditor would ordinarily modify the service auditor's report by including such information.

Elements of a Service Auditor's SOC 3 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
par. .63*d*	An identification of the criteria against which the subject matter was measured or evaluated	In a SOC 3 examination, the effectiveness of controls is evaluated against the applicable trust services criteria, which are identified in the scope paragraph.	[*See scope paragraph of report*]
par. .63*e*	A statement that identifies the responsible party and its responsibility for the subject matter being in accordance with (or based on) the criteria or for its assertion	The report should include an identification of the responsible party and its responsibilities, which generally include statements that service organization management is responsible for the following: 1. The service organization's service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service organization's service commitments and system requirements were achieved 2. Providing the accompanying assertion about whether the controls within the system were effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved	*Service Organization's Responsibilities* XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, XYZ is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Elements of a Service Auditor's SOC 3 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
		3. Selecting, and identifying in its assertion, the applicable trust services criteria 4. Having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system based on the applicable trust services criteria	
par. .63*f*	A statement that the practitioner's responsibility is to express an opinion on the subject matter or assertion, based on the practitioner's examination	As noted previously, in a SOC 3 engagement the service auditor expresses an opinion on the assertion rather than the subject matters. The report should include a statement that the service auditor is responsible for expressing an opinion, based on the examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.	*Service Auditor's Responsibilities* Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

(continued)

Elements of a Service Auditor's SOC 3 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
par. .63*g*	A statement that i. the practitioner's examination was conducted in accordance with attestation standards established by the AICPA ii. those standards require that the practitioner plan and perform the examination to obtain reasonable assurance about whether (1) the subject matter is in accordance with (or based on) the criteria, in all material respects (or equivalent language regarding the subject matter and criteria, such as the language used in the examples	As noted earlier, in a SOC 3 engagement the service auditor expresses an opinion on the assertion rather than the subject matters. In applying these requirements, the service auditor generally includes in the report the following statements: 1. The examination was conducted in accordance with attestation standards established by the AICPA. 2. Those standards require that the service auditor plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. 3. The service auditor believes the evidence obtained is sufficient and appropriate to provide a reasonable basis for the opinion.	[*See service auditor's responsibilities paragraph*]

Elements of a Service Auditor's SOC 3 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
	in paragraph .A90 of AT-C section 205, *Assertion-Based Examination Engagements*) or (2) the responsible party's assertion is fairly stated, in all material respects iii. the practitioner believes the evidence the practitioner obtained is sufficient and appropriate to provide a reasonable basis for the practitioner's opinion		

(continued)

Elements of a Service Auditor's SOC 3 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
par. .63*h*	A description of the nature of an assertion-based examination engagement	In describing the nature of a SOC 3 examination, the service auditor generally indicates that a SOC 3 examination includes the following: 1. Obtaining an understanding of the system and the service organization's service commitments and system requirements 2. Assessing the risks that controls were not effective to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria 3. Performing procedures to obtain evidence about whether controls within the system were effective to achieve the service organization's service commitments and system requirements based the applicable trust services criteria In addition, the service auditor may indicate that the examination also included performing other procedures the service auditor considered necessary in the circumstances.	Our examination included: • Obtaining an understanding of the system and the service organization's service commitments and system requirements • Assessing the risks that controls were not effective to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria • Performing procedures to obtain evidence about whether controls within the system were effective to achieve XYZ's service commitments and system requirements based the applicable trust services criteria Our examination also included performing such other procedures as we considered necessary in the circumstances.

Elements of a Service Auditor's SOC 3 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
par. .63*i*	The service auditor's report should include a statement that the service auditor is required to be independent and to meet the service auditor's other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement.	The service auditor's report should include a statement that the service auditor is required to be independent and to meet the service auditor's other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement.	We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.
par. .63*j*	A statement that describes significant inherent limitations, if any, associated with the measurement or evaluation of the subject matter against the criteria	The service auditor should consider including in the report the following statements: • There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.	*Inherent Limitations* There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to

(continued)

Elements of a Service Auditor's SOC 3 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
		• Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.	provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.
par. .63*k*	The practitioner's opinion about whether the subject matter is in accordance with (or based on) the criteria, in all material respects	The service auditor's opinion should be expressed in a statement about whether management's assertion that the controls within the service organization's system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved is fairly stated based on the applicable trust services criteria, in all material respects.	*Opinion* In our opinion, management's assertion that the controls within XYZ's medical claims processing system were effective throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Elements of a Service Auditor's SOC 3 Report — *continued*

Reference to AT-C Section 205 Requirement on Which the SOC 3 Reporting Element Is Based	*AT-C Section 205 Requirements and Relevant Application Guidance*	*SOC 3 Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3 Report Language*
par. .63*l*	The manual or printed signature of the practitioner's firm	The service auditor's report should include the manual or printed signature of the service auditor's firm.	*Service auditor's signature*
par. .63*m*	The city and state where the practitioner's report is issued	The service auditor's report should include the city and state where the service auditor's report is issued.	*City and state where the report is issued*
par. .63*l*	The date of the report (The report should be dated no earlier than the date on which the practitioner has obtained sufficient appropriate evidence on which to base the practitioner's opinion, including evidence that *a.* the attestation documentation has been reviewed; *b.* if applicable, the written presentation of the subject matter has been prepared; and *c.* the responsible party has provided a written assertion.)	The service auditor should date the report no earlier than the date on which the service auditor has obtained sufficient appropriate evidence to support the opinion, including evidence that *a.* the attestation documentation has been reviewed and *b.* service organization management has provided a written assertion.	*Date of the service auditor's report*

4.126 As discussed in chapter 1, the SOC 3 report has been designed as a general-use report; however, nothing precludes the service auditor from restricting the use of the service auditor's report to a specific group of users when the service auditor believes one or more groups of potential users are likely to misunderstand the report. Examples of circumstances in which the service auditor might include an alert restricting the use of the report include situations in which the service auditor believes the following:

- Report users need to understand how the system interacts with user entity systems.
- Report users are unable to access communications provided by the service organization, when those communications are not available to the general public.
- Report users need to understand the effectiveness of controls at the subservice organization in order to understand the service auditor's report, when the scope of the engagement carves out a subservice organization.
- Only a specific group of report users is likely to understand the service auditor's report when the opinion has been modified because of a material description misstatement or for a scope limitation.

4.127 When the service auditor concludes that the opinion on effectiveness of controls should be modified because of a material deficiency or the lack of appropriate sufficient evidence, the service auditor should follow the requirements in paragraphs .70–.83 of AT-C section 205 and generally use the guidance described in this chapter for making such modifications. However, the separate paragraphs included in the report to explain the basis for the modification would not refer to testing exceptions identified in the description of the results of the service auditor's procedures because such information is not included in a SOC 3 report.

Illustrative SOC 3 Management Assertion and Service Auditor's Report

4.128 Appendix F, "Illustrative Management Assertion and Service Auditor's Report for a SOC 3 Examination," presents an illustrative management assertion and service auditor's report that might be appropriate for a SOC 3 report.

Appendix A

Comparison of SOC 1, SOC 2, and SOC 3 Examinations and Related Reports

This appendix is nonauthoritative and is included for informational purposes only.

The term *system and organization controls* (SOC) refers to the suite of services developed by the AICPA that practitioners may provide in connection with system-level controls of a service organization or system- or entity-level controls of other organizations. The following are designations for three such examinations and the source of the guidance for performing and reporting on them:

- *SOC 1 — SOC for Service Organizations: ICFR.* AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*,[1] and AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)*
- *SOC 2 — SOC for Service Organizations: Trust Services Criteria.* AT-C section 205, *Assertion-Based Examination Engagements*, and AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*
- *SOC 3 — SOC for Service Organizations: Trust Services Criteria for General Use Report.* AT-C section 205 and AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*

Practitioners performing any of those examinations are also required to comply with the requirements in AT-C section 105, *Concepts Common to All Attestation Engagements*, because they apply to all attestation engagements. A practitioner performing a SOC 1 examination is also required to comply with the requirements in AT-C section 205.

The following table identifies differences between SOC 1, SOC 2, and SOC 3 examinations and related reports:

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

	SOC 1 Examination	*SOC 2 Examination*	*SOC 3 Examination*
What are the criteria for the examination and where are they stated?	In AT-C section 320, paragraph .15 contains the minimum criteria for evaluating the description of the service organization's system, paragraph .16 contains the criteria for evaluating the suitability of the design of the controls, and paragraph .17 contains the criteria for evaluating the operating effectiveness of the controls.	DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*,[2] contains the criteria for evaluating the description of the service organization's system. TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*,[3] contains the criteria for evaluating the design and operating effectiveness of the controls.	TSP section 100 contains the criteria for evaluating the effectiveness of controls.
What is the purpose of the report?	To provide management of the service organization, user entities, and the independent auditors of user entities' financial statements with information and a service auditor's opinion about controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. The report enables the user auditor to perform risk assessment procedures and, if the report is a type 2 report, to use the report as audit evidence that controls at the service organization are operating effectively.	To provide service organization management, user entities, business partners, and other specified parties with information and a service auditor's opinion about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy.	To provide interested parties with a service auditor's opinion about the effectiveness of controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy.

[2] All DC sections can be found in AICPA *Description Criteria*.

[3] All TSP sections can be found in AICPA *Trust Services Criteria*.

	SOC 1 Examination	*SOC 2 Examination*	*SOC 3 Examination*
What are the components of the report?	**Components of a Type 1 Report** *a*. Management's description of the service organization's system *b*. A written assertion by management of the service organization about whether, based on the criteria in management's assertion, i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented as of a specified date and ii. the controls related to the control objectives stated in management's description of the service organization's system were suitability designed to achieve those control objectives as of the specified date *c*. A service auditor's report that expresses an opinion on the matters in (*b*i)–(*b*ii)	**Components of a Type 1 Report** *a*. The description of the service organization's system *b*. A written assertion by management of the service organization about whether i. the description of the service organization's system presents the service organization's system that was designed and implemented as of a specified date in accordance with the description criteria and ii. the controls stated in the description of the service organization's system were suitability designed as of the specified date to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria as of the specified date *c*. A service auditor's report that expresses an opinion on the matters in (*b*i)–(*b*ii)	**Components of the Report** *a*. A written assertion by management of the service organization about whether the controls within the system were effective throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. As part of that assertion, management describes the boundaries of the system and the service organization's principal service commitments and system requirements. *b*. A service auditor's report on whether management's assertion is fairly stated based on the applicable trust services criteria.

(continued)

	SOC 1 Examination	*SOC 2 Examination*	*SOC 3 Examination*
	Components of a Type 2 Report *a*. Management's description of the service organization's system *b*. A written assertion by management of the service organization about whether, based on the criteria, i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period, ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives, and iii. the controls related to the control objectives stated in management's description of the service organization'	**Components of a Type 2 Report** *a*. The description of the service organization's system *b*. A written assertion by management of the service organization about whether i. the description of the service organization's system presents the service organization's system that was designed and implemented throughout the specified period in accordance with the description criteria, ii. the controls stated in the description of the service organization's system were suitably designed throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and iii. the controls stated in the description of the service organization's system operated	N/A

	SOC 1 Examination	*SOC 2 Examination*	*SOC 3 Examination*
	system operated effectively throughout the specified period to achieve those control objectives *c*. A service auditor's report that i. expresses an opinion on the matters in (*b*i)–(*b*iii) and ii. includes a description of the service auditor's tests of the controls and the results of those tests	the controls stated in the description of the service organization's system operated *c*. A service auditor's report that i. expresses an opinion on the matters in (*b*i)–(*b*iii) and ii. includes a description of the service auditor's tests of controls and the results of those tests	
Who are the intended users of the report?	Management of the service organization, user entities during some or all of the period covered by the report (for type 2 reports) and user entities as of a specified date (for type 1 reports), and auditors of the user entities' financial statements	Service organization management and specified parties who have sufficient knowledge and understanding of information such as the following: • The nature of the service provided by the service organization • How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties • Internal control and its limitations • Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements	Interested parties

(continued)

	SOC 1 Examination	*SOC 2 Examination*	*SOC 3 Examination*
		• User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services • The applicable trust services criteria • The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks	

Appendix B

Comparison of SOC 2, SOC for Supply Chain, and SOC for Cybersecurity Examinations and Related Reports

This appendix is nonauthoritative and is included for informational purposes only.

The following table compares a SOC 2 examination and related report with a SOC for Supply Chain examination and a SOC for Cybersecurity examination and related reports. Within the columns, certain text is set in bold to highlight key distinctions between the three types of examinations and related reports.

	SOC 2 Examination[1]	***SOC for Supply Chain Examination***	***SOC for Cybersecurity Examination***[2]
What are the types of organizations for which an examination may be performed?	An organization, or segment of an organization, that provides services to user entities (a service organization)	An entity[3] that produces, manufactures, or distributes products	Any type of organization

(continued)

[1] For illustrative purposes, this table focuses specifically on a type 2 SOC 2 report, which includes an opinion on both the suitability of design and operating effectiveness of controls.

[2] In a SOC 2 examination, when the service organization uses the services of a subservice organization, management may elect to use the *inclusive method* or the *carve-out method* to address those services in the description of its system.

In the cybersecurity risk management examination, however, entity management is responsible for all controls within the entity's cybersecurity risk management program, regardless of whether those controls are performed by the entity or by a third party. Therefore, the description criteria for use in the cybersecurity risk management examination require the description to address all controls within the entity's cybersecurity risk management program. AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* provides guidance for service auditors engaged to examine and report on an entity's cybersecurity risk management program, including controls within that program.

[3] If a producer, manufacturer, or distributor bundles the sale of the products with services (for instance, installation), the scope of the SOC for Supply Chain examination may also include those services. There are several factors that are considered when determining whether such services would best be addressed by a SOC for Supply Chain examination or by a SOC 2 examination. AICPA Guide *Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System (SOC for Supply Chain)* provides guidance for service auditors engaged to examine and report on a system that produces, manufactures, or distributes products, including controls over the system.

	SOC 2 Examination	*SOC for Supply Chain Examination*	*SOC for Cybersecurity Examination*
Is the examination designed to be performed at a system level or at an entity level?	Generally, the examination is performed on a system or systems that provide services.	Generally, the examination is performed on an entity's system or systems that produce, manufacture, or distribute products.	Generally, the examination is performed on an entity-wide cybersecurity risk management program, although the scope may be narrowed to a specific system, business unit, or function of the entity.
What is the purpose of the report?	To provide specified parties (who have sufficient knowledge and understanding of the service organization and its system as discussed later) with information about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy to support users' evaluations of their own systems of internal control	To provide specified parties (who have sufficient knowledge and understanding of the entity and its system, as discussed later) with information about the controls within the entity's system relevant to security, availability, processing integrity, confidentiality, or privacy to enable users to better understand and manage the risks arising from business relationships with their supplier and distribution networks	To provide general users with useful information about an entity's cybersecurity risk management program for making informed decisions
Who are the intended users?	Service organization management and specified parties who have sufficient knowledge and understanding of the service organization and its system	Entity management and specified parties who have sufficient knowledge and understanding of the entity and its system	Entity management, directors, and a broad range of general users including analysts, investors, and others whose decisions might be affected by the effectiveness of the entity's cybersecurity risk management program

	SOC 2 Examination	*SOC for Supply Chain Examination*	*SOC for Cybersecurity Examination*
What professional standards and implementation guidance are applicable to the examination?	AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Assertion-Based Examination Engagements*, in AICPA *Professional Standards* AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*	AT-C section 105 and AT-C section 205 AICPA Guide *Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System (SOC for Supply Chain)*	AT-C section 105 and AT-C section 205 AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*
Who is the responsible party?	Service organization management	Entity management	Entity management
Is the report appropriate for general use or is it restricted to specified parties?	Restricted to the use of the service organization and specified parties, such as user entities of the system throughout some or all of the period, business partners subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and	Restricted to the use of the entity and specified parties,[4] including the entity's business customers and business partners, accountants providing services to such business customers and business partners, and prospective business customers and business partners who have sufficient knowledge and understanding of the following:	Appropriate for general use[5]

(continued)

[4] Specified parties and the knowledge and understanding they are expected to have are described in more detail in chapter 1, "Introduction and Background," beginning at paragraph 1.07.

[5] The term *general use* describes reports whose use is not restricted to specified parties. Nevertheless, as discussed in chapter 4, "Forming the Opinion and Preparing the Practitioner's Report," of AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, practitioners may decide to restrict the use of their report to specified parties.

	SOC 2 Examination	*SOC for Supply Chain Examination*	*SOC for Cybersecurity Examination*
	regulators who have sufficient knowledge and understanding of the following: • The nature of the service provided by the service organization • How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties • Internal control and its limitations • Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements • User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services • The applicable trust services criteria • The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks	• The nature of the goods produced, manufactured, or distributed by the entity • Internal control and its limitations • The applicable trust services criteria • The risks that may threaten the achievement of the entity's principal system objectives and how controls address those risks	

	SOC 2 Examination	*SOC for Supply Chain Examination*	*SOC for Cybersecurity Examination*
What is the subject matter of management's assertion and the examination?	The description of the service organization's system based on the description criteria	The description of the entity's production, manufacturing, or distribution system based on the description criteria	The description of the entity's cybersecurity risk management program based on the description criteria
	Suitability of design and operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to security, availability, processing integrity, confidentiality, or privacy	Whether the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective[6] throughout the period, based on the applicable trust services criteria relevant to security, availability, processing integrity, confidentiality, or privacy	The effectiveness of controls within that program to achieve the entity's cybersecurity objectives based on the control criteria
What are the criteria for the examination?	The criteria for the description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*, in AICPA *Description Criteria*	The criteria for the description of an entity's system in DC section 300, *2020 Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report*, in AICPA *Description Criteria*	The criteria for a description of an entity's cybersecurity risk management program in DC section 100, *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*, in AICPA *Description Criteria*

(continued)

[6] Effective controls are those that are both suitably designed and operating effectively.

	SOC 2 Examination	*SOC for Supply Chain Examination*	*SOC for Cybersecurity Examination*
	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, in AICPA *Trust Services Criteria*, contains the criteria for evaluating the design and operating effectiveness of controls (*applicable trust services criteria*).	TSP section 100 in AICPA *Trust Services Criteria* contains the criteria for evaluating the effectiveness of controls (*applicable trust services criteria*).	The trust services criteria for security, availability, and confidentiality included in TSP section 100 in AICPA *Trust Services Criteria* are suitable for use as control criteria.[7]
What are the contents of the report?	A description of the service organization's system	A description of the entity's production, manufacturing, or distribution system	A description of the entity's cybersecurity risk management program
	A written assertion by service organization management about whether (*a*) the description of the service organization's system was presented in accordance with the description criteria and (*b*) the controls stated in the description were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria	A written assertion by entity management about whether (*a*) the description of the entity's system was presented in accordance with the description criteria and (*b*) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria	A written assertion by entity management about whether (*a*) the description of the entity's cybersecurity risk management program was presented in accordance with the description criteria and (*b*) controls within the program were effective in achieving the entity's cybersecurity objectives based on the control criteria

[7] For both the description criteria and control criteria in a cybersecurity risk management examination, suitable criteria other than those outlined in this appendix may also be used.

	SOC 2 Examination	*SOC for Supply Chain Examination*	*SOC for Cybersecurity Examination*
	A service auditor's[8] report that contains an opinion about whether (*a*) the description of the service organization's system was presented in accordance with the description criteria and (*b*) the controls stated in the description were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria	A practitioner's report that contains an opinion about whether (*a*) the description of the entity's system was presented in accordance with the description criteria and (*b*) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria	A practitioner's report that contains an opinion about whether (*a*) the description of the entity's cybersecurity risk management program was presented in accordance with the description criteria and (*b*) the controls within that program were effective in achieving the entity's cybersecurity objectives based on the control criteria
	A description of the service auditor's tests of controls and the results of the tests	A description of the practitioner's tests of controls and the results of the tests	

[8] The practitioner in a SOC 2 examination is referred to as a *service auditor*.

Appendix C

Appendix C-1	***Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination (Carved-Out Controls of a Subservice Organization and Complementary Subservice Organization Controls and Complementary User Entity Controls)***
Appendix C-2	***Illustrative Service Organization and Subservice Organization Management Assertions and Service Auditor's Report for a Type 2 Examination (Subservice Organization Presented Using the Inclusive Method and Complementary User Entity Controls)***
Appendix C-3	***Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation***

An illustrative type 2 report that includes the description of the system in addition to management's assertion and the service auditor's report is available on the AICPA website.

Appendix C-1

Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination (Carved-Out Controls of a Subservice Organization and Complementary Subservice Organization Controls and Complementary User Entity Controls)

This appendix is nonauthoritative and is included for informational purposes only.

In the following illustrative management assertion and service auditor's report, XYZ Service Organization has engaged the service auditor to examine and report on the description of the service organization's medical claims processing system and the suitability of design and operating effectiveness of controls relevant to security, availability, processing integrity, confidentiality, and privacy to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The example assumes that XYZ Service Organization outsources certain aspects of its system to a subservice organization and has elected to use the carve-out method for the subservice organization. In addition, complementary user entity and complementary subservice organization controls are required for XYZ Service Organization to achieve certain service commitments and system requirements based on the applicable trust services criteria. Language that has been added to the illustrative management assertion and to the service auditor's report to reflect the use of the carve-out method and the need for complementary user entity controls and complementary subservice organization controls is shown in ***boldface italics****.*

Illustrative Assertion by Service Organization Management

[*XYZ Service Organization's Letterhead*]

Assertion of XYZ Service Organization Management

We have prepared the accompanying description of XYZ Service Organization's (XYZ's) medical claims processing system titled "XYZ Service Organization's Description of its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (description criteria).[1] The description

[1] The 2018 description criteria are codified as DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*, in AICPA *Description Criteria*. As implementation guidance may be updated without changes to criteria, service organization management and the service auditor should review the most current version of DC section 200 for the most up-to-date guidance.

is intended to provide report users with information about the medical claims processing system that may be useful when assessing the risks arising from interactions with XYZ's system, particularly information about system controls that XYZ has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*.[2]

XYZ uses a subservice organization to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of XYZ's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls.

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

a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, ***and if the subservice organization and user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period.***

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria ***if complementary subservice organization controls***

[2] The 2017 trust services criteria are codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, in AICPA *Trust Services Criteria*. As points of focus may be updated without changes to criteria, service organization management and the service auditor should review the most current version of TSP section 100 for the most up-to-date guidance.

and complementary user entity controls assumed in the design of XYZ's controls operated effectively throughout that period.

Illustrative Independent Service Auditor's Type 2 Report

Independent Service Auditor's Report on a SOC 2 Examination[3]

To: Management of XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying description of its medical claims processing system titled "XYZ Service Organization's Description of its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX,[4] (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.[5]

XYZ uses a subservice organization to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of XYZ's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

---

[3] The report may also be titled "Report of Independent Service Auditors."

[4] The title of the description of the service organization's system in the service auditor's report should be the same as the title used by service organization management in its description of the service organization's system.

[5] A statement such as the following is added to the service auditor's report when information that is not covered by the report is included in the description of the service organization's system:

> The information included in section X, "Other Information Provided by XYZ Service Organization That Is Not Covered by the Service Auditor's Report," is presented by XYZ management to provide additional information and is not a part of XYZ's description. Information about XYZ's [*describe the nature of the information, for example, planned system changes*] has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service

commitments and system requirements based on the applicable trust services criteria

- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section XX.

Opinion

In our opinion, in all material respects,

a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period ***and if the subservice organization and user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period.***

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria ***if complementary subservice organization controls and complementary user entity controls assumed in the design of XYZ's controls operated effectively throughout that period.***

Restricted Use

This report, including the description of tests of controls and results thereof in section XX, is intended solely for the information and use of XYZ, user entities of XYZ's medical claims processing system during some or all of the period January 1, 20XX, to December 31, 20XX, business partners of XYZ subject to risks arising from interactions with the medical claims processing system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- ***Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements***
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[*Service auditor's signature*]
[*City and state where the report is issued*]
[*Date of the service auditor's report*]

Appendix C-2

Illustrative Service Organization and Subservice Organization Management Assertions and Service Auditor's Report for a Type 2 Examination (Subservice Organization Presented Using the Inclusive Method and Complementary User Entity Controls)

This appendix is nonauthoritative and is included for informational purposes only.

In the following illustrative management assertions and service auditor's report, XYZ Service Organization has engaged the service auditor to examine and report on the description of the service organization's medical claims processing system and its controls relevant to security, availability, processing integrity, confidentiality, and privacy to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The example assumes that XYZ Service Organization outsources certain aspects of its system to a subservice organization and has elected to use the inclusive method for the subservice organization. In addition, it assumes that service organization management has designed the controls that it expects the subservice organization to implement and operate. The example also assumes that complementary user entity controls are necessary to provide reasonable assurance that XYZ's service commitments and system requirements are achieved based on the applicable trust services criteria. Language that has been added to the illustrative service organization management assertion and to the service auditor's report to reflect the use of the inclusive method and the need for complementary user entity controls is shown in ***boldface italics****.*

Illustrative Assertion by Service Organization Management

[*XYZ Service Organization's Letterhead*]

Assertion of XYZ Service Organization Management

We have prepared the accompanying description of XYZ Service Organization's (XYZ's) medical claims processing system titled "XYZ Service Organization's Description of its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (description criteria).[1] The description is intended to provide report users with information about the medical claims

[1] The 2018 description criteria are codified as DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*, in AICPA *Description Criteria*. As implementation guidance may be updated without changes to criteria, service organization management and the service auditor should review the most current version of DC section 200 for the most up-to-date guidance.

processing system that may be useful when assessing the risks arising from interactions with XYZ's system, particularly information about system controls that XYZ has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.[2]

XYZ uses ABC Subservice Organization (ABC) to provide application maintenance and support services. XYZ's description includes a description of ABC's application maintenance and support services used by XYZ to process transactions for user entities and business partners, including the controls of XYZ and the controls designed by XYZ and operated by ABC that are necessary, in combination with controls at XYZ, for XYZ to achieve its service commitments and system requirements based on the applicable trust services criteria. ABC's assertion is presented on page XX in section YY.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls.

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

a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. the controls stated in the description, including the controls designed by XYZ and operated by ABC, were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period ***and if user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period.***

c. the controls stated in the description, including the controls designed by XYZ and operated by ABC, operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria ***if complementary user entity controls assumed in the***

[2] The 2017 trust services criteria are codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*. As points of focus may be updated without changes to criteria, service organization management and the service auditor should review the most current version of TSP section 100 for the most up-to-date guidance.

design of XYZ's controls operated effectively throughout that period.

Illustrative Assertion by Subservice Organization Management

[*ABC Subservice Organization's Letterhead*]

Assertion of ABC Subservice Organization Management

ABC Subservice Organization (ABC) provides application maintenance and support services to XYZ Service Organization (XYZ). The services provided by ABC are part of XYZ's medical claims processing system. We have prepared the portion of the accompanying description of XYZ Service Organization's medical claims processing system titled "XYZ Service Organization's Description of Its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) disclosing ABC's application maintenance and support services provided to XYZ based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (description criteria). The description is intended to provide report users with information about XYZ's medical claims processing system that may be useful when assessing the risks arising from interactions with XYZ's system, particularly information about system controls that XYZ has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

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

a. the description presents ABC's application maintenance and support services made available to XYZ throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. ABC's controls stated in the description, which were designed by XYZ, operated as described throughout the period January 1, 20XX, to December 31, 20XX, based on the applicable trust services criteria.

Illustrative Independent Service Auditor's Type 2 Report

Independent Service Auditor's Report on a SOC 2 Examination[3]

To: Management of XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying description of its medical claims processing system, ***including application maintenance and support services provided by and controls operated by ABC Subservice Organization (ABC),*** titled "XYZ Service Organization's Description of Its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*,

[3] The report may also be titled "Report of Independent Service Auditors."

in AICPA *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of XYZ's controls, ***including the controls designed by XYZ and operated by ABC,*** stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

ABC is an independent subservice organization providing application maintenance and support services to XYZ. The description includes those elements of the application maintenance and support services provided to XYZ and the controls designed by XYZ and operated by ABC that are necessary for XYZ to achieve its service commitments and system requirements based on the applicable trust services criteria.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Subservice Organization's Responsibilities

ABC has provided the accompanying assertion titled "Assertion of ABC Subservice Organization Management" (ABC assertion) about the description and the controls stated therein. ABC is responsible for preparing the portion of the description related to the application maintenance and support services provided to XYZ and the ABC assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; and implementing, operating, and documenting controls designed by XYZ, which enable XYZ to achieve its service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that

controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section XX.

Opinion

In our opinion, in all material respects,

a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. the controls stated in the description, including the controls designed by XYZ and operated by ABC, were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period ***and if the user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period.***

c. the controls stated in the description, including the controls designed by XYZ and operated by ABC, operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria ***if complimentary user entity controls assumed in the design of XYZ's controls operated effectively throughout that period.***

Restricted Use

This report, including the description of tests of controls and results thereof in section XX, is intended solely for the information and use of XYZ, user entities of XYZ's medical claims processing system during some or all of the period January 1, 20XX, to December 31, 20XX, business partners of XYZ subject to risks arising from interactions with the medical claims processing system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- ***Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements***
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services

- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[*Service auditor's signature*]
[*City and state where the report is issued*]
[*Date of the service auditor's report*]

Appendix C-3

Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation

This appendix is nonauthoritative and is included for informational purposes only.

In the following illustrative service auditor's report, XYZ Service Organization has engaged the service auditor to examine and report on the description of the service organization's medical claims processing system and the controls relevant to security, availability, processing integrity, confidentiality, and privacy, which XYZ designed, implemented, and operated to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The example assumes that XYZ Service Organization management refused to provide written representations at the end of the examination. Because of that limitation on the scope of the engagement, the service auditor decided to disclaim an opinion about whether the description presents XYZ Service Organization's medical claims processing system that was designed and implemented in accordance with the description criteria and about whether the controls included in the description were suitability designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Illustrative Independent Service Auditor's Type 2 Report

Independent Service Auditor's Report on a SOC 2 Examination[1]

To: Management of XYZ Service Organization

We were engaged to examine XYZ Service Organization's (XYZ's) accompanying description of its medical claims processing system titled "XYZ Service Organization's Description of Its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report,* in AICPA *Description Criteria*, (description criteria)[2] and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria*

---

[1] The report may also be titled "Report of Independent Service Auditors."

[2] The 2018 description criteria are codified as DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*, in AICPA *Description Criteria*. As implementation guidance may be updated without changes to criteria, service organization management and the service auditor should review the most current version of DC section 200 for the most up-to-date guidance.

for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA *Trust Services Criteria*.[3]

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria. Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination in accordance with attestation standards established by the AICPA.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Attestation standards established by the AICPA require that we request certain written representations from management, including a representation that all relevant matters are reflected in the evaluation of the description of its medical claims processing system and the suitability of design and operating effectiveness of controls within the system. We requested that management provide us with such a representation, but management refused to do so.

Because of the limitation on the scope of our examination discussed in the preceding paragraph, the scope of our work was not sufficient to enable us to express, and we do not express, an opinion on whether XYZ's description of its medical claims processing system presents the system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria, or on whether the controls stated therein were suitably designed and operating effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria, in all material respects.

---

[3] The 2017 trust services criteria are codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*. As points of focus may be updated without changes to criteria, service organization management and the service auditor should review the most current version of TSP section 100 for the most up-to-date guidance.

Appendix D

Illustrative Management Assertion and Service Auditor's Report for a Type 1 Examination

This appendix is nonauthoritative and is included for informational purposes only.

In the following illustrative management assertion and service auditor's report, XYZ Service Organization has engaged the service auditor to examine and report on the description of the service organization's medical claims processing system and the suitability of the design of its controls relevant to security, availability, processing integrity, confidentiality, and privacy to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Illustrative Assertion by Service Organization Management

[*XYZ Service Organization's Letterhead*]

Assertion of XYZ Service Organization Management

We have prepared the accompanying description of XYZ Service Organization's (XYZ's) medical claims processing system titled "XYZ Service Organization's Description of Its Medical Claims Processing System" as of December 31, 20XX, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria*, (description criteria).[1] The description is intended to provide report users with information about the medical claims processing system that may be useful when assessing the risks arising from interactions with XYZ's system, particularly information about system controls that XYZ has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.[2]

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

a. the description presents XYZ's medical claims processing system that was designed and implemented as of December 31, 20XX, in accordance with the description criteria.

---

[1] The 2018 description criteria are codified as DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*, in AICPA *Description Criteria*. As implementation guidance may be updated without changes to criteria, service organization management and the service auditor should review the most current version of DC section 200 for the most up-to-date guidance.

[2] The 2017 trust services criteria are codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, in AICPA *Trust Services Criteria*. As points of focus may be updated without changes to criteria, service organization management and the service auditor should review the most current version of TSP section 100 for the most up-to-date guidance.

b. the controls stated in the description were suitably designed as of December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date.

Illustrative Independent Service Auditor's Type 1 Report

Independent Service Auditor's Report on a SOC 2 Examination[3]

To: Management of XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying description of its medical claims processing system titled "XYZ Service Organization's Description of Its Medical Claims Processing System" as of December 31, 20XX,[4] (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria*, (description criteria) and the suitability of the design of controls stated in the description as of December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*.[5]

Service Organization's Responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of the design of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

---

[3] The report may also be titled "Report of Independent Service Auditors."

[4] The title of the description of the service organization's system in the service auditor's report should be the same as the title used by service organization management in its description of the service organization's system.

[5] A statement such as the following is added to the service auditor's report when information that is not covered by the report is included in the description of the service organization's system:

> The information included in section X, "Other Information Provided by XYZ Service Organization That Is Not Covered by the Service Auditor's Report," is presented by XYZ management to provide additional information and is not a part of XYZ's description. Information about XYZ's [*describe the nature of the information, for example, planned system changes*] has not been subjected to the procedures applied in the examination of the description and of the suitability of the design of controls to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. the description presents XYZ's medical claims processing system that was designed and implemented as of December 31, 20XX, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Restricted Use

This report is intended solely for the information and use of XYZ, user entities of XYZ's medical claims processing system as of December 31, 20XX, business partners of XYZ subject to risks arising from interactions with the medical claims processing system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[*Service auditor's signature*]
[*City and state where the report is issued*]
[*Date of the service auditor's report*]

Appendix E

Illustrative Service Auditor's Report for a SOC 2+ Examination

This appendix is nonauthoritative and is included for informational purposes only.

*In the following illustrative service auditor's report, XYZ Service Organization has engaged the service auditor to examine and report on (*a*) the description of the service organization's infrastructure services system; (*b*) the suitability of the design of its controls relevant to security, availability, processing integrity, confidentiality, and privacy to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria; (*c*) the operating effectiveness of its controls relevant to security, availability, processing integrity, confidentiality, and privacy to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and (*d*) the service organization's implementation of controls to meet the requirements of ABC Framework.*

Independent Service Auditor's Report on a SOC 2+ Engagement

To: Management of XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying description of its infrastructure services system titled "XYZ Service Organization's Description of Its Infrastructure Services System" throughout the period January 1, 20XX, to December 31, 20XX (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (appliable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. We have also examined whether the controls stated in the description were implemented to meet the requirements set forth in Sections XX through YY of ABC Framework.[1,2]

Service Organization's Responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system

[1] The service auditor should be as specific as possible when referring to the location of the criteria within the framework document.

[2] If management has not included in the description how the controls met the requirements of ABC Framework, references to "stated in the description" would be omitted when describing the implemented controls.

to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

XYZ is also responsible for selecting ABC Framework as additional criteria and implementing controls to meet the requirements set forth in Sections X.X through Y.Y of ABC Framework.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls as stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria

We are also responsible for expressing an opinion about whether the controls stated in the description were implemented to meet the requirements set forth in ABC Framework based on our examination. Attestations standards established by the AICPA require that we also plan and perform our examination to obtain reasonable assurance about whether, in all material respects, XYZ implemented controls to meet the requirements set forth in Sections X.X through Y.Y of ABC Framework.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

An examination of the description of a service organization's system, the suitability of the design and operating effectiveness of controls, and the implementation of controls to meet the requirements of ABC Framework involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements and the requirements of ABC Framework
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide

reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether the controls stated in the description were implemented to meet the requirements set forth in ABC Framework
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section XX.

Opinion

In our opinion, in all material respects,

a. the description presents XYZ's infrastructure services system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period;

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria; and

d. the controls stated in the description were implemented to meet the requirements set forth on pages XX through YY of ABC framework.[3]

Restricted Use

This report, including the description of tests of controls and results thereof in section XX, is intended solely for the information and use of XYZ, user entities of XYZ's infrastructure services system during some or all of the period January 1, 20XX, to December 31, 20XX, business partners of XYZ subject to risks arising from interactions with the infrastructure services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, regulators, or sponsoring organizations who developed ABC Framework, all of whom have sufficient knowledge and understanding of the following:[4]

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The requirements of ABC Framework
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[*Service auditor's signature*]
[*City and state where the report is issued*]
[*Date of the service auditor's report*]

---

[3] The wording of the service auditor's opinion may vary depending on the objective of the framework and the related criteria. For example, if the objective of the framework is to obtain information about the implementation and operating effectiveness of the controls to achieve objectives set forth in the framework, the opinion would also address the operating effectiveness of controls.

[4] This paragraph assumes that management and the service auditor believe all the intended users listed have sufficient knowledge of the requirements of ABC Framework to use the SOC 2+ report. In other situations, however, not all the intended users listed have that knowledge and the service auditor may need to modify this paragraph accordingly.

Appendix F

Illustrative Management Assertion and Service Auditor's Report for a SOC 3 Examination

This appendix is nonauthoritative and is included for informational purposes only.

*In the following illustrative management assertion and service auditor's report, XYZ Service Organization has engaged the service auditor to (*a*) examine the controls within the system relevant to security, availability, confidentiality, and privacy and (*b*) issue a SOC 3 report that can be posted on its website to encourage prospective customers to contract the service organization's services.*

Illustrative Assertion by Service Organization Management

[*XYZ Service Organization's Letterhead*]

Assertion of XYZ Service Organization Management

We are responsible for designing, implementing, operating, and maintaining effective controls within XYZ Service Organization's (XYZ's) transportation management system (system) throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.[1] Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria. XYZ's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

---

[1] The 2017 trust services criteria are codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, in AICPA *Trust Services Criteria*. As points of focus may be updated without changes to criteria, service organization management and the service auditor should review the most current version of TSP section 100 for the most up-to-date guidance.

We assert that the controls within the system were effective throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

An illustrative description of the boundaries of the system can be found on the AICPA website.

Attachment B

An illustrative description of a service organization's principal service commitments and system requirements can be found on the AICPA website.

Illustrative Independent Service Auditor's SOC 3 Report

Independent Service Auditor's Report on a SOC 3 Examination[2]

To: Management of XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) that the controls within XYZ's transportation management system (system) were effective throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Service Organization's Responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, XYZ is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

---

[2] The report may also be titled "Report of Independent Service Auditors."

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within XYZ's transportation management system were effective throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

[*Service auditor's signature*]
[*City and state where the report is issued*]
[*Date of the service auditor's report*]

Appendix G

Performing and Reporting in a SOC 2 Examination in Accordance With International Standards on Assurance Engagements (ISAEs) or in Accordance With Both the AICPA's Attestation Standards and the ISAEs

This appendix is nonauthoritative and is included for informational purposes only.

The advent of technology has led to the evolution of businesses that are often globally interconnected and interdependent. This has resulted in questions related to the use of SOC 2 reports internationally. For example, a service organization located in the United States might provide services to a user entity located in a foreign country (foreign user entity), or a non-U.S. CPA might be asked to perform a SOC 2 examination for a service organization located outside of the United States (foreign service organization). The purpose of this appendix is to answer some of the more commonly asked questions on this topic.

1. Inquiry — A foreign user entity of a U.S. service organization may wish to obtain a SOC 2 report from the U.S. service organization. In the United States, a SOC 2 examination is performed in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*,[1] and AT-C section 205, *Assertion-Based Examination Engagements*,[2] of the attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. However, the foreign user entity may request a service auditor's report indicating that the SOC 2 examination was performed in accordance with International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, which is issued by the International Audit and Assurance Standards Board (IAASB). The ISAEs are the international equivalent of the AICPA's attestation standards. May a U.S. CPA perform a SOC 2 examination and report in accordance with ISAE 3000 (Revised), rather than in accordance with AT-C section 205 of the attestation standards established by the AICPA?

Reply — No. A U.S. CPA may not perform a SOC 2 examination and report only in accordance with ISAE 3000 (Revised). Such reporting is not permitted under the "Compliance With Standards Rule" (ET sec. 1.310.001)[3] of the AICPA Code of Professional Conduct, which states that "a member who performs auditing,

---

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

[2] A SOC 2 examination may also be performed in accordance with AT section 101, *Attest Engagements*, of the PCAOB's interim attestation standards.

PCAOB interim attestation standards can be found in *PCAOB Standards and Related Rules*.

[3] All ET sections can be found in AICPA *Professional Standards*.

review, compilation, management consulting, tax, or other professional services shall comply with standards promulgated by bodies designated by Council." When a member is engaged to perform a professional service that is covered by established standards, the member must perform the service using such established standards.

Council has designated the Auditing Standards Board as the body with responsibility for promulgating Statements on Standards for Attestation Engagements, which govern the performance of SOC 2 examinations. Therefore, a U.S. CPA engaged to perform a SOC 2 examination must perform the examination in accordance with the attestation standards issued by the AICPA (AT-C section 205) and report accordingly.

2. Inquiry — May the U.S. CPA perform a SOC 2 examination in accordance with both AT-C section 205 of the attestation standards issued by the AICPA and ISAE 3000 (Revised) of the assurance standards issued by the IAASB?

Reply — Yes. A U.S. CPA may be engaged to perform a SOC 2 examination for the foreign user entity of a U.S. service organization (as noted above) or to perform a SOC 2 examination for a foreign service organization. A frequently asked question titled "Use of standards that have not been established by a body designated by AICPA Council,"[4] clarifies that a member is permitted to apply any relevant alternative standards in an attestation examination. Therefore, a U.S. CPA who performs a SOC 2 examination in accordance with AT-C section 205 may also perform the examination in accordance with ISAE 3000 (Revised) and issue one report that states that the examination was performed in accordance with the attestation standards established by the AICPA and ISAE 3000 (Revised) issued by the IAASB, provided the U.S. CPA complies with the requirements of both sets of standards and there are no conflicts between AT-C section 205 and IASE 3000 (Revised) that would lead the U.S. CPA to reach a different conclusion with respect to the opinion.

Although many of the requirements of AT-C section 205 and ISAE 3000 (Revised) are similar, there are certain differences. For example, under the requirements of ISAE 3000 (Revised), a practitioner may issue an examination report without obtaining a written assertion from the responsible party; under AT-C section 205, a practitioner is not permitted to issue an examination report if the practitioner has not obtained such an assertion from the responsible party, except when the responsible party is not the engaging party.[5] A SOC 2 examination performed in accordance with both the attestation standards and ISAEs is expected to be similar in scope and approach to a SOC 2 examination performed in accordance with only the attestation standards.

To make it easier for CPAs engaged to examine and report under both sets of standards, the ASB has published "Substantive Differences Between International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance*

---

[4] *Frequently Asked Questions: General ethics questions* issued by the AICPA Professional Ethics Division as of May 1, 2017. https://us.aicpa.org/content/dam/aicpa/interestareas/professionalethics/resources/tools/downloadabledocuments/ethics-general-faqs.pdf

[5] A SOC 2 examination, as described in this guide, is based on service organization management providing a written assertion to accompany the service auditor's report. Paragraph .86 of AT-C section 205, *Assertion-Based Examination Engagements*, permits a practitioner to report on a subject matter when the responsible party is not the engaging party and refuses to provide a written assertion, as long as the report discloses management's refusal and restricts use to the engaging party. However, this approach is unlikely to be appropriate in most SOC 2 engagements.

Engagements Other Than Audits or Reviews of Historical Financial Information, and AT-C sections 105, *Concepts Common to All Attestation Engagements,* and 205, *Assertion-Based Examination Engagements*, of Statements on Standards for Attestation Engagements," which identifies the substantive differences between the requirements of the attestation standards (AT-C sections 105 and 205) and ISAE 3000 (Revised). The document is available at https://us.aicpa.org/content/dam/aicpa/interestareas/frc/auditattest/downloadabledocuments/attest-clarity/differences-between-isae-3000-at-c-105-and-205.pdf.

When the U.S. CPA has performed a SOC 2 examination in accordance with the attestation standards and the ISAEs, the U.S. CPA would indicate in the report that the examination *was also conducted in accordance with ISAE 3000 (Revised)*. In addition, the U.S. CPA's report would need to include the elements of the auditor's report included in paragraphs .63–.68 of AT-C section 205 and paragraph .69 of ISAE 3000 (Revised).

The following is an illustrative report that meets the requirements in AT-C section 205 and ISAE 3000 (Revised) related to the contents of the report, when the U.S. CPA is reporting under both standards. The illustrative SOC 2 report is prepared in accordance with AT-C section 205; additions included to meet the requirements of ISAE 3000 (Revised) are shown in ***boldface italics.***

Independent Service Auditor's *Assurance* Report on a SOC 2 Examination

To: Management of XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying description of its medical claims processing system titled "XYZ Service Organization's Description of Its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria for security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Service Organization's Responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the

achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants *(*AICPA*) **and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board.*** Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and XYZ's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether the controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Testing the operating effectiveness of the controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with ***the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.***

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section XX.

Opinion

In our opinion, in all material respects,

a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period; and

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted Use

This report, including the description of tests of controls and results thereof in section XX, is intended solely for the information and use of XYZ, user entities of XYZ's medical claims processing system during some or all of the period January 1, 20XX, to December 31, 20XX, business partners of XYZ subject to risks arising from interactions with the medical claims processing system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[*Service auditor's signature*]
[*City and state where the report is issued*]
[*Date of the service auditor's report*]

3. Inquiry — Given the same fact pattern as in the previous inquiry, may a non-U.S. CPA (or equivalent, such as a Chartered Accountant) perform a SOC 2 examination in accordance with ISAE 3000 (Revised)?

Reply — Yes. If not precluded by regulations of the local jurisdiction, a non-U.S. CPA may perform a SOC 2 examination in accordance with ISAE 3000 (Revised) and report accordingly. The non-U.S. CPA may find the guidance in AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* helpful when performing such an examination.

The following is an illustrative service auditor's report that may be appropriate when reporting on a SOC 2 examination performed in accordance with ISAE 3000 (Revised). The illustrative report is based on the reporting requirements of ISAE 3000 (Revised). However, it has also been modeled after the reports in ISAE 3402, *Assurance Reports on Controls at a Service Organization*. Although the subject matter of the reports in ISAE 3402 is "controls at a service organization that provides a service to user entities that is likely to be relevant to user entities' internal control as it relates to financial reporting" rather than controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy, which is the subject matter of a SOC 2 examination, there are certain aspects of the language in the illustrative report in ISAE 3402 that more closely parallel a SOC 2 examination.

Independent Service Auditor's Assurance Report on a SOC 2 Examination

To: Management of XYZ Service Organization

Scope

We have been engaged to report on XYZ Service Organization's (XYZ's) description at pages [*bb–cc*] of its medical claims processing system throughout the period January 1, 20XX, to December 31, 20XX, (the description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria*, (description criteria) and on the design and operation of controls stated in the description to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*, (applicable trust services criteria).

Service Organization's Responsibilities

XYZ is responsible for: preparing the description and accompanying statement at page [*aa*], including the completeness, accuracy, and method of presentation of the description and statement; providing the services covered by the description; selecting the applicable trust services category or categories and stating the related controls in the description; identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and designing, implementing, and operating controls that are suitably designed and operating effectively to provide reasonable assurance that its service commitments and system requirements were achieved.

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

The firm applies International Standard on Quality Control[6] and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion the description and on the design and operation of controls related to the service commitments and system requirements stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented in accordance with the description criteria and the controls are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

An assurance engagement to report on the description and the design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not presented in accordance with the description criteria and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to obtain reasonable assurance that the service commitments and system requirements stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description.

---

[6] ISQC I, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements*.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of Controls at a Service Organization

The description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own environment. Also, because of their nature, service organization controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection of any evaluation of the suitability of design or operating effectiveness of controls to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects,

a. the description presents the medical claims processing system as designed and implemented throughout the period from January 1, 20XX, to December 31, 20XX, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period from January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period; and

c. the controls, which were those necessary to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria, operated effectively throughout the period from January 1, 20XX, to December 31, 20XX.

Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed on pages [*yy–zz*].

Intended Users and Purpose

This report and the description of tests of controls on pages [*yy–zz*] are intended only for customers who have used XYZ's medical claims processing system and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the risks arising from interactions with the medical claims processing system of XYZ Service Organization.

[*Service auditor's signature*]
[*Date of the service auditor's assurance report*]
[*Service auditor's address*]

Appendix H

Definitions

This appendix is nonauthoritative and is included for informational purposes only.

For purposes of this guide, the following terms have the meanings attributed as follows:

applicable trust services criteria. The criteria codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, in AICPA *Trust Services Criteria*, used to evaluate controls relevant to the trust services category or categories included within the scope of a particular examination.

architecture. The design of the structure of a system, including logical components, and the logical interrelationships of computers, systems, networks, or other elements, whether internally or externally hosted.

authentication. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data.

authorization. The process of granting access privileges to a user, program, or process by a person who has the authority to grant such access.

board or board of directors. Individuals with responsibility for overseeing the strategic direction of the service organization and the obligations related to the accountability of the service organization. Depending on the nature of the service organization, such responsibilities may be held by a board of directors or supervisory board for a corporation, a board of trustees for a not-for-profit service organization, a board of governors or commissioners for a government service organization, general partners for a partnership, or an owner for a small business.

boundaries of the system (or system boundaries). The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. When systems for multiple services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each system will differ. In a SOC 2 engagement that addresses the confidentiality and privacy criteria, the system boundaries cover, at a minimum, all the system components as they relate to the life cycle of the confidential and personal information within well-defined processes and informal ad hoc procedures.

business partner. An individual or business (and its employees), other than a vendor, that has some degree of involvement with the service organization's business dealings or agrees to cooperate, to any degree, with the service organization (for example, a computer manufacturer that works with another company that supplies it with parts).

carve-out method. Method of addressing the services provided by a subservice organization in which the components of the subservice organization's system used to provide the services to the service organization are excluded

from the description of the service organization's system and from the scope of the examination. However, the description identifies (*a*) the nature of the services performed by the subservice organization; (*b*) the types of controls expected to be performed at the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and (*c*) the controls at the service organization used to monitor the effectiveness of the subservice organization's controls.

collection. The process of obtaining personal information from the individual directly (for example, through the individual's submission of an internet form or a registration form) or from another party such as a business partner.

complementary subservice organization controls (CSOCs). Controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization and that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

complementary user entity controls (CUECs). Controls that service organization management assumed, in the design of the service organization's system, would be implemented by user entities and that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved.

component (of internal control). One of five elements of internal control, including the control environment, risk assessment, control activities, information and communication, and monitoring activities.

compromise. Refers to a loss of confidentiality, integrity, or availability of information, including any resulting impairment of (*a*) processing integrity or availability of systems or (*b*) the integrity or availability of system inputs or outputs.

consent. This privacy requirement is one of the fair information practice objectives. Individuals must be able to prevent the collection of their personal data, unless legally required. If an individual has a choice about the use or disclosure of personal information, consent is the individual's way of giving permission for the use or disclosure. Consent may be explicit (for example, opting in) or implied (for example, not opting out). There are two types of consent:

- **explicit consent.** A requirement that an individual "signifies" agreement with a data controller by some active communication between the parties.
- **implied consent.** When consent may reasonably be inferred from the action or inaction of the individual.

contractor. An individual, other than an employee, engaged to provide services to an entity in accordance with the terms of a contract.

control activity. An action established through policies and procedures that helps ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

controls at a service organization. The policies and procedures at a service organization that are part of the service organization's system of internal control. Controls exist within each of the five COSO internal control components: control environment, risk assessment, control activities, information and communication, and monitoring. The objective of a service organization's system of internal control is to provide reasonable assurance that its service commitments and system requirements are achieved.

controls at a subservice organization. The policies and procedures at a subservice organization that are relevant to the service organization's achievement of its service commitments and system requirements.

COSO. The Committee of Sponsoring Organizations of the Treadway Commission. COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. (See www.coso.org.)

criteria. The benchmarks used to measure or evaluate subject matter.

data controller. An organization that (alone or jointly with others) determines the purposes for and the means by which personal data is processed.

data processor. An organization that processes personal data at the direction of a data controller. In many cases, a service organization may process personal data for its business-to-business (B2B) customers (user entities), which in turn may function as data controllers. In other cases, a service organization may function as a data controller depending on the facts and circumstances.

data subjects. The individuals about whom personal information is collected.

deficiency. Term used to identify misstatements resulting from controls that were not suitably designed or did not operate effectively.

description misstatement. Term used to describe differences between (or omissions in) the description and the description criteria.

design. As used in the COSO definition of *internal control*, the internal control system design is intended to provide reasonable assurance of the achievement of an entity's objectives.

deviation. Term used to identify misstatements resulting from the failure of a control to operate in a specific instance. A deviation may, individually or in combination with other deviations, result in a deficiency.

disclosure (of information). The provision of access to or the release, transfer, or divulging in any other manner of information outside the entity holding the information. *Disclosure* is often used interchangeably with the terms *sharing* and *onward transfer*.

disposal. A phase of the data life cycle that pertains to how an entity removes or destroys data or information.

entity. A legal entity or management operating model of any size established for a particular purpose. A legal entity may, for example, be a business enterprise, a not-for-profit organization, a government body, or an academic institution. The management operating model may follow product or service lines, divisions, or operating units, with geographic markets providing for further subdivisions or aggregations of performance.

entity-wide. Activities that apply across the entity — most commonly in relation to entity-wide controls.

environmental protections and safeguards. Controls and other activities implemented by the entity to detect, prevent, and manage the risk of casualty damage to the physical elements of the information system (for example, protections from fire, flood, wind, earthquake, power surge, or power outage).

external users. Users, other than entity personnel, who are authorized by entity management, customers, or other authorized persons to interact with the entity's information system.

fraud. An intentional act involving the use of deception that results in a misstatement in the subject matter or the assertion.

inclusive method. Method of addressing the services provided by a subservice organization in which the description of the service organization's system includes a description of (*a*) the nature of the services provided by the subservice organization; (*b*) the components of the subservice organization's system used to provide services to the service organization, including the subservice organization's controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and (*c*) the controls at the service organization used to monitor the effectiveness of the subservice organization's controls. (When using the inclusive method, controls at the subservice organization are subject to the service auditor's examination procedures. Because the subservice organization's system components are included in the description, those components are included in the scope of the examination.)

information and systems. Refers to information in electronic form (electronic information) during its use, processing, transmission, and storage and systems that use, process, transmit or transfer, and store information.

information assets. Data and the associated software and infrastructure used to process, transmit, and store information.

information life cycle. The collection, use, retention, disclosure, disposal, or anonymization of confidential or personal information within well-defined processes and informal ad hoc procedures.

inherent limitations. Those limitations of all internal control systems. The limitations relate to the preconditions of internal control, external events beyond the entity's control, limits of human judgment, the reality that breakdowns can occur, and the possibility of management override and collusion.

intended users. Individuals or entities that the service organization intends will be report users.

internal control. A process, effected by a service organization's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

management's assertion. A written assertion by management of a service organization or management of a subservice organization, if applicable, about

whether (*a*) the description of the system is in accordance with the description criteria, (*b*) the controls are suitably designed, and (*c*) in a type 2 report, the controls operated effectively to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria.

management override. Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status.

operating effectiveness (or controls that are operating effectively). Controls that operated effectively provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria.

personal information. Information that is about, or can be related to, an identifiable individual.

policies. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures.

privacy notice. A written communication by entities that collect personal information to the individuals about whom personal information is collected that explains the entity's (*a*) policies regarding the nature of the information that they will collect and how that information will be used, retained, disclosed, and disposed of or anonymized and (*b*) commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information, the choices that individuals have related to their personal information, the security of such information, and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

principal service commitments. Disclosures included in the description of the service organization's system related to the service commitments made by management to its customers about the system used to provide the service. The principal service commitments are those that are likely to be useful to the broad range of SOC 2 report users.

process or control framework. A framework that contains a set of processes or controls, established by another party, that organizations are expected to implement in support of establishing an effective system of internal control. These frameworks are usually developed by an industry group, regulator, governmental entity, standard-setting body, or other organization (collectively referred to as sponsoring organizations) to obtain information from organizations with which they do business about their processes or controls. The most common types of process or control frameworks relate to security and privacy.

report users (specified users or specified parties) of a SOC 2 report. In this document, the term refers to users of a SOC 2 report. The service auditor's report included in a SOC 2 report ordinarily includes an alert

restricting the use of the report to specified parties who possess sufficient knowledge and understanding of the service organization and the system to understand the report. The expected knowledge is likely to include an understanding of the following matters:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

Users likely to possess such knowledge include user entities and their personnel, business partners and their personnel, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who understand how the service organization's system may be used to provide the services. In some situations, federal or state governmental agencies, industry consortiums, or groups of subject matter experts (collectively referred to as *sponsoring organizations*) who need information about a specific subject matter (for example, security controls over sensitive information) from members of the sponsoring organization or other entities with whom the sponsoring organization does business may also be intended users.

responsibilities of external users. Those activities and tasks that service organization management expects user entities, their employees, and any other third-party users of the system to perform for the services provided by the service organization to function as intended to meet the needs of user entities.

retention. A phase of the data life cycle that pertains to how long an entity stores information for future use or reference.

risk. The possibility that an event will occur and adversely affect the achievement of objectives.

risk of material misstatement. The risk that the description of the service organization's system that was implemented and operated is not presented in accordance with the description criteria or that controls were not suitably designed or operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved.

security event. An occurrence, arising from actual or attempted unauthorized access or use by internal or external parties, that impairs or could impair the availability, integrity, or confidentiality of information or systems, result in unauthorized disclosure or theft of information or other assets, or cause damage to systems.

security incident. A security event that requires actions on the part of an entity in order to protect information assets and resources.

senior management. The chief executive officer or equivalent organizational leader and senior management team.

service auditor. As used in this guide, a CPA who performs a SOC 2 examination of controls within a service organization's system relevant to security, availability, processing integrity, confidentiality, or privacy.

service commitments. Declarations made by service organization management to user entities and others (such as user entities' customers) about the system used to provide the service. Service commitments can be communicated in written individualized agreements, standardized contracts, service-level agreements, or published statements (for example, in a security practices statement).

service organization. An organization, or segment of an organization, that provides services to user entities.

service provider. A vendor (such as a service organization) engaged to provide services to the entity. Service providers include outsourced services providers as well as vendors that provide services not associated with business functions, such as janitorial, legal, and audit services.

SOC 2 examination. An examination engagement to report on whether (*a*) the description of the service organization's system is in accordance with the description criteria, (*b*) the controls were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and (*c*) in a type 2 report, the controls operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The SOC 2 examination is performed in accordance with the attestation standards and AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.*

SOC 3 engagement. An examination engagement to report on management's assertion about whether controls within the system were effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to one or more of the trust services categories (applicable trust services criteria).

subsequent events. Events or transactions that occur after the specified period covered by the engagement, but prior to the date of the service auditor's report, which could have a significant effect on the evaluation of the presentation of the description of the service organization's system or the evaluation of the suitability of design and operating effectiveness of controls.

subservice organization. A vendor used by a service organization that performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

suitability of design (or suitably designed controls). Controls are suitably designed if they have the potential to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved. Suitably designed controls are operated as designed by persons who have the necessary authority and competence to perform the controls.

system. Refers to the infrastructure, software, procedures, and data that are designed, implemented, and operated by people to achieve one or more of the organization's specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements.

system components. Refers to the individual elements of a system, which may be classified into the following five categories: infrastructure, software, people, procedures, and data.

system event. An occurrence that could lead to the loss of, or disruption to, operations, services, or functions and result in a service organization's failure to achieve its service commitments or system requirements. Such an occurrence may arise from actual or attempted unauthorized access or use by internal or external parties and (*a*) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems; (*b*) result in unauthorized disclosure or theft of information or other assets or the destruction or corruption of data; or (*c*) cause damage to systems. Such occurrences also may arise from the failure of the system to process data as designed or from the loss, corruption, or destruction of data used by the system.

system incident. A system event that requires action on the part of service organization management to prevent or reduce the impact of the event on the service organization's achievement of its service commitments and system requirements.

system requirements. Specifications about how the system should function to (*a*) meet the service organization's service commitments to user entities and others (such as user entities' customers); (*b*) meet the service organization's commitments to vendors and business partners; (*c*) comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (*d*) achieve other objectives of the service organization that are relevant to the trust services categories addressed by the description. Requirements are often specified in the service organization's system policies and procedures, system design documentation, contracts with customers, and government regulations.

test of controls. A procedure designed to obtain evidence about whether controls operated effectively to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria.

third party. An individual or organization other than the service organization and its employees. Third parties may be customers, vendors, business partners, or others.

trust services. A set of professional attestation and advisory services based on a core set of criteria (trust services criteria) related to security, availability, processing integrity, confidentiality, or privacy.

unauthorized access. Access to information or system components that (*a*) has not been approved by a person designated to do so by management and (*b*) compromises segregation of duties, confidentiality commitments, or otherwise increases risks to the information or system components beyond the levels approved by management (that is, access is inappropriate).

user entity. An entity that uses the services provided by a service organization.

user or intended user. An individual or entity that the service auditor expects will use the service auditor's report.

vendor. An individual or business (and its employees) engaged to provide services to the service organization. Depending on the services a vendor provides (for example, if it operates certain controls on behalf of the service organization that are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved), a vendor might also be a subservice organization.

Appendix I

Overview of Statements on Quality Management Standards

This appendix is nonauthoritative and is included for informational purposes only.

Statement on Quality Management Standards (SQMS) No. 1, *A Firm's System of Quality Management* (QM section 10),[1] was issued by the Auditing Standards Board of the AICPA in June 2022 and is effective for a firm's accounting and auditing practice as of December 15, 2025. This standard supersedes Statement on Quality Control Standards No. 8, *A Firm's System of Quality Control* (QM section 10A).

The biggest change reflected in the new QM standard is the introduction of a risk-based approach in designing, implementing, and operating a system of quality management (SQM), which helps firms identify and address risks specific to their practice and creates a more scalable approach to quality for all firms. The risk-based approach comprises (*a*) establishing quality objectives (the desired outcomes relating to the components of the SQM to be achieved by the firm); (*b*) identifying and assessing quality risks (a risk that has a reasonable possibility of occurring and, individually or in combination with other risks, adversely affecting the achievement of one or more quality objectives); and (*c*) designing and implementing responses (policies or procedures designed and implemented by the firm to address one or more quality risks).

The standard's approach emphasizes the responsibility of firm leadership for proactively managing quality and provides flexibility to deal with differences in the size of firms and the nature of the services they provide. The essence of this approach is to focus firms' attention on risks that may have an impact on engagement quality. The approach requires a firm to customize the design, implementation, and operation of its SQM based on the nature and circumstances of the firm and the engagements it performs. The standard also has an increased emphasis on a continual flow of remediation and improvement.

An SQM addresses the following eight components, which are highly integrated and do not act in a linear manner:

1. The firm's risk assessment process
2. Governance and leadership
3. Relevant ethical requirements
4. Acceptance and continuance of client relationships and specific engagements
5. Engagement performance
6. Resources
7. Information and communication
8. The monitoring and remediation process

[1] All QM sections can be found in AICPA *Professional Standards*.

The objective of the firm is to design, implement, and operate an SQM for its accounting and auditing practice that provides the firm with reasonable assurance that

a. the firm and its personnel fulfill their responsibilities in accordance with professional standards and applicable legal and regulatory requirements and conduct engagements in accordance with such standards and requirements, and

b. engagement reports issued by the firm are appropriate in the circumstances.

In this context, reasonable assurance is not intended to be obtained through independent assurance that the system is effective (for example, by having a peer review every year); instead, it is obtained through the operation of the system as a whole.

Risk Assessment Process

The purpose of the risk assessment process element of an SQM is to establish quality objectives, identify and assess quality risks, and design and implement responses to address the quality risks. The risk assessment process section of SQMS No. 1 focuses firms' attention on risks that may have an impact on engagement quality.

The risk assessment is a three-step process:

1. *Establish quality objectives.* The standard requires the firm to establish specific quality objectives for each component except risk assessment and monitoring and remediation. The firm is required to establish additional quality objectives when necessary to achieve the objective of the SQM. However, the firm may not find it necessary to establish additional quality objectives.
2. *Identify and assess risks to the achievement of the quality objectives* (referred to in the standard as *quality risks*). Identifying and assessing quality risks involves
    a. understanding the factors (that is, the conditions, events, circumstances, actions, or inactions) that may adversely affect the achievement of the quality objectives and
    b. taking into account how and the degree to which the factors may adversely affect the achievement of the quality objectives. (The assessment of identified quality risks does not require formal ratings or scores.)
        i. A risk arises from how, and the degree to which, a condition, event, circumstance, action, or inaction may adversely affect the achievement of a quality objective. Not all risks meet the definition of a *quality risk*.
3. *Design and implement responses to address the quality risks*. The nature, timing, and extent of the firm's responses to address the quality risks are based on, and responsive to, the reasons for the assessments given to the quality risks. Certain responses are specified in the standard; however, the specific responses required by the standard will not be sufficient for the firm to address all its quality risks.

Firms are also required to identify information indicating the need for additions or modifications to quality objectives, quality risks, or responses.

Governance and Leadership

The purpose of the governance and leadership element of an SQM is to promote an internal culture based on the recognition that quality is essential in performing engagements. The governance and leadership section of SQMS No. 1 addresses the expected behavior of firm leadership in setting the tone at the top, the appropriate qualifications of leadership, and holding leadership accountable through performance evaluations. The standard also addresses the importance of quality in the firm's strategic decisions and actions — including financial and operational priorities — as well as firm leadership's ability to influence decisions about the firm's resources.

The firm is required to assign ultimate responsibility and accountability for the SQM to the firm's CEO, managing partner (or equivalent), or if appropriate, managing board of partners (or equivalent). In addition, the firm is required to assign the following to designated individuals:

- Operational responsibility for the SQM
- Operational responsibility for specific aspects of the SQM, including compliance with independence requirements and the monitoring and remediation process

SQMS No. 1 emphasizes the firm's commitment to quality through a culture that reflects the firm's role in serving the public interest through consistent quality engagements. Leadership demonstrating a commitment to quality through its actions and behaviors reinforces the responsibility that all personnel hold for quality relating to the performance of engagements and activities within the SQM.

Relevant Ethical Requirements

The purpose of the relevant ethical requirements element of an SQM is to provide the firm with reasonable assurance that the firm and its personnel comply with relevant ethical requirements when performing professional responsibilities. The relevant ethical requirements component of SQMS No. 1 addresses responsibilities regarding ethical requirements for the firm and its personnel as well as others in the firm's network. The following quality objectives should be established relating to the firm and its personnel:

- Understand the relevant ethical requirements to which the firm and the firm's engagements are subject.
- Fulfill their responsibilities in relation to the relevant ethical requirements to which the firm and the firm's engagements are subject.

The firm should also ascertain that others (including the network, network firms, individuals in the network or network firms, or service providers) who are subject to the relevant ethical requirements to which the firm and the firm's engagements are subject

- understand the relevant ethical requirements that apply to them, and

- fulfill their responsibilities in relation to the relevant ethical requirements that apply to them

Examples of relationships between the relevant ethical requirements component and other components include the following:

- The information and communication component may address the communication of various matters related to relevant ethical requirements, including
  - — the firm communicating the independence requirements to all personnel and others subject to independence requirements.
  - — personnel and engagement teams communicating relevant information to the firm without fear of reprisals, such as situations that may create threats to independence or breaches of relevant ethical requirements.
- As part of the resources component, the firm may
  - — assign individuals to manage and monitor compliance with relevant ethical requirements or to provide consultation on matters related to relevant ethical requirements.
  - — use IT applications to monitor compliance with relevant ethical requirements, including recording and maintaining information about independence.

The relevant ethical requirements that apply to others depend on the provisions of the relevant ethical requirements and how the firm uses others in its SQM or in performing engagements. Examples follow:

- Relevant ethical requirements may include requirements for independence that apply to network firms or employees of network firms.
- The principle of confidentiality may apply to the firm's network, other network firms, or service providers when they have access to client information obtained by the firm.

Acceptance and Continuance of Client Relationships and Specific Engagements

The purpose of the acceptance and continuance of client relationships and specific engagements component of an SQM is to provide reasonable assurance that the firm makes appropriate judgments about whether to accept or continue a client relationship and whether to perform a specific engagement. A firm's acceptance and continuance policies represent a key element in quality management, while also mitigating litigation and business risk. This component of SQMS No. 1 also addresses quality objectives for firms around client acceptance and continuance decisions. These objectives include judgments by the firm to accept or continue a client relationship or specific engagement based on

- information obtained about the nature and circumstances of the engagement.

- information obtained about the integrity and ethical values of the client, including the identity and business reputation of the client's principal owners, key management, and those charged with its governance.
- the firm's ability to perform the engagement in accordance with professional standards. and applicable legal and regulatory requirements

SQMS No. 1 also emphasizes that the financial and operational priorities of the firm should not lead to inappropriate judgments about whether to accept or continue a client relationship or specific engagement.

Engagement Performance

The purpose of the engagement performance element of an SQM is to provide the firm with reasonable assurance that engagements are consistently performed in accordance with applicable professional standards and regulatory and legal requirements and that the firm issues reports that are appropriate in the circumstances. The engagement performance section of SQMS No. 1 provides quality objectives that firms should establish to obtain reasonable assurance that high-quality performance is being attained in the firm's engagements. Establishing and maintaining quality objectives such as the following help the firm in obtaining reasonable assurance relating to the engagement performance element of an SQM:

- Engagement teams understand and fulfill their responsibilities in connection with the engagements, including, as applicable, the overall responsibility of engagement partners for managing and achieving quality on the engagement and being sufficiently and appropriately involved throughout the engagement.
- The nature, timing, and extent of direction and supervision of engagement teams and review of the work performed is appropriate based on the nature and circumstances of the engagements and the resources assigned or made available to the engagement teams; the work performed by less experienced engagement team members is directed, supervised, and reviewed by suitably experienced engagement team members.
- Engagement teams exercise appropriate professional judgment and, when applicable to the type of engagement, maintain professional skepticism.
- Consultation on difficult or contentious matters is undertaken, and the conclusions agreed to are implemented.
- Differences of opinion within the engagement team, or between the engagement team and the engagement quality reviewer or individuals performing activities within the firm's SQM, are brought to the attention of the firm and resolved.
- Engagement documentation is assembled on a timely basis after the date of the engagement report and is appropriately maintained and retained to meet the needs of the firm and comply with law, regulation, relevant ethical requirements, and professional standards.

Resources

The purpose of the resources element of an SQM is to provide the firm with reasonable assurance that it is appropriately obtaining, developing, using, maintaining, allocating, and assigning resources in a timely manner to enable the design, implementation, and operation of the SQM. SQMS No. 1 addresses all resources that the firm needs both to operate the system and to perform engagements. These resources cover the following:

- *Technological resources.* For example, audit tools or IT applications used by the firm for independence monitoring.
- *Intellectual resources.* For example, the firm's methodology, guidance, templates, or tools.
- *Human resources.* This may include people outside the firm used in engagements, including component auditors or engagement quality reviewers who are external to the firm.

The standard focuses on what resources are needed, how they are used and maintained, and whether they are appropriate. The principles-based nature of the requirements relating to resources takes into account the variety of resources used and their source. The resources section of SQMS No. 1 also covers the use of resources from service providers and how to determine that those resources are appropriate for the intended use by the firm. A resource from a service provider could be a methodology, an IT application, or people used in an engagement. Services that come from a firm's network, if the firm belongs to a network, are not considered as coming from a service provider.

Information and Communication

The purpose of the information and communication element of an SQM is to address the importance of communicating information obtained, generated, or used both within the firm and to external parties on a timely basis to enable the design, implementation, and operation of the SQM.

This component of SQMS No. 1 underscores the importance of a continuous flow of information and communication by linking the exchange of information to the firm's culture so that it is driven from top leadership throughout the firm. The standard requires that the firm establish an information system with processes to identify, capture, process, and maintain information, acknowledging that less complex firms with fewer personnel and direct involvement of leadership may accomplish the objective with less rigorous or detailed policies and procedures.

This component of SQMS No. 1 also encourages firms to be transparent to external parties about their SQM in a relevant, innovative, and proactive manner. This component requires that firms establish policies and procedures that address when communications with external parties are appropriate. To promote continual innovation in this area, the standard provides flexibility regarding the specific information communicated, the form of that communication, and the nature, timing, and extent of communication.

Monitoring and Remediation

The purpose of the monitoring and remediation process element of an SQM is to provide the firm with relevant, reliable, and timely information about the

design, implementation, and operation of the SQM so the firm may take appropriate action to remediate identified deficiencies on a timely basis. SQMS No. 1 focuses on monitoring activities that address the entire SQM. The standard emphasizes performing tailored monitoring activities sufficient to provide a basis for the firm to evaluate the SQM.

The requirements also emphasize factors that firms should consider in designing monitoring activities, rather than prescribing such activities. The nature, timing, and extent of monitoring activities will be driven by many firm-specific factors including the following:

- How the underlying system is designed
- The nature and circumstances of the firm and engagements it performs
- The extent of changes to the system
- The results of previous monitoring activities or external inspections

This component includes a requirement to inspect completed engagements and for engagement partners to be inspected on a cyclical basis. The firm determines its inspection criteria, including how often to select completed engagements, which completed engagements to select, which engagement partners to select, and how frequently to select an engagement partner. In doing so, the firm takes into account factors such as other types of monitoring the firm does, areas of risk, and how the system is designed.

The standard includes requirements for evaluating findings, identifying deficiencies, and evaluating the severity and persuasiveness of the deficiencies. These include a requirement to investigate the root cause of identified deficiencies. The requirement is intended to be flexible to encourage firms to scale the nature, timing, and extent of the procedures to investigate the root cause of the deficiencies so that they are appropriate and tailored to the circumstances. The evaluation of the severity and pervasiveness of deficiencies is also used by leadership in evaluating the system and concluding whether it achieved its objectives.
