1-1-2018

Guide: SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy, January 1, 2018

American Institute of Certified Public Accountants (AICPA)

AICPA

Guide

SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy

SOC 2®

January 1, 2018

SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy | January 1, 2018

AICPA

9 781945 498602

AAGSOP18P

AICPA

aicpa.org | AICPAStore.com

Guide

SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy

SOC 2®

January 1, 2018

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

ISBN 978-1-94549-860-2

Preface

(Updated as of January 1, 2018)

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 "Supplement" or "Appendix." A supplement is a reproduction, in whole or in part, of authoritative guidance originally issued by a standard-setting body (including regulatory bodies) and is applicable to entities or engagements within the purview of that standard setter, independent of the authoritative status of the applicable AICPA Guide. 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 be aware of and consider the guidance in this guide that is applicable to his or her attestation engagement. If the practitioner does not apply the attestation guidance included in an applicable AICPA Guide, the practitioner should be prepared to explain how he or she complied with the SSAE provisions addressed by such attestation guidance.

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 his or her 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*.

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

In April 2016, the ASB issued SSAE No. 18, *Attestation Standards*: *Clarification and Recodification,* which includes AT-C section 105 and AT-C section 205, *Examination Engagements*. 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.

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).

Defining Professional Responsibilities in AICPA Professional Standards

AICPA professional standards applicable to attestation engagements use the following two categories of professional requirements, identified by specific terms, to describe the degree of responsibility they impose on a practitioner:

- *Unconditional requirements*. The practitioner must comply with an unconditional requirement in all cases in which such requirement is relevant. The attestation standards use the word "must" to indicate an unconditional requirement.
- *Presumptively mandatory requirements*. The practitioner must comply with a presumptively mandatory requirement in all cases in which such requirement is relevant; however, in rare circumstances, the practitioner may judge it necessary to depart from the requirement. The need for the practitioner to depart from a relevant presumptively mandatory requirement is expected to arise only when the requirement is for a specific procedure to be performed and, in the specific circumstances of the engagement, that procedure would be ineffective in achieving the intent of the requirement. In such circumstances, the practitioner should perform alternative procedures to achieve the intent of that requirement and should document the justification for the departure and how the alternative procedures performed in the circumstances

were sufficient to achieve the intent of the requirement. The attestation standards use the word "should" to indicate a presumptively mandatory requirement.

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.

Changes to the Attestation Standards Introduced by SSAE No. 18

Restructuring of the Attestation Standards

The attestation standards provide for three types of services—examination, review, and agreed-upon procedures engagements. SSAE No. 18 restructures the attestation standards so that the applicability of any AT-C section to a particular engagement depends on the type of service provided and the subject matter of the engagement.

AT-C section 105 contains requirements and application guidance applicable to any attestation engagement. AT-C section 205, AT-C section 210, *Review Engagements*, and AT-C section 215, *Agreed-Upon Procedures Engagements,* each contain incremental requirements and application guidance specific to the level of service performed. The applicable requirements and application guidance for any attestation engagement are contained in at least two AT-C sections: AT-C section 105 and either AT-C section 205, 210, or 215, depending on the level of service provided.

In addition, incremental requirements and application guidance unique to four subject matters are included in the subject matter AT-C sections. Those sections are AT-C section 305, *Prospective Financial Information*, AT-C section 310, *Reporting on Pro Forma Financial Information*, AT-C section 315, *Compliance Attestation*, and AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting.* The applicable requirements and application guidance for an engagement to report on any of these subject matters are contained in three AT-C sections: AT-C section 105; AT-C section 205, 210, or 215, depending on the level of service provided; and the applicable subject matter section.

To avoid repetition, the requirements and application guidance in AT-C section 105 are not repeated in the level of service sections or in the subject matter sections, and the requirements and application guidance in the level of service sections are not repeated in the subject matter sections, except for repetition of the basic report elements for the particular subject matter.

Practitioner Is Required to Request a Written Assertion

In all attestation engagements, the practitioner is required to request from the responsible party a written assertion about the measurement or evaluation of the subject matter against the criteria. In examination and review engagements, when the engaging party is also the responsible party, the responsible party's refusal to provide a written assertion requires the practitioner to

withdraw from the engagement when withdrawal is possible under applicable laws and regulations. In examination and review engagements, when the engaging party is not the responsible party, the responsible party's refusal to provide a written assertion requires the practitioner to disclose that refusal in the practitioner's report and restrict the use of the report to the engaging party. In an agreed-upon procedures engagement, the responsible party's refusal to provide a written assertion requires the practitioner to disclose that refusal in the practitioner's report.

Risk Assessment in Examination Engagements

SSAE No. 18 incorporates a risk assessment model in examination engagements. In examination engagements, the practitioner is required to obtain an understanding of the subject matter that is sufficient to enable the practitioner to identify and assess the risks of material misstatement in the subject matter and provide a basis for designing and performing procedures to respond to the assessed risks.

Incorporates Certain Requirements Contained in the Auditing Standards

SSAE No. 18 incorporates a number of detailed requirements that are similar to those contained in the Statements on Auditing Standards, such as the requirement to obtain a written engagement letter and to request written representations. SSAE No. 18 includes these requirements based on the ASB's belief that a service that results in a level of assurance similar to that obtained in an audit or review of historical financial statements should generally consist of similar requirements.

Separate Discussion of Review Engagements

SSAE No. 18 separates the detailed procedural and reporting requirements for review engagements from their counterparts for examination engagements. The resulting guidance more clearly differentiates the two services.

Convergence

It is the ASB's general strategy to converge its standards with those of the International Auditing and Assurance Standards Board. Accordingly, the foundation for AT-C sections 105, 205, and 210 is International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*. Many of the paragraphs in SSAE No. 18 have been converged with the related paragraphs in ISAE 3000 (Revised), with certain changes made to reflect U.S. professional standards. Other content included in this statement is derived from the extant SSAEs. The ASB decided not to adopt certain provisions of ISAE 3000 (Revised); for example, a practitioner is not permitted to issue an examination or review report if the practitioner has not obtained a written assertion from the responsible party, except when the engaging party is not the responsible party. In the ISAEs, an assertion (or representation about the subject matter against the criteria) is not required in order for the practitioner to report.

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 section 105 and AT-C section 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 customers' internal control over financial reporting and, therefore, to the audit of financial statements. The requirements and guidance for performing and reporting on such controls is provided in AT-C section 320. The AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)* is an interpretation of AT-C section 320 that assists CPAs engaged to examine and report on controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting.
- *SOC 3®—SOC for Service Organizations: Trust Services Criteria for General Use Report*. Similar to a SOC 2® engagement, in a SOC 3® examination the practitioner reports on 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 applicable trust services criteria. Although the requirements and guidance for performing a SOC 3® examination are similar to 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 section 105 and AT-C section 205. The AICPA Guide *Reporting on an Entity's*

Cybersecurity Risk Management Program and Controls is an interpretation of AT-C section 205 that assists 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.

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 B, "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 C, "Illustrative Comparison of a SOC 2® Examination and Related Report With the Cybersecurity Risk Management Examination and Related Report," compares the features of a SOC 2® examination and a cybersecurity risk management examination.

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

In February 2018, the AICPA 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* (2018 description criteria).[2] The extant description criteria included in paragraphs 1.26–.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are now codified in DC section 200A. The 2018 description criteria were established by ASEC for use by service organization management when preparing the description of the service organization's system and by the service auditors when evaluating whether the description is presented in accordance with the description criteria in a SOC 2® examination.

ASEC, in establishing and developing these criteria, followed due process procedures, including exposure of the proposed criteria for public comment. Under BL section 360, *Committees*,[3] ASEC has been designated as a senior committee and has been given authority to make public statements and publish measurement criteria without clearance from AICPA Council or the board of directors.

Revisions to Trust Services Criteria

In April 2017, ASEC issued revisions to the trust services criteria for security, availability, processing integrity, confidentiality, or privacy. Codified as TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*,[4] the revised trust services criteria were established by the ASEC for use by practitioners when providing attestation or consulting services to evaluate controls relevant to the security, availability, or

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

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

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

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

ASEC, in establishing and developing these criteria, followed due process procedures, including exposure of the proposed criteria for public comment.

The trust services principles and criteria were revised to do the following:

- *Restructure and align the trust services criteria with the Committee of Sponsoring Organizations of the Treadway Commission's 2013* Internal Control—Integrated Framework *(COSO framework)*. ASEC restructured and realigned the trust services criteria to facilitate their use in an entity-wide engagement. Because the COSO framework is a widely used and accepted internal control framework that is intended to be applied to internal control at an entity as a whole or to a segment of an entity, ASEC determined that alignment with that framework was the best way to revise the trust services criteria for use when reporting at an entity level. Therefore, the 2017 trust services criteria align with the 17 principles in the COSO framework.[5]

  The 2017 trust services criteria may be used to evaluate control effectiveness in examinations of various subject matters. In addition, they may be used to evaluate controls over the security, availability, processing integrity, confidentiality, or privacy of information and systems

  - — across an entire entity;
  - — at a subsidiary, division, or operating unit level;
  - — within a function or system; or
  - — for a particular type of information used by the entity.

- *Rename the trust services principles and criteria.* The COSO framework uses the term *principles* to refer to the elements of internal control that must be present or functioning for the entity's internal control to be considered effective. To avoid confusion between the terminology used in the COSO framework and that used in the trust services principles and criteria, the latter were renamed as the *trust services criteria.* In addition, the five principles (security, availability, processing integrity, confidentiality, and privacy) included therein are now referred to as the *trust services categories.*
- *Restructure the criteria and add supplemental criteria to better address cybersecurity risks in engagements using the trust services criteria.* The 2017 trust services criteria address risk management, incident management, and certain other areas at a more detailed level than the previous version of the criteria. In addition, the 2017 trust services criteria include new supplemental criteria to address areas that are increasingly important to

[5] ©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

information security. The new criteria are organized into the following categories:

  - *Logical and physical access controls*. The criteria relevant to how an entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access to meet the entity's objectives addressed by the engagement
  - *System operations*. The criteria relevant to how an entity manages the operation of systems and detects and mitigates processing deviations, including logical and physical security deviations, to meet the entity's objectives addressed by the engagement
  - *Change management*. The criteria relevant to how an entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made, to meet the entity's objectives addressed by the engagement

- *Add points of focus to all criteria*. The COSO framework contains points of focus that represent important characteristics of the criteria to help users apply the criteria; thus, those points of focus are included in the revised trust services criteria. In addition, points of focus have been developed for each of the new supplemental criteria described in the previous bullet. Similar to the points of focus included in the COSO framework, the points of focus related to the supplemental criteria also represent important characteristics of those criteria. The points of focus may assist management and the practitioner in evaluating whether the controls are suitably designed and operating effectively; however, use of the criteria does not require management or the practitioner to separately assess whether points of focus are addressed.

AICPA.org Website

The AICPA encourages you to visit its website at aicpa.org and the Financial Reporting Center website at www.aicpa.org/frc. The Financial Reporting Center supports members in the execution of high-quality financial reporting. Whether you are a financial statement preparer or a member in public practice, this center provides exclusive member-only resources for the entire financial reporting process, and provides timely and relevant news, guidance, and examples supporting the financial reporting process, including accounting, preparing financial statements, and performing compilation, review, audit, attest, or assurance and advisory engagements. Certain content on the AICPA's websites referenced in this guide may be restricted to AICPA members only.

Recognition

Jay Brodish, Jr.
Dora Burzenski
Joseph S. Cascio
Lawrence Gill
Steven M. Glover
Gaylen Hansen
Tracy Harding
Daniel J. Hevia
Ilene Kassman
Alan Long
Richard Miller
Daniel D. Montgomery
Steven Morrison
Richard N. Reisig
Catherine M. Schweigel
Jere G. Shawyer
Chad Singletary

Assurance Services Executive Committee (2016–2017)

Robert Dohrer, *Chair*
Bradley Ames
Christine M. Anderson
Bradley Beasley
Nancy Bumgarner
Jim Burton
Chris Halterman
Mary Grace Davenport
Jennifer Haskell
Brad Muniz
Michael Ptasienski
Joanna Purtell
Miklos Vasarhelyi

ASEC SOC 2® Working Group

Chris Halterman, *Chair*
Efrim Boritz
Brandon Brown
Jeff Cook
Charles Curran
Peter F. Heuzey
Eddie Holt
Audrey Katcher
Kevin Knight
Christopher W. Kradjan
Thomas Patterson
Binita Pradhan
John Richardson
Soma Sinha
Rod Smith
David Wood

AICPA Staff

Charles E. Landes
Vice President
Professional Standards and Services

Amy Pawlicki
Vice President
Assurance and Advisory Innovation

Erin Mackler
Director
Assurance and Advisory Services—SOC Reporting

Mimi Blanco-Best
Senior Manager
Guidance—Assurance and Advisory SOC Reporting

Tanya Hale
Senior Manager
SOC Reporting—Service Organizations

Nisha Gordhan
Manager
Product Management and Development

TABLE OF CONTENTS

Chapter		Paragraph
1	Introduction and Background	.01-.77
	Introduction	.01-.06
	Intended Users of a SOC 2® Report	.07-.13
	Overview of a SOC 2® Examination	.14-.17
	Contents of the SOC 2® Report	.18-.49
	Definition of a System	.19 -.20
	Boundaries of the System	.21-.23
	Time Frame of Examination	.24
	Difference Between Privacy and Confidentiality	.25-.26
	Criteria for a SOC 2® Examination	.27-.43
	The Service Organization's Service Commitments and System Requirements	.44-.49
	SOC 2® Examination That Addresses Additional Subject Matters and Additional Criteria	.50-.54
	SOC 3® Examination	.55-.58
	Other Types of SOC Examinations: SOC Suite of Services	.59-.68
	SOC 1®—SOC for Service Organizations: ICFR	.60-.62
	SOC for Cybersecurity	.63-.68
	Professional Standards	.69-.76
	Attestation Standards	.70-.72
	Code of Professional Conduct	.73
	Quality in the SOC 2® Examination	.74-.76
	Definitions	.77
2	Accepting and Planning a SOC 2® Examination	.01-.172
	Introduction	.01-.02
	Understanding Service Organization Management's Responsibilities	.03-.29
	Management Responsibilities Prior to Engaging the Service Auditor	.04-.25
	Management Responsibilities During the Examination	.26-.28
	Management's Responsibilities During Engagement Completion	.29
	Responsibilities of the Service Auditor	.30
	Engagement Acceptance and Continuance	.31-.34
	Independence	.35-.38
	Competence of Engagement Team Members	.39-.42
	Preconditions of a SOC 2® Engagement	.43-.65
	Determining Whether the Subject Matter Is Appropriate for the SOC 2® Examination	.44-.48
	Determining Whether Management Is Likely to Have a Reasonable Basis for Its Assertion	.49-.56

Chapter		Paragraph
2	Accepting and Planning a SOC 2® Examination—continued	
	Assessing the Suitability and Availability of Criteria	.57-.58
	Assessing the Appropriateness of the Service Organization's Principal Service Commitments and System Requirements Stated in the Description	.59-.65
	Requesting a Written Assertion and Representations From Service Organization Management	.66-.69
	Agreeing on the Terms of the Engagement	.70-.90
	Accepting a Change in the Terms of the Examination	.75-.78
	Additional Considerations for a Request to Extend or Modify the Period Covered by the Examination	.79-.90
	Establishing an Overall Examination Strategy for and Planning the Examination	.91-.109
	Planning Considerations When the Inclusive Method Is Used to Present the Services of a Subservice Organization	.96-.103
	Considering Materiality During Planning	.104-.109
	Performing Risk Assessment Procedures	.110-.126
	Obtaining an Understanding of the Service Organization's System	.110-.119
	Assessing the Risk of Material Misstatement	.120-.126
	Considering Entity-Level Controls	.127-.131
	Understanding the Internal Audit Function	.132-.136
	Planning to Use the Work of Internal Auditors	.137-.153
	Evaluating the Competence, Objectivity, and Systematic Approach Used by Internal Auditors	.139-.144
	Determining the Extent to Which to Use the Work of Internal Auditors	.145-.147
	Coordinating Procedures With the Internal Auditors	.148-.152
	Evaluating Whether the Work of Internal Auditors Is Adequate for the Service Auditor's Purposes	.153
	Planning to Use the Work of an Other Practitioner	.154-.159
	Planning to Use the Work of a Service Auditor's Specialist	.160-.166
	Accepting and Planning a SOC 3® Examination	.167-.172
3	Performing the SOC 2® Examination	.01-.229
	Designing Overall Responses to the Risk Assessment and Obtaining Evidence	.01-.11
	Considering Materiality in Responding to the Assessed Risks and Planning Procedures	.05-.08
	Defining Misstatements in This Guide	.09-.11
	Obtaining and Evaluating Evidence About Whether the Description Presents the System That Was Designed and Implemented in Accordance With the Description Criteria	.12-.78
	The Service Organization's Service Commitments and System Requirements	.24-.29

Chapter		Paragraph
3	Performing the SOC 2® Examination—continued	
	Disclosures About Individual Controls	.30-.32
	Disclosures About System Incidents	.33-.35
	Disclosures About Complementary User Entity Controls and User Entity Responsibilities	.36-.41
	Disclosures Related to Subservice Organizations	.42-.51
	Disclosures About Complementary Subservice Organization Controls	.52-.54
	Disclosures About Significant Changes to the System During the Period Covered by a Type 2 Examination	.55-.56
	Changes to the System That Occur Between the Periods Covered by a Type 2 Examination	.57-.58
	Procedures to Obtain Evidence About the Description	.59-.63
	Considering Whether the Description Is Misstated or Otherwise Misleading	.64-.68
	Identifying and Evaluating Description Misstatements	.69-.71
	Materiality Considerations When Evaluating Whether the Description Is Presented in Accordance With the Description Criteria	.72-.78
	Obtaining and Evaluating Evidence About the Suitability of the Design of Controls	.79-.105
	Additional Considerations for Subservice Organizations	.88-.91
	Multiple Controls Are Necessary to Address an Applicable Trust Services Criterion	.92-.93
	Multiple Controls to Achieve the Service Organization's Service Commitments and Service Requirements Based on the Same Applicable Trust Services Criterion	.94
	Procedures to Obtain Evidence About the Suitability of Design of Controls	.95-.100
	Identifying and Evaluating Deficiencies in the Suitability of Design of Controls	.101-.105
	Obtaining and Evaluating Evidence About the Operating Effectiveness of Controls in a Type 2 Examination	.106-.114
	Designing and Performing Tests of Controls	.110-.114
	Nature of Tests of Controls	.115-.130
	Evaluating the Reliability of Information Produced by the Service Organization	.121-.130
	Timing of Tests of Controls	.131-.133
	Extent of Tests of Controls	.134-.139
	Testing Superseded Controls	.140-.141
	Using Sampling to Select Items to Be Tested	.142-.146
	Selecting Items to Be Tested	.145-.146
	Additional Considerations Related to Risks of Vendors and Business Partners	.147-.151
	Additional Considerations Related to CSOCs	.152-.155
	Considering Controls That Did Not Need to Operate During the Period Covered by the Examination	.156

Chapter		Paragraph
3	Performing the SOC 2® Examination—continued	
	Identifying and Evaluating Deviations in the Operating Effectiveness of Controls	.157-.160
	Materiality Considerations When Evaluating the Suitability of Design and Operating Effectiveness of Controls	.161-.165
	Using the Work of the Internal Audit Function	.166-.177
	Using the Work of a Service Auditor's Specialist	.178-.180
	Revising the Risk Assessment	.181
	Evaluating the Results of Procedures	.182-.189
	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	.190-.196
	Known or Suspected Fraud or Noncompliance With Laws or Regulations	.190-.192
	Communicating Incidents of Known or Suspected Fraud, Noncompliance With Laws or Regulations, Uncorrected Misstatements, or Internal Control Deficiencies	.193-.196
	Obtaining Written Representations	.197-.212
	Requested Written Representations Not Provided or Not Reliable	.209-.211
	Representations From the Engaging Party When Not the Responsible Party	.212
	Subsequent Events and Subsequently Discovered Facts	.213-.220
	Subsequent Events Unlikely to Have an Effect on the Service Auditor's Report	.220
	Documentation	.221-.225
	Considering Whether Service Organization Management Should Modify Its Assertion	.226-.229
4	Forming the Opinion and Preparing the Service Auditor's Report	.01-.119
	Responsibilities of the Service Auditor	.01-.03
	Forming the Service Auditor's Opinion	.04-.14
	Concluding on the Sufficiency and Appropriateness of Evidence	.05-.09
	Considering Uncorrected Description Misstatements and Deficiencies	.10-.12
	Expressing an Opinion on Each of the Subject Matters in the SOC 2® Examination	.13-.14
	Describing Tests of Controls and the Results of Tests in a Type 2 Report	.15-.30
	Describing Tests of Controls and Results When Using the Internal Audit Function	.23-.27
	Describing Tests of the Reliability of Information Produced by the Service Organization	.28-.30
	Preparing the Service Auditor's SOC 2® Report	.31-.41
	Elements of the Service Auditor's SOC 2® Report	.31-.32

Chapter		Paragraph
4	Forming the Opinion and Preparing the Service Auditor's Report—continued	
	Requirement to Restrict the Use of the SOC 2® Report	.33-.35
	Reporting When the Service Organization's Design of Controls Assumes Complementary User Entity Controls	.36-.38
	Reporting When the Service Organization Carves Out the Controls at a Subservice Organization	.39-.41
	Reporting When the Service Auditor Assumes Responsibility for the Work of an Other Practitioner	.42
	Modifications to the Service Auditor's Report	.43-.67
	Qualified Opinion	.51-.53
	Adverse Opinion	.54-.55
	Scope Limitation	.56-.60
	Disclaimer of Opinion	.61-.67
	Report Paragraphs Describing the Matter Giving Rise to the Modification	.68-.88
	Illustrative Separate Paragraphs When There Are Material Misstatements in the Description	.68-.78
	Illustrative Separate Paragraphs: Material Deficiencies in the Suitability of Controls	.79-.82
	Illustrative Separate Paragraphs: Material Deficiencies in the Operating Effectiveness of Controls	.83-.88
	Other Matters Related to the Service Auditor's Report	.89-.93
	Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs	.89-.90
	Distribution of the Report by Management	.91-.93
	Service Auditor's Recommendations for Improving Controls	.94
	Other Information Not Covered by the Service Auditor's Report	.95-.104
	Illustrative Type 2 Reports	.105-.106
	Preparing a Type 1 Report	.107-.109
	Forming the Opinion and Preparing a SOC 3® Report	.110-.119
	Elements of the SOC 3® Report	.110-.115
	Elements of the Service Auditor's Report	.116-.118
	Illustrative SOC 3® Management Assertion and Service Auditor's Report	.119
	Supplement A—2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report	
	Supplement B—2018 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy	
Appendix		
A	Information for Service Organization Management	
B	Comparison of SOC 1®, SOC 2®, and SOC 3® Examinations and Related Reports	

Appendix

C Illustrative Comparison of a SOC 2® Examination and Related Report With the Cybersecurity Risk Management Examination and Related Report

D

D-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 and Complementary User Entity Controls)

D-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)

D-3 Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation

D-4 Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)

E Illustrative Management Assertion and Service Auditor's Report for a Type 1 Examination

F Illustrative Management Assertion and Service Auditor's Report for a SOC 3® Examination

G

G-1 Illustrative Management Representation Letter for Type 2 Engagement

G-2 Illustrative Management Representation Letter for Type 1 Engagement

H Performing and Reporting on 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

I Definitions

Index of Pronouncements and Other Technical Guidance

Subject Index

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 (applicable trust services 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; and explains the difference between a type 1 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 are as follows:

- *Customer support*. Providing customers of user entities with online or telephonic post-sales support and service management. 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

[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.

and related health insurance claims to be processed accurately, securely, and confidentially.

- *Enterprise 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.
- *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 (FinTech) services*. Providing financial services companies with IT-based transaction processing services. Examples of such transactions are loan processing, peer-to-peer lending, payment processing, crowdfunding, big data analytics, and asset management.

1.03 Although these relationships may increase revenues, expand market opportunities, and reduce costs for the user entities and business partners, they also result in additional risks arising from interactions with the service organization and its system. Accordingly, the management of those 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 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® report is the result of an examination of whether (*a*) the description of the service organization's system presents the system that was 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

[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.

or privacy).[3,4] This examination, which is referred to as a *SOC 2® examination,* is the subject of this guide.

1.05 Because the informational needs of SOC 2® report users vary, there are two types of SOC 2® examinations and related reports:

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 also 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 type 2 examination also includes a detailed description of the service auditor's[5] tests of controls and the results of those tests. A report on such an examination is referred to as a *type 2 report*.

1.06 A service auditor is 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 the description of the service organization's system and the suitability of design of certain controls stated in the description and be engaged to express an opinion on the operating effectiveness of other controls stated in the description.

Intended Users of a SOC 2® Report

1.07 A SOC 2® report, whether a type 1 or a type 2 report, is usually intended to provide report users with information about the service organization's system 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. For instance, the description of the service organization's system is intended to provide report users with information about the system that may be useful when assessing the risks arising

---

[3] As discussed in paragraph 2.59, 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.

[4] 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 1.31.

[5] 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.

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. 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, management and the service auditor should agree on the intended users of the report (referred to as *specified parties*). 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[7] 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 Specified parties of a SOC 2® report may include service organization personnel, 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 user entities and business partners, and regulators who have sufficient knowledge and understanding of such matters.

1.10 Other parties may also have the requisite knowledge and understanding identified in paragraph 1.08. For example, prospective user entities

---

[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.

[7] In the July 2015 version of this guide, these controls were referred to as "controls expected to be implemented at carved-out subservice organizations."

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. (If prospective users lack such knowledge and understanding, management may instead engage a service auditor to provide a SOC 3® report, as discussed in paragraph 1.13.)

1.11 Because of the knowledge that intended users need to understand the SOC 2® report, the service auditor's report is required to be restricted to specified parties who possess that knowledge. Restricting the use of a service auditor's report in a SOC 2® examination is discussed beginning in paragraph 4.33.

1.12 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.

1.13 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 1.55, 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

1.14 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.

1.15 The service auditor performs a SOC 2® examination in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*,[8] and AT-C section 205, *Examination Engagements*. Those standards establish performance and reporting requirements for the SOC 2® examination. According to those standards, an attestation examination is predicated on the concept that a party other than the practitioner (the responsible party) makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria. An *assertion* is any declaration or set of declarations about whether the subject matter is in accordance with, or based on, the criteria.

---

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

1.16 In a SOC 2® examination, service organization management is the responsible party. However, in certain situations there may be other responsible parties.[9] As the responsible party, service organization management prepares the description of the service organization's system that is included in the SOC 2® report. In addition, the service auditor is required by the attestation standards[10] to request a written assertion from management. Management's written assertion 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.

1.17 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

1.18 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:

Table 1-1

Contents of a SOC 2® Report

Type 1 Report	*Type 2 Report*
1. Description of the system as of a point in time in accordance with the description criteria	1. Description of the system throughout a period of time in accordance with the description criteria

[9] 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.

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

Contents of a SOC 2® Report—*continued*

Type 1 Report	*Type 2 Report*
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 *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	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, *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

(continued)

Contents of a SOC 2® Report—*continued*

Type 1 Report	*Type 2 Report*
	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

1.19 In the SOC 2® examination, a system is defined as "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."

1.20 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 supports 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 output 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 prepared

Boundaries of the System

1.21 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).

1.22 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.

1.23 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.

Time Frame of Examination

1.24 Paragraph .A1 of AT-C section 105 states that the subject matter of 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.

Difference Between Privacy and Confidentiality

1.25 Some individuals consider effective privacy practices to be the same as effective practices over confidential information. However, as discussed in this guide, privacy applies only to personal information,[11] whereas confidentiality applies to various types of sensitive information.[12] Therefore, a SOC 2® examination that includes the trust services privacy criteria encompasses the service organization's specific processes that address each of the following, as applicable:

- Notice of the service organization's privacy commitments and practices
- 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

1.26 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.

Criteria for a SOC 2® Examination

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

- *Description criteria*.[13] Supplement A of this guide presents an excerpt from DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2®*

---

[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).

[12] 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.

[13] The description criteria presented in supplement A, "2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report," (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*, as discussed in the following footnote. 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*, in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are

(continued)

Report,[14] which 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 1.28.

- *Trust services criteria.*[15] Supplement B of this guide presents an excerpt from TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*[16] (the 2017 trust services criteria), which 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 1.31.

Description Criteria

1.28 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, supplement A 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 should carefully consider the facts and circumstances of the entity and its environment in actual situations when applying the description criteria.

(footnote continued)

codified in DC section 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*.

When preparing a description of the service organization's system of as of December 15, 2018, or prior to that date (type 1 examination) or a description for periods ending as of December 15, 2018, or prior to that date (type 2 examination), either the 2018 description criteria or the 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain available in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

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

[15] The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. Until that date, service auditors may use either the 2016 trust services criteria or the 2017 trust services criteria as the evaluation criteria in a SOC 2® examination. After that date, the 2016 trust services criteria will be considered superseded. During the transition period, management and the service auditor should identify in the SOC 2® report whether the 2017 or 2016 trust services criteria were used.

In addition, the 2014 trust services criteria will continue to be codified in TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they are available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

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

1.29 The description criteria in supplement A were promulgated by the Assurance Services Executive Committee (ASEC), 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 description criteria are published by the AICPA and made available to the public, they are considered available to report users. Therefore, they meet the definition in paragraph .25*b*ii of AT-C section 105 for criteria that is both suitable and available for use in an attestation engagement.

1.30 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

1.31 The engaging party,[17] 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).

1.32 Service organization management evaluates the suitability of design and operating effectiveness of controls stated in the description to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to the trust services category or categories included within the scope of the examination. Such criteria are referred to throughout this guide as the *applicable trust services criteria.* For example, in a SOC 2® examination that addresses security, the trust services criteria relevant to security, which are the common criteria (CC1.1–CC9.2) presented in supplement B, would be the applicable trust services criteria.

1.33 Because applying the trust services criteria requires judgment, supplement B also presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control—Integrated Framework*[18] (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 supplement B 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.

1.34 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[19] would, if operating as described,

---

[17] The engaging party is the party or parties that engage the service auditor to perform the examination. In a SOC 2® examination, service organization management is often, but not always, the engaging party.

[18] ©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

[19] Description criterion DC5 in supplement A 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.

provide reasonable assurance that such risks would not prevent the service organization from achieving its service commitments and system requirements.

1.35 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.

1.36 The trust services criteria in supplement B were promulgated by the ASEC. The ASEC has determined that the trust services criteria are both suitable and available for use in a SOC 2® examination.

Categories of Criteria

1.37 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.

1.38 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 service categories (common criteria) and
- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

For example, if the SOC 2® examination is only on availability, the controls should address all the common criteria and the additional specific criteria for availability.

Common Criteria

1.39 The common criteria presented in supplement B (CC1–CC5) are organized into the following classifications:

a. Control environment (CC1 series)

b. Communication and information (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 sub-classifications: logical and physical access controls [CC6 series], system operations [CC7 series], change management [CC8 series], and risk mitigation [CC 9 series].)

1.40 The service organization designs, implements, and operates controls at an entity level to support the achievement of its service commitments and system requirements based on the common criteria. This is particularly true for controls that address the control environment criteria. Considering the effect of controls operated at the entity level (referred to as *entity-level controls*) in a SOC 2® examination is discussed beginning in paragraph 2.128.

1.41 Table 1-2 identifies the trust services criteria to be used when evaluating the design or operating effectiveness of controls for each of the trust services categories. As shown in that table, the common criteria constitute the complete set of criteria for the security category. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of (*a*) the common criteria (labeled in the table in supplement B as the CC series) and (*b*) the criteria applicable to the specific trust services category, which are labeled in the table in supplement B as follows:

a. Availability (A series)
b. Processing integrity (PI series)
c. Confidentiality (C series)
d. Privacy (P series)

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
Processing integrity	X	X
Confidentiality	X	X
Privacy	X	X

1.42 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 the applicable trust services criteria are met, which would mitigate those risks.

1.43 *Using the Trust Services Criteria to Evaluate Suitability of Design and Operating Effectiveness in a SOC 2® Examination.* As previously discussed, the trust services criteria presented in supplement B 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.

The Service Organization's Service Commitments and System Requirements

1.44 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.

1.45 Service organization management is responsible for establishing its service commitments and 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

1.46 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.

1.47 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
- System edits that restrict the values accepted for system input, which are defined in application design documents
- 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])

1.48 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).

1.49 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 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. 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.

SOC 2® Examination That Addresses Additional Subject Matters and Additional Criteria

1.50 A service organization may engage the service auditor to examine and report on subject matters in addition to the description of the service organization's system in accordance with the description criteria and the suitability of design and operating effectiveness of controls based on the applicable trust services criteria. In that case, the service auditor would also examine and report on whether the additional subject matter is presented in accordance with the additional suitable criteria used to evaluate it. Table 1-3 provides examples of additional subject matters and additional criteria that may be used to evaluate them.

Table 1-3

Additional Subject Matter and Additional Criteria

What Additional Information Might Be Included in the SOC 2® Report?	*What Are the Subject Matters?*	*What Are Suitable Criteria Relevant to the Subject Matters?*
Information on the physical characteristics of a service organization's facilities (for example, square footage)	A detailed description of certain physical characteristics of a service organization's facilities that includes items such as the square footage of the facilities	Criteria to evaluate the presentation of the description of the physical characteristics of the facilities
Information about historical data regarding the availability of computing resources at a service organization	Historical data related to the availability of computing resources	Criteria to evaluate the completeness and accuracy of the historical data
Information about how controls at a service organization help meet the organization's responsibilities related to the security requirements of HIPAA	Compliance with the HIPAA security requirements	Security requirements set forth in the HIPAA Administrative Simplification (Code of Federal Regulations, Title 45, Sections 164.308–316)
Information about how controls at a service organization address the Cloud Security Alliance's Cloud Controls Matrix	Controls related to security at a cloud service provider	Criteria established by the Cloud Security Alliance's Cloud Controls Matrix relevant to the security of a system

1.51 A SOC 2® engagement that includes additional subject matters and additional criteria such as those described in the preceding table is predicated on service organization management providing the service auditor with the following:

- An appropriate description of the subject matter
- A description of the criteria identified by management used to measure and present the subject matter
- If the criteria are related to controls, a description of the controls intended to meet the control-related criteria
- An assertion by management regarding the additional subject matter or criteria

1.52 The service auditor should perform procedures to obtain sufficient appropriate evidence related to the additional subject matter or criteria in accordance with AT-C section 205 and the relevant guidance in this guide. In accordance with the reporting requirements in AT-C section 205, the service auditor should identify in the service auditor's report the additional subject matter being reported on or the additional criteria being used to evaluate the subject matter and report on the additional subject matter.

1.53 In some situations, the service auditor may be requested to also include in the report a description of the service auditor's tests of controls or procedures performed to evaluate the existing or additional subject matter against the existing or additional criteria and the detailed results of those tests. In that case, paragraph .A85 of AT-C section 205 provides the following factors for the service auditor to consider before agreeing to include such information in the report:

- Whether such a description is likely to overshadow the service auditor's overall opinion, which may cause report users to misunderstand the opinion
- Whether the parties making the request have an appropriate business need or reasonable basis for requesting the information (for example, the specified parties are required to maintain and monitor controls that either encompass or are dependent on controls that are the subject of an examination and, therefore, need information about the tests of controls to enable them to have a basis for concluding that they have met the requirements applicable to them)
- Whether the parties understand the nature and subject matter of the engagement and have experience in using the information in such reports
- Whether the service auditor's procedures relate directly to the subject matter of the engagement

1.54 If the service auditor believes that the addition of a description of tests of controls or procedures performed and the results thereof in a separate section of the report is likely to increase the potential for the report to be misunderstood by the requesting parties, the service auditor may decide to add an alert paragraph that restricts the use of the report to the parties making the request. Chapter 4 discusses the requirements for an alert paragraph in further detail.

SOC 3® Examination

1.55 To market its services to prospective customers of the system, a service organization may want to provide them with a SOC 2® report. However, some of those prospective customers (system users) may not have sufficient knowledge about the system, which might cause them to misunderstand the information in the report. Consequently, distribution of the SOC 2® report for general marketing purposes is likely be inappropriate. In this situation, a SOC 3® report, which is a general use report, may be more 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 more general user needs.

1.56 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[20] 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.

1.57 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 tests of controls and the results thereof.[21] Appendix B, "Comparison of SOC 1®, SOC 2®, and SOC 3® Examinations and Related Reports," compares a SOC 2® and a SOC 3® report.

1.58 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

1.59 In 2017, the AICPA introduced the term *system and organization controls* (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization and system- or entity-level controls of other organizations. Formerly, SOC referred to *service organization*

---

[20] 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.

[21] 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.

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. The following are designations for four such examinations in the SOC suite of services:

1. SOC 1®—SOC for Service Organizations: ICFR[22]
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

SOC 1®—SOC for Service Organizations: ICFR

1.60 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. The controls addressed in AT-C section 320 are those that a service organization implements to prevent, or detect and correct, misstatements[23] in the information it provides to user entities. A service organization's controls are relevant to a user entity's internal control over financial reporting when they are part of the user entity's information and communications component of internal control maintained by the service organization.[24] Such an examination is known as a SOC 1® examination, and the resulting report is known as a SOC 1® report.

1.61 Service organizations frequently receive requests from user entities for these reports because they 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 existing user entities (for example, existing customers of the service organization), their financial statement auditors, and management of the service organization. The 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.

1.62 Appendix B 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

1.63 Cybersecurity has become a top concern for boards of directors and senior executives of many entities throughout the country, regardless of their

---

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

[23] Paragraph .10 of AT-C section 105, *Concepts Common to All Attestation Engagements*, defines a *misstatement* as a difference between the measurement or evaluation of the subject matter by the responsible party and the proper measurement or evaluation of the subject matter 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.

[24] 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 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*.

size or the industry in which they operate. In addition, governmental 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.

1.64 For those reasons, entities have begun requesting practitioners to examine and report on a description of the 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. The performance and reporting requirements for such an examination are found in AT-C section 105 and AT-C section 205. The AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* contains interpretive application guidance for practitioners performing these engagements.

1.65 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.

1.66 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). The AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* contains description criteria and trust services criteria for security, availability, and confidentiality, which may be used in the cybersecurity risk management examination.

1.67 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.

1.68 Appendix C, "Illustrative Comparison of a SOC 2® Examination and Related Report With the Cybersecurity Risk Management Examination and

Related Report," of this guide presents the differences between a SOC 2® examination and a cybersecurity risk management examination.

Professional Standards

1.69 This guide provides guidance for a service auditor performing either a type 1 or a type 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

1.70 The service auditor performs a SOC 2® examination in accordance with AT-C section 105 and AT-C section 205. AT-C section 105 applies to all engagements in which a practitioner in the practice of public accounting is engaged to issue, or does issue, an attestation report on subject matter or an assertion about subject matter that is the responsibility of another party. AT-C section 205 contains performance, reporting, and application guidance that applies to all examination engagements under the attestation standards. Therefore, a practitioner engaged to perform a SOC 2® examination should comply with all relevant requirements in both of these AT-C sections.

1.71 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.

1.72 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

1.73 The AICPA Code of Professional Conduct (code) 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, call 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)[25] 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 2.36.

---

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

Quality in the SOC 2® Examination

1.74 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 when conducting its attestation practice. Under QC section 10, *A Firm's System of Quality Control*,[26] 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.

1.75 QC section 10 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 .42 of AT-C section 105.

1.76 Paragraph .33 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 .32 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. Chapter 2 discusses assessing the competence and capabilities that members of the engagement team need to possess to perform a SOC 2® examination.

Definitions

1.77 Definitions of the terms used in this guide are included in appendix I, "Definitions."

---

[26] The QC 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, it is helpful for the service auditor to understand management's responsibilities in the engagement; therefore, this chapter also provides a brief overview of management's responsibilities.

Introduction

2.01 Prior to accepting a SOC 2® examination, AT-C section 105, *Concepts Common to All Attestation Engagements*,[1] requires the service auditor to determine that certain preconditions are met. Among other things, those preconditions require the service auditor to determine 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. Prior to engagement acceptance, a service auditor is also required to establish an understanding with management about its responsibilities and those of the service auditor in the SOC 2® examination.

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

Understanding Service Organization Management's Responsibilities

2.03 As previously stated, the service auditor is required to establish, prior to acceptance of the SOC 2® examination, an understanding with service organization management about its responsibilities and those of 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 managements' responsibilities in more detail.

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

Management Responsibilities Prior to Engaging the Service Auditor

2.04 Prior to engaging a service auditor to perform a SOC 2® examination, service organization management 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 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 2.06)
  - — Determining whether subservice organizations, if any, are to be addressed in the report using the inclusive method or the carve-out method (paragraph 2.12)
  - — If a subservice organization is to be presented using the inclusive method, obtaining agreement from subservice 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 analyzing 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

2.05 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 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 he or she does not make decisions on management's behalf, which would impair the service auditor's independence. Independence is discussed beginning in paragraph 2.36.

Considerations in Identifying Subservice Organizations

2.06 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. 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 company that owns the service organization.

2.07 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.

2.08 If the service organization's controls alone achieve its service commitments and system requirements, or if the service organization's monitoring of the vendor's services and controls is sufficient to achieve its service commitments and system requirements, the services provided by a vendor are not likely to be relevant to the SOC 2® examination. Service organization management is responsible for determining whether it uses a subservice organization.

2.09 For example, consider a vendor that is responsible for performing quarterly maintenance on a service organization's backup power system in an examination that addresses availability. This vendor would not be considered a subservice organization if the service organization implements its own controls over the vendor's services and vendor controls over its maintenance activities are not 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 for availability. However, not all situations are as easily evaluated. For example, consider a vendor that provides data center hosting services. If that vendor is responsible for monitoring server capacity and usage and for projecting future capacity demands based on historical trends, controls at the

vendor may be needed for the service organization to achieve its availability commitments based on the applicable trust services criteria for availability. On the other hand, controls at the vendor may not be necessary if the service organization independently performs high-level capacity monitoring activities and reviews the future capacity demands projected by the vendor for appropriateness.

2.10 In some instances, a service organization may stipulate in its contract with the vendor that the vendor perform certain controls that the service organization believes are necessary to address the risks related to the vendor's services. For example, a service organization may outsource its application development testing to a vendor and contractually specify that certain controls be executed by the vendor. The service organization designates a service organization employee to oversee the outsourced services, and that employee compares the 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 the vendor before changes to the application are approved by the vendor and submitted to the service organization for user acceptance testing. In this instance, the controls at the vendor may not be 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.

2.11 If the vendor is a subservice organization, the service organization's description of its system would include the information set forth in description criterion DC7 presented in supplement A, "2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report," 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

2.12 If the service organization uses a subservice organization, management is responsible for determining whether to carve out or include the subservice organization's controls within the scope of the examination. Management of a service organization may need assistance in understanding 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 (1) the nature of the services performed by the subservice organization; (2) 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 (3) 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 (*a*) the nature of the services provided by the subservice organization and (*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. (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.)

2.13 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.

2.14 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.

2.15 Although the inclusive method provides more information for report users than the carve-out method, the inclusive method may not be appropriate or feasible in all cases. Management may determine that the carve-out method is most practical in the following circumstances:

a. The challenges entailed in implementing the inclusive method, which are described in paragraphs 2.97 and 2.99, are sufficiently onerous that it is not practical to use the inclusive method.

b. The service auditor is not independent of the subservice organization. (When the inclusive method is used, the SOC 2® examination covers the service organization and the subservice organization, and the service auditor must be independent of both entities.)

c. A type 1 or type 2 service auditor's report on the subservice organization, which meets the needs of report users, is available.

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

2.16 In some cases, the subservice organization's services and controls have a pervasive effect on the service organization's system. In these circumstances, management and the service auditor would 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 is unlikely to be useful to the intended users of the report. When making this determination, consideration of the following factors may be helpful:

- The significance of the portion of the system functions performed by the subservice organization
- The complexity of the services and the types of controls that would be expected to be implemented by the subservice organization
- The extent to which the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria depends on controls at the subservice organization
- The number of applicable trust services criteria that would not be met if the types of controls expected to be implemented at the subservice organization were not implemented
- The ability of the intended users of the report to obtain sufficient appropriate evidence about the design and, in a type 2 examination, the operating effectiveness of controls at the subservice organization

In situations in which the subservice organization's services and controls have a pervasive effect on the service organization's system, management would not be able to use the carve-out method.

Considerations in the Identification of Complementary Subservice Organization Controls

2.17 As discussed earlier, a subservice organization exists when management identifies certain risks that it expects to be addressed by controls implemented by that subservice organization. When the carve-out method is used, and controls performed by the subservice organization are necessary, in combination with the service organization's controls, to provide reasonable assurance that one or more of the service organization's service commitments and system requirements were achieved, such controls are referred to as *complementary subservice organization controls* (CSOCs).[2]

2.18 When using the carve-out method, the description would identify the types of CSOCs that the subservice organization is assumed to have implemented. Examples of the types of CSOCs the subservice organization is assumed to have implemented include the following:

- Controls relevant to the completeness and accuracy of transaction processing on behalf of the service organization
- Controls relevant to the completeness and accuracy of specified reports provided to and used by the service organization
- Logical access controls relevant to the processing performed for the service organization

Management may request the service auditor's assistance when determining how to present the CSOCs in the description. For example, the service auditor can provide examples of CSOC disclosures made by others and can make recommendations to improve the presentation of the CSOCs in the description.

2.19 Chapter 3, "Performing the SOC 2® Examination," discusses the service auditor's responsibilities for obtaining an understanding of CSOCs in the

[2] In the July 2015 version of this guide, those controls were referred to as *controls expected to be implemented at carved-out subservice organizations.*

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

2.20 Usually, user entities must perform specific activities in order 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 service and 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*. However, in some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the user entity performing certain activities in a defined manner. In these instances, the service organization expects the user entity to implement necessary controls and to perform them completely and accurately in a timely manner. Such controls are referred to as *complementary user entity controls* (CUECs).

2.21 A service organization's controls are usually able to provide reasonable assurance that the service organization's service commitments or system requirements were achieved without the implementation of CUECs because the service organization restricts its service commitments and system requirements to those matters that are its responsibility and that it can reasonably perform.

2.22 Consider, for example, 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 limits the service organization's responsibilities because the criterion 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 that inadvertently includes employees who should not have been included, the service organization has still met CC6.2. 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, identifying the authorized users and communicating that information to the service organization are not considered CUECs.

2.23 In other situations, a control may be necessary for 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 criterion. 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 at the user entity to protect the components of the service organization's system located at the user entity.

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

2.24 In addition to controls that the service organization expects at the subservice organization, 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 the subservice organization has a SOC 2® examination, such activities may be identified in the section of its description that describes CUECs. Such activities may also be described in user documentation published by the subservice organization or the agreement between the service organization and subservice organization. For example, a service organization that outsources aspects of its technology infrastructure to a subservice organization may obtain a type 1 or type 2 SOC 2® report from the subservice organization and discover that the subservice organization's description of its system includes the following CUEC:

> User entities should have controls in place to restrict access to system resources and applications to appropriate user entity personnel.

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

- 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.

Management Responsibilities During the Examination

2.26 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
- 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 service organization will not intervene in the work the internal auditor performs 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 are relevant to the description of the service organization's system and assertion (paragraph .25*b*iii(1) of AT-C section 105)
  - Access to additional information that the service auditor may request from management for the examination (paragraph .25*b*iii(2) of AT-C section 105)
  - 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 (paragraph .25*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 intentional acts that could adversely affect the presentation of the description of the service organization's system, the suitability of design of its controls, or, in a type 2 examination, the operating effectiveness of controls
  - Any 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 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 could have a significant effect on management's assertion (paragraph .50 of AT-C section 205)

2.27 Management acknowledges these responsibilities in an engagement letter or other suitable form of written communication. Appendix A, "Information for Service Organization Management," provides further information about management's responsibilities in the SOC 2® examination.

2.28 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 2.27 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 and the suitability of the design 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 2.97.

Management's Responsibilities During Engagement Completion

2.29 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 recommend that management modify the description)
- Modifying management's written assertion, if appropriate (see discussion beginning at paragraph 3.226)
- Providing the service auditor with written representations (see discussion beginning at paragraph 3.197)

Responsibilities of the Service Auditor

2.30 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 .24–.25 of AT-C section 105 have been met (see paragraph 2.44)
- 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 2.71)
- Reaching an understanding with management regarding their willingness and ability to provide a written assertion at the conclusion of the examination (see paragraph 2.67)
- 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 2.92)
- 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 2.111)

Engagement Acceptance and Continuance

2.31 With respect to the acceptance and continuance of client relationships and specific engagements, paragraph .27 of QC section 10, *A Firm's System of Quality Control*,[3] states that the firm should establish policies and procedures for the acceptance and continuance of client relationships and specific engagements, 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.

2.32 The quality control requirements for competence and ethical behavior are reiterated in paragraph .27 of AT-C section 105, which states 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 2.41.)

[3] The QC sections can be found in AICPA *Professional Standards*.

c. has determined that the engagement to be performed meets all the preconditions for an attestation engagement. (See paragraph 2.44.)

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

2.33 Quality control policies and procedures to comply with the quality control requirements often include consideration of the integrity and reputation of service organization management and significant shareholders or principal owners to determine whether the firm's reputation is likely to suffer by association. Generally, the service auditor will accept or continue a client relationship only after he or she has considered the integrity of service organization management, significant shareholders, or principal owners and has no information that would lead the service auditor to believe that the client lacks integrity. Absent such information, a service auditor generally would conclude that it is unlikely that association with the client would expose the service auditor to undue risk of damage to his or her professional reputation or financial loss.

2.34 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

2.35 Independence, as defined by the AICPA Code of Professional Conduct, is required for examination-level engagements to report on controls at a service organization. The independence assessment process may address 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.

2.36 The "Independence Rule" (ET sec. 1.200.001)[4] 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 section 1.297) of the "Independence Rule" establishes special independence requirements for a service auditor who provides services under the attestation standards. In addition, the "Conceptual Framework Approach" subtopic (ET section 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.

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

2.37 When performing engagements in which independence is required in accordance with the attestation standards, 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, 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.

2.38 When the service auditor is not independent but is required by law or regulation to accept the engagement and report on the subject matter, 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 the lack of independence, the service auditor should include all the reasons therefor.

Competence of Engagement Team Members

2.39 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 with the appropriate competence and capabilities. For that reason, as discussed in paragraph 2.33, the service auditor should not accept the SOC 2® examination unless he or she has determined that the individuals who would perform the engagement have the appropriate competence and capabilities to perform it.

2.40 When considering the competence and capabilities of engagement team members, the engagement partner should be satisfied that the team assigned to the engagement collectively has 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 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 technology 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 legal and regulatory requirements relevant to the examination

2.41 In addition, the engagement partner should make sure 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.

2.42 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 2.161.

Preconditions of a SOC 2® Engagement

2.43 A 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 .24–.25 of AT-C section 105 are met:

a. The service auditor is independent in accordance with the AICPA Code of Professional Conduct. (See paragraph 2.36.)

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. the 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 1.04; determining whether the subject matters are appropriate is discussed beginning at paragraph 2.45.)

d. The criteria used to prepare and evaluate the subject matters 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 1.29 and 1.36; the appropriateness of the principal service commitments and system requirements stated in the description is discussed beginning at paragraph 2.60.)

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

i. access to all information relevant to the measurement, evaluation, or disclosure of the subject matter;

ii. access to additional information that he or she may request; and

iii. unrestricted access to service organization personnel.

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

2.44 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, in certain situations, the subject matters may not be appropriate due to specific circumstances. The service auditor should determine whether aspects of the subject matters impair their appropriateness before accepting the engagement.

2.45 According to paragraph .A37 of AT-C section 105, subject matter is appropriate if it is identifiable, capable of consistent measurement or evaluation based on the criteria, and can be subjected to procedures for obtaining sufficient appropriate evidence to support an opinion. In a SOC 2® examination, the service auditor should consider 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 should 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 1.21.

2.46 In evaluating the appropriateness of the subject matter when determining whether to accept or continue a SOC 2® examination, relevant matters to consider may include the functions performed by the system, how subservice organizations are used, how information about subservice organizations will be presented in the description of the service organization's system (inclusive or carve-out method), the relevance to the system of the trust services category or categories included within the scope of the examination, and the period of time covered by the examination. For example, assume that service organization management wishes to engage the service auditor to perform a type 2 examination for a period of less than two months. In such circumstances, the service auditor may conclude that it is unlikely that sufficient appropriate evidence can be obtained to support an opinion.

2.47 When the subject matter of the engagement relates to only one part of a broader subject matter and, as a result, paragraph .A41 of AT-C section 105 indicates that the examination may not meet the information needs of intended users, the service auditor may question accepting an engagement. 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.

2.48 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 Management Is Likely to Have a Reasonable Basis for Its Assertion

2.49 Paragraph 2.45 indicates that, as one of the preconditions of the SOC 2® examination, the service auditor should determine whether the subject matters are appropriate for the engagement. According to paragraph .A36 of AT-C section 105, one element of the appropriateness of the subject matters is the existence of a reasonable basis for measuring or evaluating the subject matters.

2.50 Service organization management is responsible for having a reasonable basis for its assertion about the description and the 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. The procedures 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.

2.51 AT-C section 205 does not include requirements for the service auditor to perform procedures to determine whether management has a reasonable basis for its assertion. However, 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 with management the basis for its assertion prior to engagement acceptance. This will assist 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 his or her opinion, which is also a precondition of the examination.

2.52 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 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.

2.53 If service organization management determines the risks associated with 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 subservice organization by members of the service organization's internal audit function
- Reviewing and reconciling output reports
- Holding periodic discussions with the subservice organization personnel and evaluating subservice organization performance against established service level objectives and agreements
- Making site visits to the subservice organization
- Inspecting a type 2 SOC 2® report on the subservice organization's system
- Monitoring external communications, such as complaints from user entities relevant to the services performed by the subservice organization

2.54 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.

2.55 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.

2.56 If the service auditor believes that 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.

Assessing the Suitability and Availability of Criteria

2.57 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 supplement A and the trust services criteria in supplement B, "Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy," 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 .25ii of AT-C section 105 for criteria that is both suitable and available for use in an attestation engagement.

2.58 The Committee of Sponsoring Organizations of the Treadway Commission defines internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance." For a service organization's system, these objectives are the achievement of service commitments made to user entities and other system requirements that service organization management establishes for the functioning of the system. Consequently, when the trust services criteria are used to evaluate the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls to provide reasonable assurance that the service organization's system objectives were achieved, the controls are evaluated against their ability to achieve the service organization's service commitments and system requirements. Therefore, the service auditor obtains the service organization's service commitments and system requirements and assesses their appropriateness.

Assessing the Appropriateness of the Service Organization's Principal Service Commitments and System Requirements Stated in the Description

2.59 As stated in chapter 1, service organization management is responsible for 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. Because of the importance of disclosures about the service organization's service commitments and system requirements to users of a SOC 2® report, description criterion DC2 requires service organization management to disclose the principal service commitments, which are those that are likely to be relevant to the broad range of SOC 2® report users. Such disclosure enables report users to better understand how the system operates and how management and the service auditor evaluated whether controls were suitably designed and, in a type 2 examination, operated effectively. 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 commitment common to most user entities is likely to be relevant to the broad range of SOC 2® report users, that commitment would be a principal service commitment and service organization management would describe it in the description.

2.60 In other cases, however, the service organization may make a different commitment about system availability to an individual user entity that requires greater system availability than most user entities. Service organization management ordinarily would not disclose that commitment because it is unlikely to be relevant to the broad range of SOC 2® report users. Because that service commitment is not disclosed in the description, the individual user entity understands that the evaluation of the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls was made based on the service organization's achievement of its principal service commitments and system requirements (that is, those common to the majority of user entities); therefore, the individual user entity may need to obtain

additional information from the service organization regarding the achievement of its specific availability commitment.

2.61 When the description addresses privacy, service organization management discloses the service commitments and system requirements identified in the service organization's privacy notice or in its privacy policy that are relevant to the system being described. When making such disclosures, it may also be helpful to report users if service organization management describes the purposes, uses, and disclosures of personal information as permitted by user entity agreements.

2.62 An example of disclosure of a service organization's principal service commitments and system requirements is included in appendix D-4, "Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)."

2.63 Likewise, management should disclose only the principal system requirements that are relevant to the trust services category or categories addressed by the description and that are likely to be relevant to the broad range of SOC 2® report users. 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 relevant to the broad range of SOC 2® report users.

2.64 Because of the close relationship between the trust services criteria and the service organization's service commitments and system requirements, the service auditor should consider, prior to accepting the examination, whether the principal service commitments and system requirements to be stated in the description are appropriate for the SOC 2® examination. (The service auditor, however, does not have a responsibility to opine on the appropriateness of the commitments and requirements.)

2.65 If the service auditor believes that the service commitments and system requirements identified by management and stated in the description are not appropriate for the SOC 2® examination, the service auditor should discuss the matter with management. If management is unwilling to revise the description to include the service commitments and system requirements that the service auditor believes would result in a SOC 2® report that is likely to meet the common needs of the broad range of users, the service auditor may decide (*a*) to refuse to accept the engagement or (*b*) to restrict the use of the report to those users who are able to understand the risks not addressed by the service organization's service commitments and system requirements. Chapter 3 discusses considering the disclosures that service organization management makes about its 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[5]

2.66 Paragraph .10 of AT-C section 205 requires the service auditor to request a written assertion from the responsible party that addresses all the subject matters in the SOC 2® examination. Specifically, the assertion addresses 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.

2.67 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 each of the subject matters discussed in paragraph 1.04 and is not materially inconsistent with the subject matter or the service auditor's report. Illustrative examples of management assertions are presented in appendix D-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 and Complementary User Entity Controls);" appendix D-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 D-3, "Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation."

2.68 If management refuses to provide a written assertion, paragraph .82 of AT-C section 205 requires the service auditor to withdraw from the engagement when withdrawal is possible under applicable laws and regulations. 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, the operating effectiveness of controls.

2.69 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 expected representations prior to engagement acceptance. Appendix G, "Illustrative Management Representation Letters," presents

---

[5] As discussed beginning at paragraph 2.97, 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.

examples of representation letters that might be appropriate in a type 1 and type 2 examination.

Agreeing on the Terms of the Engagement

2.70 Paragraph .07 of AT-C section 205 requires the service auditor to agree on, and document in a written communication such as an engagement letter, the terms of the engagement with the engaging party. A written agreement 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.

2.71 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 American Institute of Certified Public Accountants

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

2.72 Paragraph .41 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. If the engaging party is the responsible party, the service auditor may wish to include this matter in the engagement letter.

2.73 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. Additional matters that may affect the service auditor's understanding of the terms of the engagement and how the terms should be documented in a recurring engagement are discussed in paragraph .09 of AT-C section 205.

2.74 Although not required by the attestation standards, the service auditor would ordinarily expect the engaging party to sign the engagement letter. The engaging party's refusal to sign the engagement letter would be a relevant factor in the service auditor's consideration of the integrity of the client and

the service auditor's decision about whether to accept or continue the engagement. If service organization management is the engaging party and refuses to sign the engagement letter, the service auditor should decline to accept or perform the SOC 2® examination, unless that is not allowed by applicable law or regulation.

Accepting a Change in the Terms of the Examination

2.75 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 .29 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

2.76 Other changes to the scope of the engagement, however, may not be considered reasonable 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 exclude portions of the system from the scope of the examination, may be unreasonable because of the likelihood that the service auditor's opinion would be modified. 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.

2.77 If, after using professional judgment, the service auditor believes there is reasonable justification to change the terms of the engagement from those originally contemplated, the service auditor would issue an appropriate report on the service organization's system. The attestation standards do not require the service auditor's report to 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 agreement to evidence agreement to the change among the parties.

2.78 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 should take appropriate action, which could include disclaiming an opinion on the description and the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls, or withdrawing from the engagement.

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

2.79 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. The service auditor should consider 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.

2.80 In many cases, the scope of the description of the service organization's system for the new period would be unchanged from the scope for the original period; therefore, the procedures the service auditor has performed to obtain evidence about the description would be relevant to the engagement covering the extended or modified period. If the scope of 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 also be relevant to the service auditor's opinions addressing the extended or modified period.

2.81 As an example, assume the service auditor performed tests of the operating effectiveness of controls during the original period (January 1, 20X1, to June 30, 20X1) for a sample of 13 items that relate to the period April 1, 20X1, through June 30, 20X1. In that case, the tests of operating effectiveness performed on the sample of 13 items could be used as evidence for the extended or modified period.

2.82 The service auditor would also obtain an 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. Paragraphs 3.62 and 3.108, 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.

2.83 The service auditor may decide that it is necessary to perform additional tests for the portion of the extended or modified period not included in the original period, and the results of those tests, along with any additional information of which the service auditor becomes aware, would be considered in forming a conclusion about the description, the suitability of the design of controls or, in a type 2 examination, the operating effectiveness of controls for the extended or modified period.

2.84 When forming the opinion, the service auditor considers conclusions reached during the original period and 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

2.85 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, 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

2.86 Obtaining management's written representations is discussed beginning in paragraph 3.187. When the examination covers an extended period, and the service auditor has requested written representations from management, the representation letter would 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

2.87 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 whether disclosures are required in, the service

auditor's report. Similarly, deficiencies noted in the extended or modified period are also evaluated to determine their effect on the service auditor's report.

2.88 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 considers 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.

2.89 For deficiencies identified during the original period that have not been remediated, the service auditor may evaluate the reasons that the deficiencies have not been remediated and consider the effect on the examination.

2.90 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 4 months were untested. Twenty-five items were tested in the original period, 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. Thirteen items were tested for the modified period, 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 trust services criteria would be based on a deviation rate of 2 of 25.

Establishing an Overall Examination Strategy for and Planning the Examination

2.91 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 specialists is used in the engagement, proper planning helps the service auditor coordinate their work.

2.92 Paragraph .11 of AT-C section 205 requires a service auditor to 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 performed by the engagement partner 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 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.

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.

2.93 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

2.94 Paragraph .13 of AT-C section 205 includes more detailed requirements and additional explanatory guidance that the service auditor should consider when developing the engagement plan.

2.95 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

2.96 When service organization management elects to use the inclusive method, subservice organization management is also a responsible party in the SOC 2® examination. Accordingly, subservice organization management has to comply with the requirements of AT-C sections 105 and 205 that relate to the responsible party, including providing the service auditor with a written assertion[6] and representation letter at the conclusion of the examination. Therefore, use of the inclusive method involves extensive planning and communication among the service auditor, the service organization, and the subservice organization.

2.97 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.

2.98 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 controls

[6] Subservice organization management's written assertion addresses the same matters addressed by service organization management's assertion. However, paragraph 2.103 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.

2.99 During planning, the service auditor should determine whether the subservice organization will provide a written assertion and representation letter. In addition, 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.

2.100 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.

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

- 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 auditor performs for the service auditor (paragraph 2.153)
- 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 management is aware of and that is relevant to the description of the subservice organization's system and assertion (paragraph .25*b*iii(1) of AT-C section 205)
  - Access to additional information that the service auditor may request from subservice management for the examination (paragraph .25*b*iii(2) of AT-C section 205)
  - 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 .25*b*iii(3) of AT-C section 205)
- 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 intentional acts that could adversely affect the description of the service organization's system, the suitability of design of controls,[7] or, in a type 2 examination, the operating effectiveness of controls (Paragraph 2.104 discusses a situation in which service organization management designs the controls at the subservice organization.)
- Any 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 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 could have a significant effect on subservice management's assertion (paragraph .50 of AT-C section 205)

2.102 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 complying with any of the requirements 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.

2.103 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 instance, 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

[7] Subservice organization management's written assertion addresses the same matters addressed by service organization management's assertion. However, paragraph 2.103 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.

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 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.

Considering Materiality During Planning

2.104 When establishing the overall strategy for and planning the examination, paragraph .16 of AT-C section 205 requires the service auditor to consider both qualitative and quantitative materiality factors. Due to the vast number of controls within even a small system, the service auditor needs to consider materiality to determine the nature, timing, and extent of procedures necessary to obtain sufficient appropriate evidence to support the service auditor's opinion in the SOC 2® examination. Adoption of an appropriate materiality allows the service auditor to prioritize testing efforts and supports an effective and efficient engagement.

2.105 In the SOC 2® examination, materiality relates to the likelihood and magnitude of the risks that threaten the achievement of the service organization's service commitments and system requirements and whether the controls the service organization has designed, implemented, and operated were effective in mitigating those risks to an acceptable level based on the applicable trust services criteria.

2.106 Accordingly, the service auditor should consider the nature of threats and the likelihood and magnitude of the risks arising from those threats to the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria. For example, the service auditor should consider the technical environment and whether the realization of security-related threats or exploitation of vulnerabilities related to the security of specific information assets, which appear inconsequential, could expose (either directly or indirectly) information assets and thereby result in failure to achieve the service organization's service commitments and system requirements. If access to another system (used to provide other services not addressed by the SOC 2® examination) could provide access to the service organization's system that is being examined, and the service auditor determines there is a high likelihood that such a vulnerability might be exploited, the service auditor is likely to consider access to the other system in the SOC 2® examination.

2.107 The service auditor's consideration of materiality is a matter of professional judgment and is affected by the service auditor's perception of the common information needs of the broad range of report users as a group. In this context, it is reasonable for the service auditor to assume that report users possess a certain level of knowledge as described in paragraph 1.08.

2.108 When considering materiality, the service auditor typically considers whether misstatements in the description or deficiencies in the suitability of design of controls or, in a type 2 examination, the operating effectiveness of controls, could reasonably be expected to influence the relevant decisions made by the broad range of report users discussed in chapter 1. However, if the examination has been designed to meet the informational needs of a specific subset

of such SOC 2® report users (and the report is restricted to those specific users), the service auditor considers the possible effect of such misstatements on the decisions that may be made by that specific subset of report users.

2.109 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 .17 of AT-C section 205 requires the service auditor to reconsider materiality. Chapter 3 of this guide discusses materiality considerations during the performance of the SOC 2® examination in further detail.

Performing Risk Assessment Procedures

Obtaining an Understanding of the Service Organization's System

2.110 The service auditor should obtain an understanding of the service organization's system, including controls within the system. That understanding should include the service organization's processes and procedures used to do the following:

a. Prepare the description of the service organization's system, including the determination of the service organization's service commitments and system requirements

b. Identify the controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria

c. Assess the suitability of the design of the controls

d. In a type 2 examination, assess the operating effectiveness of controls

2.111 Based on paragraph .14 of AT-C section 205, the service auditor's understanding should be sufficient to do the following:

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

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

2.112 If the service organization has an internal audit function, the service auditor's understanding of the service organization's system should include the following:

a. The nature of the internal audit function's responsibilities and how the internal audit function fits in the service organization's organizational structure

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

The service auditor's responsibilities when a service organization has an internal audit department are discussed further beginning in paragraph 2.133.

2.113 Obtaining an understanding of the service organization's system, including related controls, assists the service auditor in the following:

- Identifying the boundaries of the system and how it interfaces with other 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 specified period to achieve them

2.114 When a separate SOC 2® report exists for a subservice organization, obtaining and reading the SOC 2® report and paying particular attention to the CUECs identified by the subservice organization in the report helps the service auditor evaluate whether controls at the service organization are suitably designed. It also assists the service auditor in evaluating the CSOCs identified by service organization management and evaluating whether there are any CUECs identified in the subservice organization's SOC 2® report that are the responsibility of the service organization's user entities and that should be included in the service organization's description of its CUECs.

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

- Inquiring 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
- Observing operations and inspecting documents, reports, and printed and electronic records of transaction processing
- Inspecting a selection of agreements between the service organization and its user entities and business partners
- Reperforming the application of a control
- Reading relevant reports received from regulators

2.116 One or more of the procedures discussed in the preceding paragraph may be accomplished through the performance of a walk-through. 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 program 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.

2.117 Service organization management may use either a formal or an informal process to prepare the description of the service organization's system. For example, a small service organization that prepares only one report per year is likely to have an informal process in which a few employees with personal knowledge of the operation of the system are assigned responsibility

for drafting the description of the service organization's system and the draft is reviewed by senior management. A large service organization with many interrelated services and multiple reports that address systems that span many functional units is more likely to have a formal process. Such a process is likely to include a project management role that coordinates preparation of the description by different functional areas and review of the description by key executives across the organization. These two different types of processes are likely to be subject to different sources of misstatement. An understanding of the service organization's process for preparing the description may assist the service auditor in

- identifying possible sources of material misstatement in the description,
- determining the likelihood of such misstatements, and
- designing procedures to evaluate whether the description is presented in accordance with the description criteria.

2.118 An understanding of the process for determining the risks that would prevent the service organization's controls from providing reasonable assurance that the service organization's service commitments and system requirements were achieved, and for designing and implementing controls to address those risks, may assist the service auditor in identifying deficiencies in the design of controls. Some service organizations have a formal risk assessment process based on the applicable trust services criteria. In those circumstances, the service auditor may be able to inspect the risk assessment and controls documentation prepared by management to obtain an understanding of this process.

2.119 Often the service organization's system of internal control includes monitoring activities and system reports for management that permit management to continuously or periodically monitor the operating effectiveness of controls. Management may also make use of internal audit evaluations as part of its assessment of the effectiveness of controls. Finally, management may periodically perform specific procedures to assess the effectiveness of controls through controls self-assessment programs and functions that are responsible for testing the effectiveness of controls. In most cases, management will use a combination of the various assessment techniques. Most controls assessment techniques include documentation of their performance, permitting the service auditor to inspect the documentation as part of obtaining an understanding of the system.

Assessing the Risk of Material Misstatement

2.120 The service auditor's understanding of the service organization's system and related controls should be sufficient to enable the service auditor to do the following:

- Identify and assess the risks that
  - — the description of the service organization's system that was implemented and operated is not presented in accordance with the description criteria.
  - — because of deficiencies in the design of controls, the controls are not suitably designed throughout the specified period to provide reasonable assurance that the

service organization's service commitments and system requirements based on the applicable trust services criteria would be achieved.

— in a type 2 examination, the controls did not operate effectively throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved.

- Provide a basis for designing and performing further procedures that are responsive to the assessed risks and for obtaining reasonable assurance to support the service auditor's opinion on the description, the suitability of design of controls, and, in a type 2 examination, the operating effectiveness of controls.

2.121 When assessing the risks of material misstatement, paragraph .15 of AT-C section 205 states that the service auditor should obtain an understanding of internal control, which, in the case of a SOC 2® examination, focuses on obtaining an understanding of controls over the preparation of the description, evaluating their design, and determining whether they have been implemented by making inquiries of the personnel responsible for the description and by performing other procedures. In addition, the service auditor should consider the controls, including monitoring activities that the service organization has designed and implemented, that provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

2.122 The service auditor should also consider whether the risk assessment procedures and other procedures related to obtaining the understanding indicate 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, misappropriation of user entity or business partner 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.

2.123 As previously discussed, the risk of material misstatement relates to the likelihood and magnitude of the risks that threaten the achievement of the service organization's service commitments and system requirements and whether the controls the service organization has designed, implemented, and operated were effective in mitigating those risks. In the SOC 2® examination, risk assessment often begins with identifying and assessing the types, likelihood, and impact of risks that affect the preparation of the description, the suitability of design of controls, and, in a type 2 examination, the operating effectiveness of controls within the system. For example, risks to the achievement of the service organization's service commitments and system requirements may arise from any of the following:

- Intentional (for example, fraud) and unintentional internal and external acts
- Identified threats and vulnerabilities to and deficiencies of the system
- The use of subservice organizations that store, process, or transmit sensitive information on the service organization's behalf

- The type of employee personnel (finance, administrative, operations, IT, sales and marketing, and so on) and others (contractors, vendor employees, business partners, and so on) with access to the system
- The lack of CUECs and CSOCs, when those controls are necessary, that are suitably designed and, in a type 2 examination, operating effectively

2.124 The risk of material misstatement may also be affected by inherent risks that affect the preparation of the description of the service organization's system and the suitability of design of controls and, in a type 2 examination, the operating effectiveness of the service organization's controls. Paragraph .A10*a*i of AT-C section 105 defines *inherent risk* as the susceptibility of the subject matter 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 subservice organizations.

2.125 Once the service auditor has assessed the risks, the service auditor should consider the controls the service organization has designed, implemented, and operated to mitigate those risks. As required by paragraph .18 of AT-C section 205, the service auditor should consider the assessed risk of material misstatement as the basis for designing and performing further procedures whose nature, timing, and extent (*a*) are responsive to assessed risks of material misstatement and (*b*) allow the service auditor to obtain reasonable assurance about whether the description is presented in accordance with the description criteria, whether the controls were suitably designed, and, in a type 2 examination, whether the controls operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

2.126 Most of the service auditor's procedures in forming an opinion on the description and the suitability of controls and, in a type 2 examination, the operating effectiveness of controls consist of obtaining and evaluating evidence. Procedures to obtain evidence include inspection, observation, reperformance, and analytical procedures, often in some combination, in addition to inquiry. Chapter 3 provides additional guidance on performing examination procedures in the SOC 2® examination.

Considering Entity-Level Controls

2.127 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 communication and information (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.

2.128 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.

2.129 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.

2.130 The service auditor should understand the root cause of any identified deficiencies in entity-level controls and 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

2.131 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. The description of the service organization's system presented in appendix D illustrates such disclosures. It also illustrates, in section 4 of the description, the tests the service auditor may perform to determine whether the entity-level controls operated effectively throughout the period.

Understanding the Internal Audit Function

2.132 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.

2.133 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.

2.134 If the service organization has an internal audit function, as part of understanding the service organization's system, the service auditor ordinarily obtains an understanding of the following:

a. The nature of the internal audit function's responsibilities and how the internal audit function fits into the service organization's organizational structure

b. The activities performed or to be performed by the internal audit function as they relate to the SOC 2® examination

2.135 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 should consider the effect on his or her conclusions regarding the effectiveness of monitoring activities.

2.136 When obtaining an understanding of the internal audit function's responsibilities and activities, the service auditor makes inquiries of internal audit personnel and reads 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 should be taken into consideration as part of the risk assessment and in determining the nature, timing, and extent of the service auditor's planned procedures.

Planning to Use the Work of Internal Auditors

2.137 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.

2.138 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.[8]

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

2.139 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 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

2.140 When evaluating competence, the service auditor should consider the attainment and maintenance of knowledge and skills of the internal audit

[8] Regardless of whether the service auditor plans to use the 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.

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

2.141 When evaluating objectivity, the service auditor should 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)[9]

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

2.142 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.

---

[9] As indicated in paragraph .A18 of AT-C section 105, 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.

2.143 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 should be used. However, as noted in paragraph .A46 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.

2.144 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

2.145 The extent to which the service auditor plans to use the work of the internal audit function is a matter of professional judgment. Because the service auditor has sole responsibility for expressing an opinion on the description, on the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls, the service auditor makes all significant judgments in the examination, including when to use the work of the internal audit function in obtaining evidence.

2.146 To prevent undue use of the internal audit function in obtaining evidence, the service auditor uses less of the work of the internal audit function and performs 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 .43 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.

2.147 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.

Coordinating Procedures With the Internal Auditors

2.148 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 with management the planned use of the work of the internal audit function as a basis for coordinating the work of internal auditors with the service auditor's procedures. 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.

2.149 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

2.150 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).

2.151 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.

2.152 When planning to use internal auditors to provide direct assistance, paragraph .41 of AT-C section 205 requires the service auditor to obtain written acknowledgment from management 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

2.153 When using the work of the internal audit function, 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

2.154 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, the suitability of design of controls, and, in a type 2 examination, the operating effectiveness of controls.

2.155 Paragraph .31 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

2.156 If the service auditor expects to use the work of the other practitioner, paragraph .31 of AT-C section 105 requires the service auditor to 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 2.36 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. (Upon completion of the other

practitioner's work, 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 2.157*c*ii, 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.)

2.157 In applying paragraph .31 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 would need to comply with the requirements in paragraph .31 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 commitment 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 .31 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.

2.158 When using the work of an other practitioner, paragraph .A57 of AT-C section 205 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.

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

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

2.160 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 .36 of AT-C section 205 requires the service auditor to do the following:

a. Evaluate the specialist's competence, capabilities, and objectivity.

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.

2.161 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, he or she 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 should 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 his or her work will help achieve the objectives of the engagement.

2.162 When evaluating the objectivity of the service auditor's external specialist, the service auditor may inquire of 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 management (or the engaging party, if different) of which the specialist is aware.

2.163 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, he or she 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.

2.164 When considering the relevance of the service auditor's specialist's field of expertise to the engagement, the service auditor should consider (*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, and (*d*) the nature of internal and external data or information used by the service auditor's specialist.

2.165 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 .38 of AT-C section 205 states 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, such as involvement in the firm's recruitment and training programs

2.166 In addition to the matters discussed in this section, paragraph .36 of AT-C section 205 also requires the service auditor to 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 3.170.

Accepting and Planning a SOC 3® Examination

2.167 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 4.112.

2.168 Management's responsibilities during acceptance and planning of a SOC 3® examination include the following:

- Defining the scope of the examination, as discussed in paragraph 2.04
- 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 2.12 and throughout this chapter

2.169 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.

2.170 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. 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. 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.

2.171 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.

2.172 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 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.

Designing Overall Responses to the Risk Assessment and Obtaining Evidence

3.01 Assessment of the risks of material misstatement is affected by many factors, including materiality considerations (see paragraph 3.05) and the service auditor's understanding of the effectiveness of the control environment or other components of internal control related to the service provided to user entities and business partners. 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 ineffective aspects of the control environment or other components of internal control.

3.02 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 input to output designed to identify exceptions) or may decide to test the entire population to determine whether controls are operating effectively.

3.03 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)

3.04 After the service auditor has assessed the risks of material misstatement, paragraphs .20–.21 of AT-C section 205, *Examination Engagements*,[1] require the service auditor to respond to the assessed risks when designing and performing examination procedures. Specifically, they require the service auditor to (*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.

Considering Materiality in Responding to the Assessed Risks and Planning Procedures

3.05 Paragraph .A15 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 in light of the surrounding circumstances.

3.06 In a SOC 2® examination, the service auditor needs to consider materiality 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 allows the service auditor to prioritize testing efforts and supports an effective and efficient engagement.

3.07 When considering materiality regarding the description, the service auditor should consider whether description misstatements (including omissions), individually or in the aggregate, could reasonably be expected to influence relevant decisions of the broad range of report users. Paragraph 3.67 discusses materiality considerations when evaluating whether the description presents the system that designed and implemented in accordance with the description criteria.

3.08 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 3.161.

Defining Misstatements in This Guide

3.09 Paragraph .10 of AT-C section 105, *Concepts Common to All Attestation Engagements*, defines a *misstatement* as follows:

> A difference between the measurement or evaluation of the subject matter by the responsible party and the proper measurement or evaluation of the subject matter based on the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions. In certain engagements, a misstatement may be referred to as a *deviation*, *exception*, or *instance of noncompliance*.

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

3.10 In this guide, the following terms are used 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 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.

Description misstatements and deficiencies that are material are likely to result in a modification of the service auditor's opinion, whereas those that are immaterial would not.

3.11 The service auditor accumulates misstatements and deficiencies related to each of the subject matters of the examination—the description, the suitability of design of controls, and, in a type 2 examination, the operating effectiveness of controls—to determine whether the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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, "Forming the Opinion and Preparing the Service Auditor's Report," discusses the effect that the service auditor's opinion modification on one subject matter may have on the other subject matters.

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

3.12 As previously discussed, the description of the service organization's system 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.

3.13 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 supplement A, "2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report." Generally, management prepares the description from documentation supporting the system of internal control and system operations, as well as from consideration of the policies, processes, and procedures (controls) within the system used to provide the services.

3.14 Although the description is generally narrative in nature, there is no prescribed format for the description. In addition, flowcharts, matrixes, tables, graphics, context diagrams, or a combination thereof, may be used to supplement the narratives contained within the description.

3.15 Additionally, the description can be organized in a variety of different ways. 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). Alternatively, it may be organized by components of the system (infrastructure, software, people, data, and processes and procedures) and 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.

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 or the services provided by the system, particularly if certain aspects of those services are not relevant to the report users or are beyond the scope of the SOC 2® examination. For example, a service organization's processes related to billing for the services provided to user entities are unlikely to be relevant to report users. Similarly, although the description may include procedures within both manual and automated systems by which services are provided, the description need not necessarily disclose every step in the process.

3.17 Ordinarily, a description of a service organization's system in a SOC 2® examination is presented in accordance with the description criteria when it does the following:

- Describes the system that the service organization has implemented (that is, placed into operation) to provide the services
- Includes information about each description criterion, to the extent it is relevant to the system being described
- Does not inadvertently or intentionally omit or distort information that is likely to be relevant to report users' decisions

3.18 Although the description should 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.

3.19 A description that (*a*) states or implies that certain IT components exist when they do not, (*b*) states or implies that certain processes and controls have been implemented when they are not being performed, or (*c*) contains statements that cannot be objectively evaluated (for example, advertising puffery) is not presented in accordance with the description criteria.

3.20 The service auditor should obtain and read the description of the service organization's system and perform procedures to determine whether the description is presented in accordance with the description criteria. Determining whether the description of the service organization's system is presented in accordance with the description criteria involves comparing the service auditor's understanding of the service provided to user entities to the system through which the service is provided based on the trust services category or categories included within the scope of the examination.

3.21 When evaluating whether the description is presented in accordance with the description criteria, the service auditor should consider the implementation guidance for each criterion in supplement A. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. Because the implementation guidance does not address all possible situations, the service auditor should consider the specific facts and circumstances of the service organization when applying the description criteria.

3.22 Determining whether the description of a service organization's system is presented in accordance with the description criteria involves, among other things, evaluating whether each control stated in the description has been implemented. Controls have been implemented when they have been placed in operation rather than existing only in the description. 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, "Accepting and Planning a SOC 2® Report." In addition, the procedures described beginning in paragraph 3.59 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 modify the description to remove the controls from the description, the service auditor should consider the effect of the misstatement on his or her conclusion about the description. Paragraph 4.70 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, the service auditor should consider whether the failure to implement those controls results in controls not being suitably designed. (Paragraph 3.156 discusses a situation in which controls do not operate during the period of the examination.)

The Service Organization's Service Commitments and System Requirements

Disclosures About Service Commitments and System Requirements

3.24 As discussed in chapter 2, description criterion DC2, *The principal service commitments and system requirements*, requires service organization management to disclose the principal service commitments and system requirements in the description. Disclosure of a service organization's principal service commitments and system requirements is necessary to enable 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. (Although DC2 only requires disclosure of the *principal* service commitments and system requirements, service organization management is responsible for designing the system to achieve the service commitments it makes to user entities and the system requirements that are necessary to enable the system to achieve them.)

3.25 The service commitments that a service organization makes to user entities may 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 relevant to the common needs of the broad range of SOC 2® report users.

3.26 When deciding whether the disclosures stated in the description are appropriate, the service auditor may consider matters such as the following:

a. Are the 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 may 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.

b. When the SOC 2® report is designed for a broad range of users, does the description summarize 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 addresses the commitments made to all user entities but is silent on the commitments made to specific user entities.

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

3.27 As discussed in chapter 2, during the engagement acceptance process, the service auditor considers whether the service commitments and system requirements stated in the description are appropriate for the engagement. The prior section of this chapter discusses considerations for determining whether related disclosures are appropriate in accordance with description criterion DC2. This section discusses the situation in which, after accepting the SOC 2® examination, the service auditor becomes 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.

3.28 Such a situation might happen when, for example, during the performance of further procedures, the service auditor becomes 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 a requirement would not be achieved. In addition, it did not design, implement, and operate controls to mitigate such risks. Accordingly, the service organization's service commitments and system requirements are incomplete and, therefore, not appropriate in the circumstances. In that situation, the service auditor may conclude that a modification of the opinion is appropriate because 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; or
- Because controls over the objective-setting process were not suitably designed, 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.*

3.29 In such a situation, the service auditor should discuss the matter with service organization management. If service organization management is unwilling to revise the service commitments and system requirements to address the service auditor's concerns, the service auditor should consider the effect on his or her opinion. 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 is likely to have a pervasive effect on the SOC 2® examination. Accordingly, it is likely that the service auditor would express an adverse opinion on the description, the suitability of controls, and, in a type 2 examination, the operating effectiveness of controls. Expressing an adverse opinion in a SOC 2® examination is discussed beginning in paragraph 4.54.

Disclosures About Individual Controls

3.30 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 3-1 presents information about each control that generally would be included in the description.

Table 3-1

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 codes***[2] 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.
Who: The party responsible for 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***.

[2] 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*
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.
When: The frequency with which the control is performed, or the timing of its occurrence	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.

3.31 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, 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 4.15.

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

Disclosures About System Incidents

3.33 Description criterion DC4 requires service organization management to 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. Specifically, 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

3.34 The following is an example of disclosures about an identified system incident that resulted in a significant failure of the service organization to achieve one of its availability commitments:

> System incidents for XYZ may include, but are not limited to, the following:
>
> - Unauthorized disclosure of sensitive information
> - Theft or loss of equipment that contains potentially sensitive information
> - Extensive virus or malware outbreak or traffic
> - Attempts (either failed or successful) to gain unauthorized access to a system or its data
> - Compromised user account
> - Extensive disruption of the TMS services
>
> In February 20XX, XYZ experienced a denial-of-service attack on its transportation management system (TMS) that supports the transportation managements 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 attempted attack prevented XYZ from achieving its availability commitments and requirements based on trust services criterion A1.2, *The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.*

3.35 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, the service auditor would modify the opinion on suitability of design or operating effectiveness, or both.

Disclosures About Complementary User Entity Controls and User Entity Responsibilities

3.36 As discussed in chapter 2, complementary user entity controls (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.

3.37 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*.

3.38 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. However, because user responsibilities are often voluminous, they are often communicated through other methods (for example, by describing them in user manuals). Consequently, disclosure of user entity responsibilities in the description is usually not practical. As a result, description criterion DC7 does not require service organization management to disclose user entity responsibilities. Instead, management identifies in the description the types of communications it makes to external users about user entity responsibilities. The form and content of such communication is the responsibility of service organization management.

3.39 When service organization management communicates user entity responsibilities only to specified parties (such as in contracts with user entities), the service auditor considers whether other intended users of the SOC 2® report are likely to misunderstand it. If other intended users are likely to misunderstand it, the service auditor should restrict the report to specified parties who are unlikely to misunderstand the examination and the report. If service organization management does not want the service auditor to restrict the use of the report, 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.

3.40 When service organization management includes significant user entity responsibilities in the description, management and the service auditor evaluate those disclosures as part of the evaluation about whether the description is presented in accordance with the description criteria.

3.41 The description is presented in accordance with the description criteria if the CUECs are complete, accurately described, and relevant to the service organization's achievement of its service commitments and system requirements based on the applicable trust services criteria. 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 he or she considers necessary.

Disclosures Related to Subservice Organizations

3.42 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

3.43 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

3.44 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 controls at the service organization and controls at the subservice organization.

3.45 In addition, as also discussed in chapter 2, 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

3.46 When the carve-out method is used, management does not include a description of the controls that operate only or primarily 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

3.47 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 at the subservice organization.

3.48 Service organization management is not required to disclose the identity of the subservice organization. However, that information is typically needed by 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.

3.49 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 is not specific 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.

3.50 Regardless of whether the carve-out or inclusive method is selected, the description of the service organization's system and the scope of the service auditor's examination include the controls designed, implemented, and operated at the service organization to monitor the effectiveness of controls at the subservice organization. Controls over subservice organizations are usually a necessary part of a system of internal control in order for it to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. These types of controls are evaluated using trust services criterion CC9.2, *The entity assesses and manages risks associated with vendors and business partners*. Such monitoring controls may include some combination of (1) ongoing monitoring to determine that potential issues are identified timely and (2) separate evaluations to determine that internal controls are effective over time. Examples of monitoring controls include reviewing and reconciling output reports, holding periodic discussions with subservice organization personnel, making regular site visits to the subservice organization, performing tests of controls at the subservice organization by members of the service organization's internal audit function, reviewing type 1 or type 2 reports on the subservice organization's system, and monitoring external communications (such as customer complaints) relevant to the services provided by the subservice organization.

3.51 Chapter 4 presents illustrative paragraphs that might be added to the service auditor's report when there are description misstatements related to disclosures about the use of one or more subservice organizations.

Disclosures About Complementary Subservice Organization Controls

3.52 As discussed in chapter 2, when using the carve-out method, there may be situations in which the achievement of one or more of the service organization's service commitments or system requirements based on the applicable trust services criteria 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 stated 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 controls lists.

3.53 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 includes the subservice organization's responsibilities for implementing them and indicates 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.

3.54 Because CSOCs 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 or system requirements are achieved based on the applicable trust services criteria, the service auditor also considers CSOCs when evaluating the suitability of design of controls, as discussed beginning at paragraph 3.152.

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

3.55 Description criterion DC9 requires the description to 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.

3.56 Significant changes to be disclosed consist of those that are likely to be relevant to the broad range of report users. Disclosure of such changes is expected to include an appropriate level of detail, such as the date the changes occurred and how the system differed before and after the changes. Examples of significant changes to a system include the following:

- Changes to the services provided
- Significant changes to IT and security personnel
- Significant 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)

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

3.57 In some cases, a service auditor may issue a type 2 report covering a period of time beginning after the period of time in which a prior type 2 report ended. In other words, the type 2 reports do not cover a continuous period, which results in a gap between the periods covered by the reports.

3.58 If a significant change occurs during the gap period, service organization management may decide that such changes are likely to be considered significant to report users. In that case, management may include a description of such changes 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.

Procedures to Obtain Evidence About the Description

3.59 The service auditor may perform a variety of procedures to obtain evidence about whether the description presents the system that was designed and implemented in accordance with the description criteria, including a combination of the following:

- Discussing with management and other service organization personnel the content of management's assertion and the description
- Reading the service organization's annual report, if any, to understand
  - — the nature of the service organization's operations and the types of services offered to user entities and business partners,
  - — the service organization's network environment and the information and systems the service organization uses when interacting with customers, and
  - — other matters related to the system
- Reading the service organization's service commitments and system requirements to determine whether they are appropriate for the specific engagement circumstances (Paragraphs 2.60 and 3.27 discuss the appropriateness of the service organization's service commitments and system requirements.)
- 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 contracts with user entities and business partners (such as performance or service level agreements), marketing materials distributed to user entities and business partners or posted on the service organization's website, and other available documentation to
  - — better understand the specific services provided to user entities and
  - — evaluate whether the controls the service organization has implemented are suitably designed to achieve the service organization's service commitments to those user entities (for example, reading service level agreements may help the service auditor understand the specific processing commitments made, including commitments related to the timeliness of processing, expected rates of error, or individuals who have access to confidential information)
- Observing controls or other activities performed by service organization personnel
- 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 types of 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 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;
  - — 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 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 sample contracts with subservice organizations and vendors (for example, contract templates or a selection of contracts) 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 and vendors, including the service organization's process for assessing and managing system risks associated with those subservice organizations and vendors;
  - — the process the service organization uses to identify user entity responsibilities or CUECs that should be in place at the service organization, when the carve-out method is used to present the services provided by a subservice organization; and

  - — the procedures the service organization performs to monitor the effectiveness of controls performed by such subservice organizations and vendors, when 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
- Reading documents describing laws, regulations, or industry standards relevant to the service organization's service commitments and system requirements

3.60 Performing walk-throughs provides evidence about whether the controls within the system have been implemented. Performing a walk-through involves making inquiries of service organization management and other personnel and requesting that they 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, and 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.

3.61 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.

3.62 When performing the SOC 2® examination, the service auditor should also obtain an understanding of changes in the service organization's system implemented during the period covered by the examination. If the service auditor believes that the changes would be considered significant by the broad range of report users, the service auditor should determine whether those changes have been 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. If such changes have not been included in the description, the service auditor may ask management to amend the description to include

that information. If service organization management refuses to include this information in the description, the service auditor should consider the effect on his or her opinion on the description.

3.63 A conclusion 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.

Considering Whether the Description Is Misstated or Otherwise Misleading

3.64 Based on paragraph .60 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 .A73 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,[3] depending on their nature and significance.

3.65 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 4.95.

3.66 Although the description should be presented in accordance with the description criteria, paragraph .60 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.

3.67 As part of the service auditor's evaluation of whether the description is misleading within the context of the engagement, the service auditor may consider whether the description

- contains statements that cannot be objectively evaluated. For example, describing a service organization as being the "world's best" or "most respected in the industry" is subjective and, therefore, could be misleading to report users.
- contains or implies certain facts that are not true (for example, that certain IT components exist when they do not or that certain processes and controls have been implemented when they are not being performed).

---

[3] Subsequent events are discussed beginning in paragraph 3.213.

- 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).

3.68 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 information. If service organization management refuses to amend the description, the service auditor should consider the effect on his or her opinion about the description.

Identifying and Evaluating Description Misstatements

3.69 As discussed in paragraph 3.10, the term *description misstatement* is used when describing differences between (or omissions in) the description and the description criteria. The following are examples of description misstatements:

- *Inclusion of inappropriate information.* For example, controls that have not been implemented, information that is not measurable, or service commitments and system requirements that are incomplete

- *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*

3.70 Paragraph .45 of AT-C section 205 requires the service auditor to accumulate description misstatements or deficiencies identified during the engagement, other than those that are clearly trivial. In addition, the service auditor should accumulate deviations that have not been determined to rise to the level of a deficiency and consider whether, in the aggregate, they result in a deficiency.

3.71 The service auditor also considers the potential effect on the description of deficiencies or deviations in 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 3.72, the service auditor should modify the opinion on the description. 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.

Materiality Considerations When Evaluating Whether the Description Is Presented in Accordance With the Description Criteria

3.72 As previously discussed, applying the description criteria requires judgment. One of those judgments involves the informational needs of report users. For most SOC 2® reports, there is a broad range of specified parties. Therefore, the description is intended to meet the common informational needs of the specified parties and does not ordinarily include information about every aspect of the system that may be considered important to each individual report user. However, an understanding of the perspectives and information needs of the broad range of intended SOC 2® report users is necessary to determine whether the description is presented in accordance with the description criteria and is sufficient to meet their needs. As discussed in chapter 1, "Introduction and Background," users of a SOC 2® report are expected to have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide them, among other matters. As a result, the service auditor assumes that the report users have such knowledge and understanding.

3.73 When considering materiality regarding the description, the service auditor considers whether misstatements or omissions in the description, individually or in the aggregate, could reasonably be expected to influence decisions of specified parties to the SOC 2® report. For example, in a SOC 2® examination on controls relevant to privacy, the service auditor may determine that the description fails to disclose a principal service commitment involving compliance with the European Union's General Data Protection Regulation, to which the service organization is subject. If the service auditor determines that such information could reasonably be expected to influence the decisions of SOC 2® report users, the service auditor may conclude that the 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.[4]

3.74 Paragraph .A15 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).

3.75 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.

3.76 Examples of qualitative factors ordinarily considered when determining whether the description is presented in accordance with the description criteria include the following:

- Whether the description of the service organization's system includes the significant aspects of system processing

[4] 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.

- Whether the description is prepared at a level of detail likely to be meaningful to report users
- Whether each of the relevant description criteria in supplement A has been addressed without using language that omits or distorts the information
- Whether the characteristics of the presentation are appropriate, given that the description criteria allow for variations in presentation

3.77 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 and 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. The description includes such information because it is likely to be relevant to report users and, therefore, such information would be considered 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 tape as a control, but it has not identified physical security controls over the tape storage location as a control because management has concluded that the 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 material or 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.

3.78 Paragraph .17 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 and Evaluating Evidence About the Suitability of the Design of Controls

3.79 Suitably designed controls, if complied with satisfactorily, 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. Paragraph .15 of AT-C section 205 states that 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.

3.80 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 that threaten the achievement of the service commitments and system requirements.

3.81 Evaluating the suitability of the design of controls involves assessing whether the controls stated in the description 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. When making this evaluation, the service auditor does the following:

- Obtains an understanding of management's risk assessment process as discussed in the subsequent paragraph and assesses the completeness and accuracy of management's identification of those risks
- Evaluates the linkage between the controls identified in the description and those risks
- Determines that the controls have been implemented

If the inclusive method is used to present the services and controls performed by a subservice organization, the service auditor also performs these procedures with respect to the controls at the subservice organization.

3.82 The service auditor's evaluation of management's risk assessment process (that is, the assessment of potential system events and circumstances that could threaten the achievement of the service organization's service commitments and system requirements) includes consideration of items such as the following:

- The process service organization management uses to
  - — assess risk and design and implement controls to mitigate those risks,
  - — identify the service organization's service commitments and system requirements,
  - — identify information used by the system to provide the service to user entities and business partners and determine the threats to that information,
  - — incorporate information from its monitoring activities that identify potential system events and circumstances that were previously not considered
  - — identify 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
- Evidence about the operating effectiveness of controls that indicated there was a deficiency in the design of the controls

- The frequency with which service organization management updates the risk assessment and supporting risk management processes and controls
- Whether service organization management uses an appropriate security framework for managing its system processes and controls (for example, the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity" [NIST cybersecurity framework] or International Standardization Organization/International Electrotechnical Commission [ISO/IEC] Standards 27001 and 27002) as part of its assessment and management process

3.83 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 policies and procedures that are less formal and detailed but sufficient for the service auditor to evaluate;
- 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.

3.84 Other matters that may be relevant when determining whether controls are suitably designed include the following:

- Whether the applicable control or set of controls adequately addresses the risks that threaten the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria.
- 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.
- 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.
- 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 by service organizations.

3.85 Identified risks that may affect the achievement of the service organization's service commitments and system requirements also encompass fraud, such as management override of identified controls at the service organization, 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.

The service auditor should consider the risks of both fraud and errors when evaluating the suitability of the design of controls.

3.86 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 in place at the service organization. If the subservice organization has identified such responsibilities or CUECs, the service auditor should evaluate whether service organization management has considered these responsibilities or CUECs in its assessment of risks that would prevent the service organization from achieving one or more of its service commitments or system requirements.

3.87 When considering the suitability of design, the service auditor may determine that some system components (such as network access points, databases, or transactions) are subject to greater threats or have vulnerabilities that are more likely to be exploited. In such instances, controls designed and implemented to prevent or detect system events associated with these threats and vulnerabilities may require greater precision and reliability to be considered suitably designed.

Additional Considerations for Subservice Organizations

3.88 As previously discussed, service organization management is responsible for monitoring the suitability of design and operating effectiveness of controls at a subservice organization, regardless of whether management has elected to use the inclusive or carve-out method. For that reason, the description needs to disclose the controls that 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 3.50. 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 3.154. If a type 1 or type 2 report is used as part of the monitoring of services provided by the subservice organization, the service organization may indicate the type of report used in its description. A service organization 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, the service organization may indicate in its description whether the subservice organization's report is a type 1 or type 2 report.

3.89 When a service organization uses a subservice organization, the service organization may need to implement controls to achieve its service commitments and system requirements. The controls to be implemented may be communicated in an authoritative communication or as CUECs in a type 1 or type 2 report provided by the subservice organization. If the subservice organization's type 1 or type 2 report identifies the need for CUECs at the service organization, the service organization controls stated in the description should include controls the service organization has implemented to address the CUECs identified.

3.90 If the service organization obtains the subservice organization's type 1 or type 2 report that identifies the need for CUECs, during planning, service organization management considers how to address that information in its description. For example, a service organization that outsources aspects of its technology infrastructure to a subservice organization may find that the subservice organization's description of its systems includes the following CUEC:

> User entities should have controls in place to restrict access to system resources to appropriate user entity personnel.

3.91 To address the CUEC included in the subservice organization's description, the service organization 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 an Applicable Trust Services Criterion

3.92 The service organization may have different 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 multiple controls when determining whether the controls have been suitably designed to address each of the risks associated with a particular criterion.[5] 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 the other controls the

[5] Supplement B, "2018 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy," of this guide 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 based on the applicable trust services criteria were achieved.

service organization has designed and implemented to achieve the other aspects of that criterion.

3.93 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 conclude that controls were not suitably designed to process transaction requests received via telephone.

Multiple Controls to Achieve the Service Organization's Service Commitments and Service Requirements Based on the Same Applicable Trust Services Criterion

3.94 In other situations, the service organization may perform several control activities directed at meeting an applicable trust services criterion in order to achieve its service commitments and service requirements. Consequently, if the service auditor evaluates certain control activities as being ineffective in meeting a particular criterion, the service auditor may be able to obtain evidence about the operating effectiveness of other implemented control activities. If the service auditor determines that the identified control is not suitably designed to meet the criterion, and determines that one or more other implemented controls are suitably designed to meet it, the service auditor would ordinarily ask management to revise the description to exclude the control that is not suitably designed and include the control or controls that are suitably designed to meet the criterion.

Procedures to Obtain Evidence About the Suitability of Design of Controls

3.95 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).

3.96 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

3.97 As discussed beginning in paragraph 2.56, 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 identification of risks and the suitability of design of the controls implemented to mitigate those risks.

3.98 When using evidence and other information to evaluate the suitability of the design of the controls within the system, the service auditor should consider the following information about the controls:

- The frequency or timing of the occurrence or performance of the control
- 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)
- 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)
- Evidence that contradicts the assertion that the control is functioning as designed, such as the rate of system incidents identified related to the control

Additional Considerations When the Carve-Out Method Is Used for a Subservice Organization

3.99 If the service organization uses the carve-out method for a subservice organization, the service auditor also evaluates 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 also considers 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. 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 prepared using this guide

3.100 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*.

Identifying and Evaluating Deficiencies in the Suitability of Design of Controls

3.101 A deficiency in the design of a control occurs when

- a necessary control is missing or
- an existing control is not properly designed (for example, because the control does not address the risks that threaten the achievement of one or more of the service organization's service commitments or system requirements).

3.102 In contrast, a deficiency in the operation of a control exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or competence to perform the control effectively. A service organization may be able to correct a deficiency in the operation of a control, for example, by designating a more qualified individual to perform the control. However, if the design of the control is deficient, the control will not be effective regardless of who performs it. For that reason, the service auditor often would not test the operating effectiveness of a control that has a deficiency in design. Instead, the service auditor generally would consider the design of other controls that address the same risks.

3.103 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.

3.104 After performing the procedures and considering the guidance in paragraphs 3.79–3.105, the service auditor should accumulate instances in which controls were not suitably designed or were not properly implemented, which are considered deficiencies in the SOC 2® examination. As part of the evaluation, the service auditor should assess 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. The service auditor should also consider the potential effect of other factors that may affect the opinion on the suitability of the design of controls, such as misstatements in the description 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 3.161.

3.105 Paragraphs 4.79–4.88 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 and Evaluating Evidence About the Operating Effectiveness of Controls in a Type 2 Examination

3.106 Controls are suitably designed if they have the potential to meet the applicable trust services criteria, thereby enabling the service organization's controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. 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.

3.107 In the type 2 examination, the service auditor tests the operating effectiveness of the controls stated in the description based on the applicable trust services criteria. The service auditor performs procedures (known 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.

3.108 When performing a type 2 examination, description criterion DC9 indicates that a description should disclose relevant details of changes to the service organization's system during that period. If the service auditor believes changes to the system would be considered significant by report users, the service auditor should determine whether the description includes such information. In addition, the service auditor should consider whether superseded controls are relevant to the achievement of one or more service commitments or system requirements based on the applicable trust services criteria. If so, the service auditor should, if possible, test the superseded controls before the change. If the service organization has used the inclusive method, the service auditor should consider changes to controls at both the service organization and the subservice organization. Paragraph 4.72 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.

3.109 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

3.110 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.

3.111 The service organization's control environment, risk assessment, information and communications, and monitoring components of internal control related to the service provided to user entities and business partners may enhance or mitigate the effectiveness of specific controls. If the service auditor determines that certain aspects of the control environment or other components of the service organization's internal control are not effective, 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 resulting from the less effective aspects of these internal control components. In some situations, the service auditor may conclude that controls are not operating effectively because of deficiencies in one or more of the components of internal control.

3.112 When performing the type 2 examination, the service auditor should test the operating effectiveness of controls that service organization management stated in the description of the service organization's system. By including those controls in the description, service organization management has identified them as part of the system of internal control that provides reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

3.113 When more than one control is necessary to address a risk that would prevent the service organization from achieving one or more of its service commitments and system requirements, the service auditor considers whether a combination of controls is necessary, as discussed in paragraph 3.92. If a combination of controls is necessary, the service auditor considers evidence about whether all the controls are operating effectively; deficiencies are evaluated in the same way. The service auditor also considers the risk that one or more of the controls will not operate effectively.

3.114 A service organization may have more than one control that addresses a risk that would prevent the service organization from achieving one or more of its service commitments and system requirements. In such situations, if a deficiency exists in the suitability of design of one control, another control may be suitably designed. In that case, the service auditor should perform procedures to test the operating effectiveness of the suitably designed control, identify the control that was tested in the description of tests of controls and results, and determine the effect of the results of those procedures on the service auditor's report.

Nature of Tests of Controls

3.115 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 should do the following:

a. Make inquiries and perform other procedures such as inspection (for example, of documents, reports, or electronic files), observation (for example, of the application of the control), or reperformance, to obtain evidence about the following:

i. How the control was applied (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 other controls and, if so, whether it is necessary to obtain evidence supporting the operating effectiveness of those other controls.

c. Determine an effective method for selecting the items to be tested to meet the objectives of the procedure.

3.116 Inquiry alone does not provide sufficient appropriate evidence of the operating effectiveness of controls. Some tests of controls provide more convincing evidence of the operating effectiveness of controls than others. 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 supplement the observation with other procedures to obtain sufficient appropriate evidence regarding the operating effectiveness of the control throughout the period. For example, the service auditor may inspect the video tapes that monitor the entrance of the facility, select a sample of individuals who enter the building, and determine whether the names of those individuals were included on the service organization's list of authorized individuals during that period.

3.117 Because of the nature and methods of data storage used by the system, the service auditor may find the use of analytics to be a highly effective technique in performing his or her procedures, such as in the following examples:

- 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.
- 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 perform procedures to validate the completeness and accuracy of the information received from the entity, as discussed beginning in paragraph 3.121.

3.118 The type of control being tested may affect the nature, timing, and extent of the testing performed by the service auditor. For example, for some controls, operating effectiveness is evidenced by documentation. In such circumstances, the service auditor may inspect the documentation. Other controls may not leave evidence of their operation that can be tested at a later date, and accordingly, the service auditor may need to test the operating effectiveness of such controls at various times throughout the specified period.

3.119 There may be instances in which evidence that would have demonstrated the operating effectiveness of a control may be lost, misplaced, or inadvertently deleted by the service organization. In such instances, the service auditor evaluates the type of evidence available and whether the operating effectiveness of the control can be tested through other procedures, such as observation, that would provide sufficient appropriate evidence throughout the period. However, depending on the control activity and its significance, tests such as observation may not alone provide sufficient appropriate evidence. If such tests do not provide sufficient evidence, the service auditor should consider whether other controls are operating effectively. If one or more of the criteria are not met, the service auditor should modify the opinion. When modifying the opinion, the service auditor should consider whether the deficiency results from a failure of the control to operate effectively or from the inadvertent destruction of evidence (for example, the destruction of the computer hard disk on which the evidence was stored).

3.120 In addition to procedures to directly test the operating effectiveness of a control, the service auditor may also perform procedures to indirectly obtain evidence about whether the control functioned to prevent or detect errors and fraud. For example, when testing the operating effectiveness of vulnerability scanning controls, the service auditor may use his or her own vulnerability scanning tool to detect unidentified vulnerabilities to assess the operating effectiveness of those controls. By comparing the results of the independent vulnerability scan to the results of the service organization's vulnerability scanning control, the service auditor can evaluate the effectiveness of the control. As another example, the service auditor might obtain a listing of the system incidents identified throughout the period and compare the vulnerabilities exploited to the controls implemented to identify deficiencies in the design or operation of the related control activities. This testing can be used to identify deficiencies in specific controls designed to prevent or detect those incidents in a timely manner, permitting the service auditor to evaluate the effectiveness of the specific controls.

Evaluating the Reliability of Information Produced by the Service Organization

3.121 When using information produced by the entity, paragraph .35 of AT-C section 205 requires the service auditor to 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

3.122 The reliability of information depends on the nature and source of the information and the circumstances under which it is obtained. From the service auditor's perspective, the following are the three types of information produced by a service organization:

- Information provided by the service organization 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
- Information prepared for user entities, for example, a reporting package provided to user entities, system-generated reports, an invoice, or a payroll file reflecting the results of processing a payroll

3.123 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. As an example, the effectiveness of a control, such as the periodic review of user access, is affected by the completeness and accuracy of the information used to prepare the user access reports. In this situation, the service auditor would inspect the scripts used to create user access reports for accuracy of logic.

3.124 The information may be produced only once or on a recurring basis for use in the execution of a control. The information may be produced manually by management or generated from a system. When the information produced by the system is provided to the service auditor, the service auditor assesses how the information is used, the source of the information, and the impact the information could have on the examination.

3.125 The service auditor identifies the information produced by the service organization while performing procedures to assess the design, implementation, and operating effectiveness of controls within the system. When assessing the information produced, the service auditor should consider the reliability of the information, specifically the completeness and accuracy of the information. For example, if the service auditor intends to test a population of user terminations during the period under examination, the service auditor would perform procedures to determine that the lists of terminated users generated by the human resource management system are complete and accurate.

3.126 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 the data. The information may also provide evidence of the operating effectiveness of a control. When assessing information used in the execution of controls, the service auditor should consider the following factors:

- The level of assurance being sought from the control
- 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)

3.127 As part of evaluating and testing the design of a review control, the service auditor may need to consider obtaining a sufficient understanding and documenting conclusions about the following matters:

- How the control is 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
- The steps involved in investigating and resolving matters identified by the review

The service auditor's test of the precision of each review control may include evaluating the same aspects of the control to determine that the control operated the same way each time it was tested. The service auditor may need to determine whether the evidence gathered through the tests performed demonstrates that the review control consistently identifies appropriate items for follow-up and that matters identified for investigation are 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.

3.128 Questions that may be asked when evaluating the reliability of information produced by the service organization may include the following:

- Where 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)
- How is the information used?
- What affect 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 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?

3.129 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 specific procedures that address this information. 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, the service auditor should evaluate the reliability of the information produced by the service organization throughout the period.

3.130 The following are examples of 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.

Timing of Tests of Controls

3.131 The following are factors that are 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 should be tested through observation
- The significance of the control being tested

3.132 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, provides 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 at an interim period, the service auditor should determine the extent of additional testing necessary for the remaining period.

3.133 Paragraph 4.81 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

3.134 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 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, and 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.

3.135 The service auditor should test the operating effectiveness of the controls throughout the period covered by the examination and determine whether the control has occurred a sufficient number of times to be assessed as operating effectively. The following are examples of how this guidance may be applied by the service auditor:

- 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 test period, the more likely the service auditor will be unable to perform sufficient testing and obtain sufficient appropriate evidence to express an opinion on the operating effectiveness of controls.
- If the examination is for a six-month period from January 1 to June 30, 20XX, and a control operates only annually in December, the service auditor is unable to test the operating effectiveness of the control within the period.

3.136 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.

3.137 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 because of the inexperience of the person performing the controls, the service auditor may decide to increase the number

of items tested in the current examination to determine whether the deficiency was effectively corrected.

3.138 Generally, IT processing is inherently consistent; therefore, the service auditor may be able to limit the testing to one or a few instances of the control 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 should 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 where the automated control is configurable, the service auditor should perform procedures to evaluate the configuration. 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 functionality of the control in the production environment differs from that in the non-production environment and perform procedures to determine that the environment being tested matches that of the production environment.

3.139 Automated application controls may be tested only once or a few times if effective IT general controls are present. 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 his or her conclusion regarding the suitability of design or operating effectiveness of the control and performs additional testing as deemed necessary.

Testing Superseded Controls

3.140 If (*a*) the service organization makes changes to controls during the period, (*b*) 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, and (*c*) the service auditor believes the changes would be considered significant by report users, the service auditor should, if possible, test the superseded 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.

3.141 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 and determine the effect on the service auditor's report. If the circumstances result in a scope limitation, the service auditor should modify the service auditor's opinion. (See the relevant paragraphs within paragraphs .68–.84 of AT-C section 205 for reporting requirements when the service auditor is unable to obtain sufficient appropriate evidence.) Paragraph 4.85 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

3.142 If a control operates frequently, the service auditor may consider whether to use audit sampling when testing the operating effectiveness of the control. When determining the extent of tests of controls and whether sampling is appropriate, the service auditor should consider (*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. The AICPA Audit Guide *Audit Sampling* may be useful to the service auditor when performing sampling.

3.143 Before deciding to use sampling in a SOC 2® engagement, the service auditor should consider whether sampling is an appropriate strategy for testing the control. The following are examples of considerations the service auditor might take into account:

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 a 100 percent test of the control using data analytics is necessary 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 more effective to perform a 100 percent test of the data evidencing the effective operation of the control than selecting and testing a sample.

3.144 In such circumstances, sampling may not be an appropriate 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

3.145 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.

3.146 The service auditor's selection of sample items should be reasonably expected to be representative of the population, resulting in a sample that is

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

3.147 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.

3.148 In response to such risks, service organization management needs to understand the nature of those risks and assess the likelihood and magnitude of such risks. The controls that service organization management designs, implements, and operates in response to those risks depend on whether the third party's 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. For example, a managed services vendor might be responsible for monitoring server capacity and usage and for projecting future capacity demands based on historical trends. In that scenario, controls at the vendor are likely to be necessary and the vendor would be considered a subservice organization. Therefore, service organization management would consider matters, such as those described beginning in paragraph 2.12, to determine whether to use the inclusive or the carve-out method for the subservice organization.

3.149 In contrast, the service organization may design and implement control activities that address the risks represented by interactions with the vendor, or the service organization may have designed and implemented processes and procedures to monitor the activities of the vendor. If so, the vendor's controls are not likely to be necessary for the service organization to achieve its availability commitments and system requirements based on the applicable trust services criteria for availability. In the same data center hosting example noted in the preceding paragraph, the service organization independently performs high-level capacity monitoring activities and reviews the future capacity demands projected by the vendor for appropriateness. In this scenario, the service organization's controls alone may be sufficient to provide reasonable assurance that its availability commitments were achieved based on the applicable trust services criteria.

3.150 Processes and procedures 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

- Assessing, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives
- Assigning responsibility and accountability for the management of risks 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
- Implementing procedures for addressing issues identified with vendor and business partner relationships
- Implementing procedures for terminating vendor and business partner relationships

3.151 During the examination, the service auditor performs procedures to evaluate whether controls over vendors and business partners are suitably designed and, in a type 2 examination, operated effectively.

Additional Considerations Related to CSOCs

3.152 If the service organization uses the carve-out method for the services and controls of a subservice organization, the service auditor also 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). If there are CSOCs, the service auditor should determine 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. 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 are 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*.

3.153 The service auditor should also perform 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.

3.154 Although a service organization can contract with a subservice organization to perform functions that form a portion of the service organization's system, it still retains obligations to user entities with regard to those functions. As a result, part of its system of internal control includes activities to manage the risks associated with vendors and business partners, including activities to manage the risks associated with the functions performed by the subservice organization. In evaluating the suitability of the design and operating effectiveness of controls, the service auditor considers the nature and extent of the service organization's monitoring controls when determining the nature, timing, and extent of testing to perform. For example, if the service organization has obtained a type 2 report from a subservice organization, the service auditor would review the report to determine whether management has adequately evaluated it by assessing (*a*) the relevance of the system description and CSOCs to the service organization's system and (*b*) any deviations requiring further evaluation and response by service organization management. If service organization management has been unable to obtain a type 2 report, the service auditor should consider whether management has directly tested the subservice organization's controls by obtaining evidence about the effectiveness of the subservice organization's controls. However, unless the service auditor is reperforming management's tests of the subservice organization's controls, the service auditor's performance of tests directly on the subservice organization's controls would not provide evidence about the suitability of the design and operating effectiveness of the service organization's controls. In any event, the service auditor should obtain sufficient appropriate evidence of the effectiveness of the CSOCs. In addition, the service auditor needs to consider whether the subservice organization's use of its own IT system and connections to the service organization's IT network represents new vulnerabilities that need to be assessed and addressed as part of the service organization's risk assessment.

3.155 When there are CSOCs, the service auditor's report would be modified to refer to them. Appendix D-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 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

3.156 The description of the service organization's system may include controls that ordinarily operate during the period covered by the examination. However, in certain circumstances, some controls may not need to operate during that period because the circumstances that warranted the operation of the controls did not occur during the period. For example, controls related to providing a new user with identification and authentication credentials may not operate if no new users were added during the period. When management informs the service auditor that the circumstances requiring the operation of certain controls did not occur, the service auditor performs procedures to corroborate management's statement and describes, 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 his or her opinion on the operating effectiveness of the controls. However, in certain

circumstances where most or all of the controls evaluated by a particular criterion did not need to operate, additional language would be added to the service auditor's report, as discussed in chapter 4.

Identifying and Evaluating Deviations in the Operating Effectiveness of Controls

3.157 When evaluating the results of tests of controls and the significance of deviations noted, the service auditor should accumulate instances in which controls did not operate effectively. Generally, if controls are not operating effectively to provide reasonable assurance that one or more service commitments or system requirements were achieved based on the applicable trust services criteria, the deficiency is considered material. The service auditor also considers the potential impact of other factors that may affect the opinion on the operating effective of controls, such as misstatements in the description or deficiencies noted in the suitability of the design of controls.

3.158 If the service auditor becomes aware that any identified deviations have resulted from fraud, the service auditor should assess 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. In addition, paragraph .33 of AT-C section 205 states that the service auditor should respond appropriately to fraud or suspected fraud and noncompliance or suspected noncompliance with laws or regulations affecting the subject matter that are identified during the engagement. Paragraph .A29 of AT-C section 205 indicates that in these circumstances (unless prohibited by law, regulation, or ethics standards), it may be appropriate for the service auditor to, for example, do the following:

- Discuss the matter with the appropriate party or parties.
- Request that the responsible party consult with an appropriately qualified third party, such as the service organization's legal counsel or a regulator.
- Consider 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 the responsible party.
- Obtain legal advice about the consequences of different courses of action.
- Communicate with third parties (for example, a regulator).
- Withdraw from the engagement.

3.159 In performing his or her 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 because it may have occurred as a result of ineffective controls shared between the service organization's systems. If that is the case, the service auditor should reconsider the assessment of the risk of material misstatement. In addition, if the system incident is related to a security breach, the service auditor should 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 due to an advanced persistent threat that has not been detected. As a result of the reassessment of risk, the service auditor may determine that additional procedures need to be performed or that management needs to identify additional controls that are suitably designed and operating effectively in order to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

3.160 The service auditor determines whether the effects of identified deviations, individually or in the aggregate, are material with respect to the operating effectiveness of controls based on a consideration of materiality, as discussed beginning in paragraph 3.161. If the effects of identified deviations are material, the service auditor should modify the opinion on operating effectiveness as discussed in chapter 4.

Materiality Considerations When Evaluating the Suitability of Design and Operating Effectiveness of Controls

3.161 Paragraph 3.72 discusses materiality considerations related to the description, including making materiality assessments based on the understanding of the common information needs of the broad range of report users. This section discusses materiality considerations that can affect the service auditor's conclusion about whether controls are suitably designed.

3.162 When considering whether controls within the program were suitably designed and operating effectively, the service auditor ordinarily considers a number of factors, including the following:

- The nature of threats, and the likelihood and magnitude of the risks arising from those threats, to the system used to provide the services.
- The technical environment, including whether the realization of those threats or the exploitation of vulnerabilities related to aspects of the service organization's environment that appear inconsequential or are seemingly unrelated to the system could expose (either directly or indirectly) the system and result in ineffective system controls. For example, if access to the service organization's email server could provide access to the service organization's system, and the service auditor determines there is a high likelihood that such a vulnerability might be exploited, the service auditor is likely to consider access to the service organization's email service to be material in the SOC 2® examination.
- The nature of threats arising from error or fraud, and the likelihood and magnitude of the risks arising from such threats, to the operation of processes and controls that support the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria, and the vulnerabilities of those processes and controls to those threats. For instance, the security operation center staff's lack of knowledge of new types of cyberattacks may result in the failure to detect, in

a timely manner, system incidents that could significantly affect the service organization's achievement of its service commitments and system requirements.

3.163 The service auditor should consider both qualitative and quantitative factors when evaluating the suitability of design of controls. 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 need to be considered if the applicable trust services criteria are met 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, the service organization has not identified physical security controls over the tape storage location in its description because management concluded 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 presume that 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, support the processes and controls stated in the description; for this reason, they would ordinarily expect the service auditor to test and evaluate those controls as part of the evaluation of suitability of design and operating effectiveness.
- *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 such 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 the 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. Requirements established by laws and regulations may therefore need to be included in the consideration of materiality and the related engagement strategy. For laws and regulations that have a direct effect (for example, laws protecting sensitive personal information), the service organization may establish service commitments and system requirements about compliance with such laws. Other laws and regulations may be less directly linked to security and the other trust services categories; however, they may still be relevant to the examination (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).
- *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 an 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. An example of this 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 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.

3.164 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 but would be considered when evaluating the operating effectiveness of the controls. Note, however, that the service auditor should carefully consider the effect of identified deviations, either individually or in combination with other identified deviations, on the controls' ability to mitigate assessed risks.

3.165 Paragraph .17 of AT-C section 205 indicates the service auditor should reconsider materiality if the service auditor becomes aware of information during the examination that would have caused him or her to have initially determined a different materiality.

Using the Work of the Internal Audit Function

3.166 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 management 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.

3.167 When using the work of the internal audit function, paragraph .40 of AT-C section 205 requires the service auditor to 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.

3.168 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

3.169 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.

3.170 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.

3.171 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.

3.172 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.

3.173 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).

The 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.

3.174 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.

3.175 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.

3.176 When using internal auditors to provide direct assistance, paragraph .42 of AT-C section 205 requires the service auditor to 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.

3.177 Paragraph .44 of AT-C section 205 requires the service auditor, before the completion of the engagement, to 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

3.178 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 .36 of AT-C section 205 requires the service auditor to evaluate the adequacy of the work of the service auditor's specialist for the service auditor's purposes.

3.179 According to paragraph .36 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 are significant to the work of the service auditor's specialist, the relevance, completeness, and accuracy of that source data

3.180 If the service auditor determines that the work of the service auditor's specialist is not adequate, paragraph .37 of AT-C section 205 requires the service auditor to

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

3.181 Paragraph .34 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 3.159), 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 Results of Procedures

3.182 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 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) should be considered by the service auditor and, therefore, also constitutes evidence.

3.183 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 4.05. As discussed in paragraphs .46–.47 of AT-C section 205, if the service auditor is unable to obtain necessary further evidence, the service auditor should consider the implications for the service auditor's opinion. Such implications are discussed in paragraphs .68–.84 of AT-C section 205.

3.184 The service auditor evaluates the results of all procedures performed and conducts both a quantitative (for example, rates of deviations in testing a control using a sample-based testing strategy) and qualitative analysis of whether identified description misstatements and deficiencies in the suitability of design and, in a type 2 examination, deviations in the operating effectiveness of controls result in a description that is not presented in accordance with the description criteria or in controls that are not suitably designed or operating effectively. 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 than the management-prescribed resolution requirement to complete, but that difference was not material (for example, final resolution took two days longer than prescribed). In such an instance, the service auditor may conclude that the deficiencies were not material. However, if the service auditor's testing determined that entity personnel failed to follow up at all for the two instances, he or she might conclude that the controls were not effective in achieving one or more service commitments or system requirements based on the applicable trust services criteria.

3.185 When evaluating the results of procedures, the service auditor investigates the nature and cause of any identified description misstatements and deficiencies or deviations in the effectiveness of controls and determines 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 misunderstood by 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 that have been 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 or whether they are likely to affect only one of them
- Whether
  - a previously tested control (or combination of 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 should 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 magnitude 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
- Whether report users could be misled if the service auditor's opinion were not modified to reflect the identified deficiencies

3.186 According to paragraph .A105 of AT-C section 205, 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 the SOC 2® examination might be those that are, in the service auditor's professional judgment,

a. not confined to only specific aspects of the conclusion about control effectiveness or,

b. if so confined, represent or could represent a substantial proportion of the conclusions about suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls.

3.187 Factors that may be considered when determining whether the identified deviations may have a pervasive effect on other controls include the following:

- The effect that entity-level controls have on the operation of other controls. Deviations in entity-level controls often have a pervasive effect on other controls.
- 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 deviations in the operation of controls in one system will have an effect on the operation of controls in another one.
- The extent to which deficiencies in certain key controls have a pervasive effect on other controls. For example, a service auditor is unlikely to issue an unmodified opinion on controls of a service organization that does not have effective controls over the detection of system events relevant to security.

3.188 Paragraph .45 of AT-C section 205 also requires the service auditor to accumulate description misstatements or deficiencies identified during the engagement, other than those that are clearly trivial. In addition, the service auditor should accumulate deviations that have not been determined to rise to the level of a deficiency and consider whether, in the aggregate, they result in a deficiency.

3.189 If the service auditor identifies material description misstatements, material deficiencies in the suitability of design of controls or, in a type 2 examination, deviations in the operating effectiveness of controls, the service auditor

should modify the opinion. 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 of this guide discusses modifications to the service auditor's report.

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

3.190 As discussed in chapter 2, the service auditor has a responsibility to consider known or suspected incidents of fraud[6] and noncompliance with laws or regulations. 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 3.163, 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.

3.191 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

[6] Paragraph .10 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.

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

3.192 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 which 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

3.193 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). The service auditor may also consider whether to communicate other matters.

3.194 If the service auditor identifies or suspects noncompliance with laws or regulations that are not relevant to the subject matters of the SOC 2® examination, the service auditor should determine whether he or she has a responsibility to report the identified or suspected noncompliance to parties other than management (and the engaging party, if different).

3.195 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. However, the service auditor's legal responsibilities may vary by jurisdiction and, in

certain circumstances, the duty of confidentiality may be overridden by statute, law, or courts of law. A duty to notify parties outside the entity may exist

- in response to a court order or
- in compliance with requirements for examinations of service organizations that receive financial assistance from a government agency.

3.196 Because potential conflicts with the service auditor's ethical and legal confidentiality obligations may be complex, the service auditor may decide to consult with legal counsel before discussing noncompliance with parties outside the service organization.

Obtaining Written Representations

3.197 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.

3.198 The service auditor should 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.

3.199 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 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.

3.200 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.

3.201 Paragraph .50 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. The representations in the SOC 2® examination should do the following:

a. Include management's assertion about the subject matters[7] based on the criteria.[8]

b. State that

i. all relevant matters are reflected in the measurement or evaluation of the subject matters or assertion.

ii. 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.

c. Acknowledge responsibility for

i. the subject matters and the assertion,

ii. selecting the criteria, and

iii. determining that such criteria are appropriate for management's purposes.

d. State 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.

e. State that management has provided the service auditor with all relevant information and access.

f. State that management believes the effects of uncorrected misstatements (description misstatements and deficiencies) are immaterial, individually and in the aggregate, to the subject matters.

g. State 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;

ii. its knowledge of any actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the subject matters;

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.

3.202 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

---

[7] Within this section of the guide, the term *subject matters* refers to the subject matters in the SOC 2® examination: (1) the description, (2) the suitability of design of controls, and (3) in a type 2 examination, the operating effectiveness of controls.

[8] Within this section of the guide, the term *criteria* refers to both the description criteria and the trust services criteria.

to request certain representations that address the period before the change and the period after the change).

3.203 In many SOC 2® examinations, the service auditor also requests additional representations about whether service organization management has disclosed any of the following of which it is aware:

a. Instances of noncompliance with laws and regulations or uncorrected misstatements attributable to the service organization

b. Knowledge of any actual, suspected, or alleged fraud that could adversely affect the description of the service organization's system or the achievement of the service organization's service commitments or system requirements

3.204 The written representations required 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.

3.205 When written representations are directly related to matters that are material to the subject matter, 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.

3.206 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 3.201 from subservice organization management. Obtaining written representations from subservice organization management when the inclusive method is used is discussed beginning in paragraph 2.97.

3.207 Illustrative representation letters that may be appropriate for use in a type 1 and type 2 examination are included in appendix G.

3.208 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 should lead the service auditor to consider the effect of the matter on his or her 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 should 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

3.209 Paragraph .55 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.

3.210 In such circumstances, the guidance in that paragraph states that the service auditor should

- discuss the matter with the appropriate party or parties,
- 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.

3.211 Ordinarily, in the SOC 2® examination, 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 both or to withdraw from the engagement.

Representations From the Engaging Party When Not the Responsible Party

3.212 When the engaging party is not the responsible party, paragraph .52 of AT-C section 205 requires the service auditor to 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. Those representations should do the following:

a. Acknowledge that the responsible party is responsible for the subject matter and assertion.

b. Acknowledge the engaging party's responsibility for selecting the criteria, when applicable.

c. Acknowledge the engaging party's responsibility for determining that such criteria are appropriate for its purposes.

d. State that the engaging party is not aware of any material misstatements in the subject matter or assertion.

e. State 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. Address other matters as the service auditor deems appropriate.

Subsequent Events and Subsequently Discovered Facts

3.213 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.

3.214 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.

3.215 Paragraph .48 of AT-C section 205 requires the service auditor to 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

3.216 Paragraph .48 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 .49 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.

3.217 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.

3.218 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.

3.219 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

3.220 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

3.221 Paragraphs .34–.41 of AT-C section 105 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.

3.222 Additionally, paragraphs .87–.89 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 sections 105 and 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 .55 of AT-C section 205 (see discussion beginning in paragraph 3.209)
    v. Who reviewed the engagement work performed and the date and extent of such review

b. The results of the procedures performed and the evidence obtained

3.223 In addition to the items in the preceding paragraphs, documentation in the SOC 2® examination should include the following:

- If the service auditor has identified information that is inconsistent with the service auditor's final conclusions, how the service auditor addressed the inconsistency
- 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,

— the circumstances encountered;

— any new or additional procedures performed, evidence obtained, and conclusions reached and their effect on the report; and

— when and by whom the resulting changes to the documentation were made and reviewed

3.224 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

3.225 Paragraphs .A117–.A119 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

3.226 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.

3.227 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 our other three facilities.

3.228 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 the 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.*

3.229 If service organization management is unwilling to modify its assertion to align with the service auditor's opinion, the service auditor should consider the implications for the service auditor's opinion. For example, the service auditor should 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 or 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.

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 (1) the description presents the system that was designed and implemented throughout the period in accordance with the description criteria, (2) 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 (3) 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 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 4.31, and any modifications to the report that the service auditor determines are necessary in the circumstances

4.03 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, appendix E, "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

4.04 When forming an opinion, paragraph .59 of AT-C section 205, *Examination Engagements*,[1] requires the service auditor to evaluate

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

a. the service auditor's conclusion about the sufficiency and appropriateness of evidence obtained during the examination and

b. whether uncorrected misstatements are material, individually or in the aggregate.

Concluding on the Sufficiency and Appropriateness of Evidence

4.05 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 its relevance 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.

4.06 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.

4.07 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, 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.

4.08 Evidence obtained from different sources or 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.

4.09 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 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 its environment

Considering Uncorrected Description Misstatements and Deficiencies

4.10 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. For example, information such as the following—which differs significantly from the information on which the risk assessment and planned procedures were based—may come to the service auditor's attention:

- The nature and number of identified description misstatements and deficiencies. (This may change the service auditor's professional judgment about the reliability of sources of information.) For example, the service auditor may discover that management was unaware that detection tools were not implemented over a server that is a component of the system under examination. In response, the service auditor may consider whether additional testing is needed to evaluate whether controls over the server are effective and whether detection measures over other system components would mitigate the risk or detect incidents related to the server.

- Identified discrepancies in relevant information, or conflicting or missing evidence.
- Procedures performed toward the end of the engagement that indicate a previously unrecognized risk of material misstatement. 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.

4.11 The service auditor also evaluates the effect of such uncorrected description misstatements or 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.

4.12 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, he or she should modify the opinion to express a qualified or adverse opinion. Reporting when the service auditor decides to modify the opinion is discussed beginning in paragraph 4.43.

Expressing an Opinion on Each of the Subject Matters in the SOC 2® Examination

4.13 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

[2] The description criteria presented in this document (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*, in a SOC 2® report (note: the TSP sections can be found in AICPA *Trust Services Criteria*). The 2018 description criteria are codified in DC section 200 in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26-.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are codified in DC section 200A.

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2 examination), either the 2018 description criteria or the 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

commitments and system requirements were achieved based on the applicable trust services criteria,[3] 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.

4.14 When the service auditor concludes that an opinion modification on one of the subject matters is appropriate, the service auditor should also consider 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 a significant subsequent event. The service auditor may conclude that, because the subsequent event did not affect the suitability of design or operating effectiveness of controls during the period covered by the examination, 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 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.

---

[3] The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in TSP section 100A-1 until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

Describing Tests of Controls and the Results of Tests in a Type 2 Report[4]

4.15 A service auditor's report for a type 2 examination should contain a reference to a description of the service auditor's tests of controls and results thereof. 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. The service auditor's report contains a reference to the description of the service auditor's tests of controls and the results of those tests.

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	Required	Required
Whether the items tested represent all or a selection of the items in the population	Required	Required
The nature of the tests performed in sufficient detail to enable report users to determine the effect of such tests on their risk assessments	Required	Required
The number of items tested	Not required	Required
The number and nature of the deviations	N/A	Required
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 4.23)	Required, if the work of the internal audit function has been used in tests of controls to obtain evidence	Required, if the work of the internal audit function has been used in tests of controls to obtain evidence

4.16 The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because the service auditor does not have the ability to determine whether a deviation will have significance to an individual report user, beyond whether it prevents a control from operating effectively. Consequently, the service auditor's description of tests of controls and results includes all 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."

[4] For brevity, the word *tests* as used hereinafter refers to tests of the operating effectiveness of controls, also known as *tests of controls*.

Appendix D-4, "Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System," contains an example of a description of tests of controls in which no deviations have been identified.

4.17 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 Security Office are defined. • the reporting relationship of the Chief Information Security Officer to service organization leadership is defined.
The extent of testing, including whether the items tested represent all or a selection of the items in the population	Selected *a sample of requests for access to the system made during the months of March, June, September, and December 20XX* to determine if access was granted or denied based on the entity's access criteria...
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...

(continued)

Relevant Information When Describing Tests of Controls—*continued*

Relevant Information When Describing a Test of Controls	*Example*
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 underlying electronic audit evidence (for example, system-generated reports)	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...

4.18 In describing the extent of testing, the service auditor should indicate whether items tested represent all or a selection of the items in the population. The service auditor is not required to indicate the size of the sample unless deviations have been identified during testing.

4.19 If deviations have been identified, the service auditor should disclose 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 service organization achieved its service commitments and system requirements based on the applicable trust services criteria. When sampling is used and deviations have been identified, it is helpful to report users if both the sample size and population size are presented.

4.20 If deviations in tests of controls have been identified, it may be helpful to report users 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. 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 4.95).

4.21 If management's responses to deviations in tests of controls are included in the description of the service organization's system, such responses

usually are included along with the description of the applicable control and related criteria. In these circumstances, the service auditor should determine, through inquiries in combination with other procedures, whether there is evidence supporting the action described by management in its response. If the response includes forward-looking information, such as future plans to implement controls or to address deviations, such information is 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 4.95.

4.22 The following example illustrates the description of tests of controls for which 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 90 days after the employee's last day of work. Tested an additional sample of 15 terminated employees and found no additional deviations.

Describing Tests of Controls and Results When Using the Internal Audit Function

4.23 If the work of the internal audit function has been used, the service auditor should not refer to the work of the internal audit function in the service auditor's opinion. Notwithstanding its degree of autonomy and objectivity, the internal audit function is not independent of the service organization. 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.

4.24 If the work of the internal audit function has been used in tests of controls to obtain evidence, the section of the SOC 2® report in which the service auditor describes the tests of controls and results should include a description of the internal auditor's work and of 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 tests of controls performed by internal auditors as part of 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.)

4.25 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.

4.26 The following are examples of introductory material that may be included in the description of tests of controls and results to inform report users that the service auditor has used the work of the internal audit function to perform tests of controls:

- 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.

4.27 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

4.28 When the service auditor performs procedures to assess the reliability of information produced by the service organization, the service auditor's procedures would 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.

4.29 The following is an example of language that may be included in the description of tests of controls and results to inform report users that the service auditor has performed procedures that address the reliability of information provided by the service organization to the service auditor in response to an ad hoc request from the service auditor and information used in the execution of a control:

> 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.

4.30 When the service auditor performs procedures to assess the reliability of information prepared for user entities, the procedures performed by the service auditor would be included in the description of the tests of operating

effectiveness of the applicable control and the results of the tests. The following is an example of language that may be used when the description of the procedures performed is included in the description of the tests of the operating effectiveness of the applicable control and the results of the tests to inform readers of the specific procedures the service auditor performed to address the reliability of information used in the execution of a control:

> Obtained a daily termination report that was produced automatically from the Human Resources Management System and provided to the facilities manager during the period. Inspected the query used to generate the daily termination report used in the execution of the control to determine whether terminations are appropriately included in the report provided to the facilities manager.

Preparing the Service Auditor's SOC 2® Report

Elements of the Service Auditor's SOC 2® Report

4.31 AT-C section 205 identifies the elements to be included in a service auditor's examination report. It also provides requirements for adding an alert to that report 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 D-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 and Complementary User Entity Controls)," presents an illustrative service auditor's type 2 report.

4.32 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 included in the report related to the use of a subservice organization and because of the need for CUECs and CSOCs is shown in ***boldface italics.***

[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 E, "Illustrative Management Assertion and Service Auditor's Report for a Type 1 Examination," presents an illustrative type 1 report.

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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
.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
.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: XYZ 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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
.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	The report should identify the subject matter of a SOC 2® examination, which generally includes the following: 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	*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 Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (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* (AICPA, *Trust Services Criteria*).

(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 Requirement*	*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 disclose the actual controls at the subservice organization. Our examination did not include the services***

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 Requirement*	*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 CSOCs that are suitably designed and operating effectively are necessary, along with controls at the service organization, to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria;	***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***

(continued)

[6] Column four 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 D-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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		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 may also wish to include a statement that the examination did not include the services provided by the subservice organization and that he or she has not evaluated the suitability of the design or operating effectiveness of the CSOCs.	***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.***

[7] 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 Requirement*	*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 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 complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the service organization, to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria;	

(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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		b. the description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls; *c.* the examination did not include such complementary user entity controls and the service auditor has not evaluated the suitability of the design or operating effectiveness of such controls.[8]	
.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 is 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]*

[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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
.63*e*i	A statement that identifies the responsible party and its responsibility for the subject matter 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: 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	*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 [*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

(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 D-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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		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 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	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.
.63*e*ii	A statement that the practitioner's responsibility is to express an opinion on the subject matter or assertion, based on the practitioner's examination	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.

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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
.63*f*	A statement that 1. the practitioner's examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants 2. those standards require that the practitioner plan and perform the examination to obtain reasonable assurance about whether 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 in paragraph .A82 of AT-C section 205)	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 American Institute of Certified Public Accountants. 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 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 American Institute of Certified Public Accountants. 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.

(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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
	3. the practitioner believes the evidence the practitioner obtained is sufficient and appropriate to provide a reasonable basis for the practitioner's opinion	3. The service auditor believes the evidence obtained is sufficient and appropriate to provide a reasonable basis for the opinion.	
.63*g*	A description of the nature of an 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	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

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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		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 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	• 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

(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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		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.	• Evaluating the overall presentation of the description Our examination also included performing such other procedures as we considered necessary in the circumstances.
.63*h*	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 the objectives of controls 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. • 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* 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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 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, 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.
.A85	Because the practitioner's report is intended to include a description of the procedures performed by the practitioner and the results of those procedures, the practitioner should consider whether to add an alert that restricts the use of the report to parties who are likely to understand the report as discussed beginning in paragraph 4.33.	The elements of the service auditor's description of procedures performed and results thereof are discussed beginning in paragraph 4.15. [*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. [See section 4 of Appendix D-4, "Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)," for illustrative language.]

(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 Requirement***	***SOC 2® Reporting Elements and Additional Guidance***	***Illustrative Service Auditor's Type 2 Report Language***
.63*i*	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 complementary controls assumed in the design of XYZ's controls 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 Requirement*	*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 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, 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 2.17 and the discussion of CUECs beginning in paragraph 2.20.	*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.***

(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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
.64*a* .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 1. 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 limited 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, including those who have sufficient knowledge and understanding of the following: *a.* The nature of the service provided by the service organization	*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 organizations, and other parties *c.* Internal control and its limitations

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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
	2. identify the specified parties for whom use is intended, and 3. state that the report is not intended to be and should not be used by anyone other than the specified parties.	*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 *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	***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

(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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
		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 At his or her discretion, the service auditor may specifically identify the specified parties 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.	This report is not intended to be, and should not be, used by anyone other than these specified parties.
.63*j*	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*

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 Requirement*	*SOC 2® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's Type 2 Report Language*
.63*k*	The city and state where the practitioner practices	The service auditor's report should include the city and state where the service auditor practices.	*Service auditor's city and state*
.63*l*	The date of the report	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*

Requirement to Restrict the Use of the SOC 2® Report

4.33 A SOC 2® report is, by definition, intended to include a description of the procedures performed by the service auditor and the results of those procedures. According to paragraph .A85 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.

4.34 Table 4-3 presents the requirements for an alert paragraph from paragraphs .64–.65 of AT-C section 205. The service auditor's report should include each of those elements in the alert paragraph.

4.35 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.

Reporting When the Service Organization's Design of Controls Assumes Complementary User Entity Controls

4.36 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.

4.37 If there are CUECs, description criterion DC6 requires that fact to be disclosed in the description of the service organization's system. In addition, 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 should 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. Illustrative language related to CUECs and CSOCs is shown in boldface italics in table 4-3.

4.38 In addition, service organization management would modify its assertion to reflect the modifications to the service auditor's report discussed in the preceding paragraph. Illustrative language is shown in boldface in the management assertion presented in appendix D-4, "Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)."

Reporting When the Service Organization Carves Out the Controls at a Subservice Organization

4.39 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.

4.40 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.

4.41 To inform report users about the potential effect of CSOCs, the service auditor's report should contain similar disclosures as those described in the preceding paragraph. In addition, it should 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. Illustrative language is shown in boldface in the management assertion presented in appendix D-4, "Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)."

Reporting When the Service Auditor Assumes Responsibility for the Work of an Other Practitioner

4.42 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

4.43 Paragraph .68 of AT-C section 205 requires the service auditor to 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.

4.44 In applying paragraphs .68–.69 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.

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 misstatements, deficiencies, and deviations when making their own risk assessments.

4.45 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 .A103 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

4.46 When determining the type of modified opinion to be issued, the service auditor evaluates whether identified (*a*) description misstatements (including omissions) or (*b*) deficiencies or deviations in the suitability of the design and operating effectiveness of the controls are material. Materiality considerations related to the description are discussed beginning in paragraph 3.72, and considerations related to the suitability of design and operating effectiveness of controls are discussed beginning in paragraph 3.161.

4.47 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 Modification

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

4.48 Paragraph .69 of AT-C section 205 states that, when the service auditor modifies the opinion, the service auditor should include a separate paragraph in the service auditor's report that provides a description of the matters giving rise to the modification.

4.49 Examples of separate paragraphs that describe the matters giving rise to a modification are provided beginning in paragraph 4.68.

4.50 When determining whether to modify the service auditor's report, the service auditor considers the individual and aggregate effect of identified misstatements in the description of the service organization's system and identified deficiencies or deviations in the suitability of the design and operating effectiveness of the controls throughout the specified period. Chapter 3 discusses materiality, including the quantitative and qualitative factors the service auditor considers, in further detail.

Qualified Opinion

4.51 The service auditor expresses a qualified opinion in the following circumstances:

- The service auditor 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 and 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 misstatements. The section beginning in paragraph 4.56 discusses qualifications because of scope limitations.

4.52 When material misstatements in the description or deficiencies in the design or operation of controls are identified, the service auditor generally expresses a qualified opinion if (1) the identified misstatements in the description of the service organization's system are limited to one or more, but not all, aspects of the description; (2) the identified deficiencies in the suitability of the design or operating effectiveness of the controls result in the failure of the controls to provide reasonable assurance that one or more, but not all, of its service commitments and system requirements were achieved based on the applicable trust services criteria; and (3) the identified misstatements and deficiencies do not otherwise affect the service auditor's opinion on other aspects of the description of the service organization's system or on whether controls were suitably designed or operated effectively.

4.53 When the service auditor has determined that a qualified opinion is appropriate because of material misstatements or deficiencies, the service auditor's report would be modified by doing the following:

- 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 requirement 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

4.54 Paragraph .72 of AT-C section 205 states that a practitioner should issue an adverse opinion when he or she concludes that the 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 expresses an adverse opinion in a SOC 2® examination if the description misstatements in the description of the service organization's system or deficiencies or deviations 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.

4.55 When the service auditor has determined that an adverse opinion is appropriate, the service auditor expresses an adverse opinion on each of the subject matters in the examination. When expressing an adverse opinion, the service auditor should add a separate paragraph to the service auditor's report describing the matters giving rise to the modification and should modify the opinion paragraph of the service auditor's report as follows. New language is shown in boldface italics; deleted text is shown by 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*** operated 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 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

4.56 A service auditor may express an unmodified opinion only when he or she has conducted the examination in accordance with the attestation standards. If the service auditor has been unable to apply all of the procedures considered necessary in the circumstances, the service auditor would not have complied with the attestation standards.

4.57 According to paragraph .A107 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.

4.58 When there is a scope limitation, the service auditor should determine 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 .70 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 and 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 4.61.)

4.59 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

4.60 If the service auditor decides to express 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.

Disclaimer of Opinion

4.61 Paragraph .74 of AT-C section 205 indicates that 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 misstatements, if any, could be both material and pervasive.

4.62 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 what those standards require of the service auditor.
  - — describing the nature of an examination engagement or identifying the procedures performed and the results of those procedures.

4.63 If the service auditor decides to disclaim 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 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.

4.64 Other situations in which the service auditor should disclaim an opinion include the following:

- 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 4.66).
- 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.

4.65 Appendix D-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

4.66 Ordinarily, if management 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, the service auditor may conduct the engagement and, ultimately, should disclaim an opinion.

4.67 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 American Institute of Certified Public Accountants 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

4.68 Chapter 3 presents several situations in which the service auditor determines 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. If the service auditor decides to continue with the engagement, the service auditor should modify the opinion paragraph of the report.

4.69 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 4.70.

Description Includes Controls That Have Not Been Implemented

4.70 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

4.71 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

4.72 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

4.73 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

4.74 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 who 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

4.75 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

4.76 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 based on the applicable trust services for availability 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

4.77 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 requests 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.

Other Information Provided by the Service Organization Is Materially Inconsistent With Information in the Description of the Service Organization's System

4.78 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

4.79 Chapter 3 presents several situations in which the service auditor determines 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 this situation are presented beginning at paragraph 4.80.

Controls Are Not Suitably Designed

4.80 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 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.*

Controls Were Not Suitably Designed During a Portion of the Period

4.81 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, the procedures, however, did not include controls for the authorization, testing, and documentation of changes to the system before those changes were placed into operation. 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 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.*

Scope Limitation Related to Suitability of Design of Controls

4.82 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. The Example Service Organization's logging software was replaced on July 15, 20X0, and sufficient appropriate evidence that independent research and resolution was 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 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.*

Illustrative Separate Paragraphs: Material Deficiencies in the Operating Effectiveness of Controls

4.83 Chapter 3 presents several situations in which the service auditor determines 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 are presented beginning at paragraph 4.84.

4.84 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 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.*

Scope Limitation Related to Operating Effectiveness of Controls

4.85 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.*

Controls Did Not Operate During the Period Covered by the Report

4.86 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.
- Service organization management would modify its assertion to identify which key processes did not operate during the period and indicate that they did not operate because the circumstances that warranted the operation of those processes and associated controls did not occur during the period.
- 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.
- The service auditor would include in the report a separate paragraph emphasizing the controls that did not operate and that no tests of those controls were performed.

4.87 However, if any applicable trust services criteria are not addressed because they are not relevant to a particular service organization's system (for example, because the related controls are performed by a subservice organization or are otherwise not relevant to the services being provided), then the service organization's description needs to include an explanation of why the criteria are not addressed.

4.88 The following is an example of a separate paragraph that might be added to the service auditor's report in this situation:

> Example Service Organization's description of its payroll system discusses its cybersecurity incident response and recovery plan (CIRP), which includes the controls implemented and operated to respond to and recover from security incidents. Example Service Organization's CIRP includes procedures to help understand, contain, monitor, or eradicate a security incident; restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data; and communicate with affected parties. However, during the period [*date*] through [*date*], Example Service Organization did not experience a security incident that would warrant the operation of the response and recovery processes and controls within its CIRP. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria CC7.4, *The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate,* and CC7.5, *The entity identifies, develops, and implements activities to recover from identified security incidents.*

Other Matters Related to the Service Auditor's Report

Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs

4.89 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)

4.90 In such situations, the service auditor should include an emphasis-of-matter paragraph or other-matter paragraph, as applicable, in the service auditor's report. 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*.[10] 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

4.91 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.

4.92 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.

4.93 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, the service auditor should consider informing the engaging party that restricted-use reports are not intended for distribution to non-specified parties, and the service auditor should 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.

---

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

Service Auditor's Recommendations for Improving Controls

4.94 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

4.95 Service organization management may wish to include, in the description of the service organization's system, in a separate section of the report, or in an attachment to the description, other information that is not covered by the service auditor's report.

4.96 The service auditor should identify any information not covered by the service auditor's report that is included in a document containing the service auditor's report. Typically, this is information that is beyond the scope of the engagement but that the service organization wishes to communicate to report users. 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

4.97 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 4.100 on the other information.

4.98 Paragraph 4.104 presents a separate paragraph that would be added to the service auditor's report to identify other information that (*a*) is not covered by the service auditor's report and (*b*) is appropriately segregated and identified as such.

4.99 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 should determine through inquiries, in combination with other procedures, whether there is evidence supporting the action described by management in its response.

4.100 Paragraph .57 of AT-C section 205 indicates that if, prior to or after the release of the service auditor's report, the service auditor is willing to permit the inclusion of the service auditor's report in a document that contains the description of the service organization's system or management's assertion and other information, the service auditor should read the other information to identify the following:

a. Material inconsistencies with the description of the service organization's system, management's assertion, or the service auditor's report

b. A material misstatement of fact 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.)

4.101 Paragraph .57 of AT-C section 205 indicates that if a material misstatement of fact or a material inconsistency exists (as described in paragraph 3.09), the service auditor should discuss the matter with service organization management. The service auditor would ordinarily request that management correct or delete the other information.

4.102 If management refuses to correct or delete the other information containing a material inconsistency or a material misstatement of fact, paragraph .A67 of AT-C section 205 identifies the following examples of further actions the service auditor may take:

- Requesting the appropriate party or parties to 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

4.103 Paragraph 4.78 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.

4.104 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.

Illustrative Type 2 Reports

4.105 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.

4.106 Appendix D contains the following illustrative type 2 reports:

- Appendix D-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 and Complementary User Entity Controls)"
- Appendix D-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 D-3, "Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation"
- Appendix D-4, "Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)"

Headings in those illustrative reports are optional.

Preparing a Type 1 Report

4.107 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 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*].

4.108 The service auditor does not express an opinion about whether the controls operated effectively. Accordingly, the service auditor's type 1 report would not include a description of the service auditor's tests of controls and the results thereof.

4.109 Appendix E, "Illustrative Management Assertion and Service Auditor's Report for a Type 1 Examination," presents an illustrative type 1 report. Headings in that illustrative report are optional.

Forming the Opinion and Preparing a SOC 3® Report

Elements of the SOC 3® Report

4.110 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.

4.111 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 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

4.112 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 a 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.

4.113 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 the subservice organization's controls are included in the description of the boundaries of the system and examination or whether they have been carved out from the description and examination
- Any other information that is likely to assist report users in understanding the limitations on the service auditor's examination and opinion

4.114 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 need to modify the language of the SOC 3® report to include them.

Service Auditor's Opinion

4.115 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. However, paragraph .62 of AT-C section 205 also permits a service auditor to express an opinion on the suitability of the design and operating effectiveness of the controls within the system.

Elements of the Service Auditor's Report

4.116 As in a SOC 2® report, the elements to be 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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
.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
.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: XYZ Service Organization

(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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
.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	The report should identify the subject matter of a SOC 3® examination, which is 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.*[11]	*Scope* We have examined XYZ Service Organization's (XYZ's) accompanying assertion, titled "Assertion of XYZ Service Organization Management" (assertion),[12] 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* (AICPA, *Trust Services Criteria*).

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

[12] 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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
.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]*
.63*e*	A statement that identifies the responsible party and its responsibility for the subject matter 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	*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

(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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
		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 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	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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
.63*e*	A statement that the practitioner's responsibility is to express an opinion on the subject matter or assertion, based on the practitioner's examination	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 American Institute of Certified Public Accountants. 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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
.63*f*	A statement that 1. the practitioner's examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants 2. those standards require that the practitioner plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects 3. the practitioner believes the evidence the practitioner obtained is sufficient and appropriate to provide a reasonable basis for the practitioner's opinion	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 American Institute of Certified Public Accountants. 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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
.63*g*	A description of the nature of an 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.

(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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
.63*h*	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. • 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.	*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.

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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
.63*i*	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.
.63*j*	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*
.63*k*	The city and state where the practitioner practices	The service auditor's report should include the city and state where the service auditor practices.	*Service auditor's city and state*

(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 Requirement*	*SOC 3® Reporting Elements and Additional Guidance*	*Illustrative Service Auditor's SOC 3® Report Language*
.63*l*	The date of the report	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 and (2) service organization management has provided a written assertion.	*Date of the service auditor's report*

4.117 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 misstatement or for a scope limitation.

4.118 When the service auditor believes 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 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

4.119 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.

Supplement A

2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report

This supplement contains authoritative AICPA Assurance Services Executive Committee material.

The description criteria and related implementation guidance in this supplement have been extracted from DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*,[1] issued in February 2018 by the AICPA's Assurance Services Executive Committee.[2] The complete text may be found at www.aicpa.org/soc4so.

Description Criteria	*Implementation Guidance*
The description contains the following information:	When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
DC 1: The types of services provided	Examples of the types of services provided by service organizations are as follows: • *Customer support.* Providing customers of user entities with online or telephonic post-sales support and service management. Examples of these services are warranty inquiries and investigating and responding to customer complaints.

(continued)

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

[2] The description criteria codified as DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, (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*, of AICPA *Trust Services Criteria* (see supplement B). The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are codified as DC section 200A.

When preparing a description of the service organization's system as of December 15, 2018, or prior to that date (type 1 examination) or a description for periods ending as of December 15, 2018, or prior to that date (type 2 examination), either the 2018 description criteria or the 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain available in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

Description Criteria	*Implementation Guidance*
	• *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. • *Enterprise 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. • *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 (FinTech) services.* Providing financial services companies with information technology-based transaction processing services. Examples of such transactions are loan processing, peer-to-peer lending, payment processing, crowdfunding, big data analytics, and asset management.
DC 2: The principal service commitments and system requirements	A system of internal control is evaluated using the trust services criteria within the context of the entity's ability to achieve its business objectives and sub-objectives. When a service organization provides services to user entities, its objectives and sub-objectives relate primarily to the following: *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

Description Criteria	*Implementation Guidance*
	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*. Although service organization management is responsible for designing, implementing, and operating controls to provide reasonable assurance that it achieves its system objectives, management is required to disclose in the description only its *principal* service commitments and system requirements, as discussed in the subsequent section. *Principal Service Commitments*. Disclosure of the principal service commitments and system requirements enables report users to understand the objectives that drive the operation of the system and how the applicable trust services criteria were used to evaluate whether controls were suitably designed and operated effectively. Service commitments include those made to user entities and others (such as customers of user entities), to the extent those commitments relate to the trust services category or categories addressed by the description. For example, service commitments could also include those made as part of the National Institute of Standards and Technology (NIST) risk management framework for government agencies and other parties. The service commitments a service organization makes to user entities and others are based on the needs of those entities. In identifying the service commitments to be disclosed, service organization management may begin by reviewing the commitments it made to user entities. Service commitments may be communicated to user entities in many ways, such as through contracts, service level agreements, and published policies (for example, a privacy policy). No specific form of communication is required.

(continued)

Description Criteria	*Implementation Guidance*
	A service organization may make service commitments on many different aspects of the service being described, 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 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 6 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 request from its customers. Service organization management need not disclose every service commitment, but only those that are relevant to the broad range of SOC 2® report users (that is, the principal service commitments). For example, when the description addresses availability, a service organization may make the same system availability commitment to the majority of its user entities. Because information about the availability commitment common to most user entities is likely to be relevant to the broad range of SOC 2® report users, service organization management would describe that principal availability commitment in the description.

Description Criteria	*Implementation Guidance*
	In other cases, however, a service organization may make a different commitment about system availability to an individual user entity that requires greater system availability than most user entities. Service organization management ordinarily would not disclose that commitment because it is unlikely to be relevant to the broad range of SOC 2® report users. Because that service commitment is not disclosed in the description, the individual user entity understands that the evaluation of the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls was made based on the service organization's achievement of its principal service commitments and system requirements (that is, those common to the majority of user entities); therefore, the individual user entity may need to obtain additional information from the service organization regarding the achievement of its specific availability commitment. When the description addresses privacy, service organization management discloses the service commitments and system requirements identified in the service organization's privacy notice or in its privacy policy that are relevant to the system being described. When making such disclosures, it may also be helpful to report users if service organization management describes the purposes, uses, and disclosures of personal information as permitted by user entity agreements. *Principal System Requirements*. System requirements are the specifications about how the system should function to do the following: • Meet the service organization's service commitments to user entities and others (such as user entities' customers) • Meet the service organization's commitments to vendors and business partners

(continued)

Description Criteria	*Implementation Guidance*
	• Comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations • 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. The following are examples of system requirements: • Workforce member fingerprinting and background checks established in government banking regulations • System edits that restrict the values accepted for system input, which are defined in application design documents • 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, established by industry groups or other bodies, such as the Simple Object Access Protocol (SOAP) • Business processing rules and standards established by regulators, for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA) 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).

Description Criteria	*Implementation Guidance*
	The principal system requirements that need to be disclosed are those that are relevant to the trust services category or categories addressed by the description and that are likely to be relevant to the broad range of SOC 2® report users. In identifying which system requirements to disclose, service organization management may consider 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, internal requirements related to the operating margin for the services associated with the system are not relevant to the broad range of SOC 2® report users and, therefore, need not be disclosed.
DC 3: The components of the system used to provide the services, including the following: *a. Infrastructure* *b. Software* *c. People* *d. Procedures* *e. Data*	*Infrastructure.* Disclosures about the infrastructure component include matters such as the collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and related 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.* Disclosures about the software component include matters such as the application programs, the IT system software that supports those 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 and laptop applications. *People.* Disclosures about the people component include the personnel involved in the governance, management, operation, security, and use of the system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

(continued)

Description Criteria	*Implementation Guidance*
	Procedures. Disclosures about the automated and manual procedures implemented by the service organization primarily relate to those through which services are provided. These include, as appropriate, procedures through which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared. A process consists of a series of linked procedures designed to accomplish a particular goal (for example, the process for managing third party risks). Procedures are the specific actions undertaken to implement a process (for example, the procedure in place to assess and manage the requisition and engagement of vendors). For that reason, service organization management may find it easier to describe procedures in the context of the process of which they are a part. Policies are 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. The service organization deploys control activities through policies that establish what is expected and procedures that put policies into action. Reports and other information prepared by the service organization may also be included in the description to enable report users to better understand the order of activities performed by the service organization. System components may also be described using specific technical terms that will help create a clearer understanding of the service organization's system and system boundaries. Technical terms can also aid report users in understanding the service organization's physical and logical components when considering a service organization's impact on the user entities. It may be helpful for service organizations to enhance their system descriptions using open systems interconnect (OSI) seven-layer model concepts. An organization could describe how and on which layer specific components of the system are operated, for example, with a statement such as this:

Description Criteria	*Implementation Guidance*
	Encrypted connections are made to the service organization using client virtual private network (VPN) hardware that connects system users via secure shell (SSH) to secure file transfer protocol (SFTP) servers that operate following transport layer security (TLS) standards and protocols. *Data.* Disclosures about the data component include types of data used by the system, transaction streams, files, databases, tables, and output used or processed by the system. When the description addresses the confidentiality or privacy categories, other matters that may be considered for disclosure about the data component include the following: • The principal types of data created, collected, processed, transmitted, used, or stored by the service organization and the methods used to collect, retain, disclose, dispose of, or anonymize the data • Personal information that warrants security, data protection, or breach disclosures based on laws or commitments (for example, personally identifiable information, protected health information, and payment card data) • Third-party entity information (for example, information subject to confidentiality requirements in contracts) that warrants security, data protection, or breach disclosures based on laws or commitments When the description addresses controls over confidentiality and privacy, management would address, at a minimum, all the system components as they relate to the information life cycle of the confidential and personal information used in providing the service within well-defined processes and informal ad hoc procedures.

(continued)

Description Criteria	*Implementation Guidance*
	Boundaries of the system. Not all activities performed at the service organization are part of the system being described. Determining the functions or processes that are outside the boundaries of the system and describing them in the description may be necessary to prevent report users from misunderstanding the boundaries of the system. Therefore, if there is a risk that report users might be confused about whether a specific function or process is part of the system being described, the description needs to clarify which processes or functions are included in the examination. For example, the following functions or processes at the service organization may be outside the boundaries of the system being described: • The process used to invoice user entities for the services provided by the service organization. • The conversion of new user entities to the service organization's systems. For some service organizations, such conversions are handled by an entirely different system than the one being described. • The receipt of data from sources outside the system being described. An example is a payroll processing system that receives information inputs from an employer in a ready-to-process state, which limits the responsibility of the service organization's system to processing the inputs provided by the employer to produce direct bank deposits to specified bank accounts. *Third Party Access.* Vendors, business partners, and others (third parties) often store, process, and transmit sensitive data or otherwise access a service organization's system. These third parties may provide components of the system. Service organization management may need to describe the components of the system provided by such third parties. Such disclosures may include, for example, the nature of the third parties' access and connectivity to the service organization's system.

Description Criteria	*Implementation Guidance*
DC 4: For identified 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 those service commitments and system requirements, as of the date of the description (for a type 1) or during the period of time covered by the description (for a type 2), as applicable, the following information: *a.* Nature of each incident *b.* Timing surrounding the incident *c.* Extent (or effect) of the incident and its disposition	Judgment is needed when determining whether to disclose an incident. However, consideration of the following matters as they relate to the system being described may help make that determination: • Whether the incident resulted from one or more controls that were not suitably designed or operating effectively • Whether the incident resulted in a significant failure in the achievement of one or more of the service organization's service commitments and system requirements • Whether public disclosure of the incident was required (or is likely to be required) by cybersecurity laws or regulations • Whether the incident had a material effect on the service organization's financial position or results of operations and required disclosure in a financial statement filing • Whether the incident resulted in sanctions by any legal or regulatory agency • Whether the incident resulted in the service organization's withdrawal from material markets or cancellation of material contracts Disclosures about identified security incidents are not intended to be made at a detailed level, which 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. Rather, 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.

(continued)

Description Criteria	*Implementation Guidance*
	Assume that the service organization identified a security breach that resulted in the service organization's failure to achieve one or more of its service commitments and system requirements. The breach, which occurred six months prior to the start of the period covered by the description, had not been fully remediated during the period covered by the description. In this example, management would likely need to disclose the incident in the description 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. In addition, service organization management should consider whether to disclose known incidents at a subservice organization, regardless of whether management has elected to use the inclusive or carve-out method.
DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), presents the criteria for each of the trust services categories. A description is presented in accordance with this criterion when it includes information about each of the criteria related to the trust services category or categories covered by the description (applicable trust services criteria), including controls related to the control environment, risk assessment process, information and communication, monitoring activities, and control activities. For example, if the description addresses availability, 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.

Description Criteria	*Implementation Guidance*
DC 6: If service organization management assumed, in the design of the service organization's system, that certain controls would be implemented by user entities, and those 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 would be achieved, those complementary user entity controls (CUECs)	*Complementary User Entity Controls.* CUECs are those controls that service organization management assumed, in the design of the system, would be implemented by user entities and 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. Usually, a service organization can achieve its service commitments and system requirements without depending on the implementation of CUECs at user entities because the service organization restricts its service commitments and system requirements to those matters that are its responsibility and that it can reasonably perform. Consider trust services criterion (CC) 6.2: > 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. CC 6.2 limits the service organization's responsibilities because the criterion requires only that the system register 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. The user entity is responsible for identifying the users and supplying the service organization with a list of authorized users. If the user entity provides a list that inadvertently includes employees who are not authorized, the service organization has still met the criterion. Accordingly, identifying the authorized users and communicating that information to the service organization are not considered CUECs.

(continued)

Description Criteria	*Implementation Guidance*
	The description is presented in accordance with this criterion if the CUECs are complete, accurately described, and relevant to the service organization's achievement of its service commitments and system requirements. *User Entity Responsibilities.* In addition to CUECs, user entities may have other responsibilities when using the system. Those responsibilities are necessary for the user entity to derive the intended benefits of using the services of the service organization. For example, the user of an express delivery service is responsible for providing complete and accurate recipient information and for using appropriate packaging materials. Such responsibilities are referred to as user entity responsibilities. Trust services criterion CC 2.3 states *[t]he entity communicates with external parties regarding matters affecting the functioning of internal control*. This would include communication of user responsibilities. However, because user entity responsibilities can be voluminous, they are often communicated through other methods (for example, by describing them in user manuals). Consequently, disclosure of user entity responsibilities in the description is usually not practical. Instead, management ordinarily identifies in the description the types of communications it makes to external users about user entity responsibilities. The form and content of such communication is the responsibility of service organization management. When service organization management communicates user entity responsibilities only to specific parties (such as in contracts with user entities), management considers whether other intended users of the SOC 2® report are likely to misunderstand it; in that case, management should limit the use of the report to those specific parties. If service organization management does not want to limit the use of the report, management would include the significant user entity responsibilities in the description of the service organization's system to prevent

Description Criteria	*Implementation Guidance*
	users from misunderstanding the system and the service auditor's report. In that case, the report would be appropriate for the broad range of SOC 2® users. When service organization management includes significant user entity responsibilities in the description, management evaluates those disclosures as part of its evaluation about whether the description is presented in accordance with the description criteria.
DC 7: If the service organization uses a subservice organization and the controls 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, the following: *a.* When service organization management elects to use the inclusive method: i. The nature of the service provided by the subservice organization ii. The controls 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 are achieved	*Inclusive method.* When service organization management elects the inclusive method, the relevant aspects of the subservice organization's infrastructure, software, people, procedures and data are considered part of the service organization's system and are included in the description of the service organization's system. Although the relevant aspects are considered a part of the service organization's system, the portions of the system that are attributable to the subservice organization would be separately identified in the description. Such disclosures include the aspects of the internal control components relevant to identification and assessment of risks that would prevent the service organization from achieving its service commitments and system requirements and the design, implementation, and operation of controls to address them. The description would separately identify controls at the service organization and controls at the subservice organization. However, there is no prescribed format for differentiating between the two. *Carve-out method.* When service organization management elects the carve-out method, consideration may be given to disclosure of the identity of the subservice organization when such information may be useful to user entities or business partners who want to obtain information about and perform procedures related to the services provided by the subservice organization.

(continued)

Description Criteria	*Implementation Guidance*
iii. Relevant aspects of the subservice organization's infrastructure, software, people, procedures, and data iv. The portions of the system that are attributable to the subservice organization *b.* When service organization management decides to use the carve-out method: i. The nature of the service provided by the subservice organization ii. Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization iii. 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 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 (commonly referred to as complementary subservice organization controls or CSOCs)	Complementary subservice organization controls (CSOCs) are controls that service organization management assumed, in the design of the system, would be implemented by subservice organizations and 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. When using the carve-out method, the description would identify the types of CSOCs that the subservice organization is assumed to have implemented. It is important that the description also includes the subservice organization's responsibilities for implementing those CSOCs and indicates that the related service commitments and system requirements can be achieved only if the CSOCs are suitably designed and operating effectively during the period addressed by the description. To be meaningful to report users, management includes only CSOCs that are specific to the services provided by the system being described. CSOCs may be presented as broad categories of controls or types of controls rather than as individual controls. Service organization management may wish to include in the description a table that identifies those instances in which service commitments and system requirements are achieved solely by the service organization's controls and those in which a combination of controls at the service organization and CSOCs are needed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. Examples of CSOCs include the following: • Controls relevant to the completeness and accuracy of transaction processing on behalf of the service organization • Controls relevant to the completeness and accuracy of specified reports provided to and used by the service organization

Description Criteria	*Implementation Guidance*
	• General IT controls relevant to the processing performed for the service organization • Data centers are protected against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). The description is presented in accordance with this criterion if the CSOCs are complete, accurately described, and relevant to the service organization's achievement of the service commitments and system requirements related to the system being described. *Other matters.* A service organization that uses multiple subservice organizations may prepare its description using the carve-out method for one or more subservice organizations and the inclusive method for others. Regardless of the method service organization management selects, the description 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. Such monitoring controls may include, but are not limited to, a combination of the following: • Testing of controls at the subservice organization by members of the service organization's internal audit function • Reviewing and reconciling output reports • Holding periodic discussions with the subservice organization personnel and evaluating subservice organization performance against established service level objectives and agreements • Making site visits to the subservice organization • Inspecting type 2 SOC 2® reports on the subservice organization's system

(continued)

Description Criteria	*Implementation Guidance*
	• Monitoring external communications, such as complaints from user entities relevant to the services performed by the subservice organization
DC 8: Any specific criterion of the applicable trust services criteria that is not relevant to the system and the reasons it is not relevant	If one or more applicable trust services criteria are not relevant to the system being described, service organization management includes in the description an explanation of why such criteria are not relevant. For example, an applicable trust services criterion may not be relevant if it does not apply to the services provided by the service organization. Assume user entities—not the service organization—collect personal information from the user entities' customers. When the description addresses controls over privacy, service organization management would not disclose in its description the user entities' controls over collection; however, the reason for that omission would be disclosed. In contrast, the existence of a policy prohibiting certain activities is not sufficient to render a criterion not applicable. For example, when the description addresses controls over privacy, it would be inappropriate for service organization management to omit from the description disclosures of personal information to third parties based only on the fact that the service organization's policies forbid such disclosures. Instead, the description would describe the policies and related controls for preventing or detecting such disclosures.
DC 9: In a description that covers a period of time (type 2 examination), the relevant details of significant changes to the service organization's system and controls during that period that are relevant to the service organization's service commitments and system requirements	Significant changes to be disclosed consist of those that are likely to be relevant to the broad range of report users. Disclosure of such changes is expected to include an appropriate level of detail, such as the date the changes occurred and how the system differed before and after the changes. Examples of significant changes to a system include the following: • Changes to the services provided • Significant changes to IT and security personnel

Description Criteria	*Implementation Guidance*
	• Significant 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)

Supplement B

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

This supplement contains authoritative AICPA Assurance Services Executive Committee material.

The trust services criteria for security, availability, processing integrity, confidentiality, and privacy and the related points of focus in this supplement have been extracted from TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*,[1] issued in April 2017 by the AICPA's Assurance Services Executive Committee.[2] The complete text may be found at www.aicpa.org/cybersecurityriskmanagement.

The following table presents the trust services criteria and the related points of focus for security, availability, processing integrity, confidentiality, and privacy, which are applicable to a SOC 2® examination. In the table, criteria and related points of focus that come directly from the Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control—Integrated Framework* (COSO framework)[3] are presented using a normal font. In contrast, criteria and points of focus that apply to engagements using the trust services criteria are presented in *italics*.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	CONTROL ENVIRONMENT
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:

(continued)

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

[2] The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. Until that date, service auditors may use either the 2016 trust services criteria or the 2017 trust services criteria as the evaluation criteria in a SOC 2® examination. After that date, the 2016 trust services criteria will be considered superseded. During the transition period, management and the service auditor should identify in the SOC 2® report whether the 2017 or 2016 trust services criteria were used.

In addition, the 2014 trust services criteria will continue to be codified in TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they are available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

[3]

	• Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.
	• Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.
	• Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
	• Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.*
CC1.2	**COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
	• Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.
	• Operates Independently—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.

	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Supplements Board Expertise—The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.*
CC1.3	**COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.
	• Establishes Reporting Lines—Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.
	• Defines, Assigns, and Limits Authorities and Responsibilities—Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Addresses Specific Requirements When Defining Authorities and Responsibilities—Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.*
	• *Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities—Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.*

(continued)

CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Establishes Policies and Practices—Policies and practices reflect expectations of competence necessary to support the achievement of objectives.
	• Evaluates Competence and Addresses Shortcomings—The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.
	• Attracts, Develops, and Retains Individuals—The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.
	• Plans and Prepares for Succession—Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers the Background of Individuals—The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Considers the Technical Competency of Individuals—The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Provides Training to Maintain Technical Competencies—The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.*

CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Enforces Accountability Through Structures, Authorities, and Responsibilities—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.
	• Establishes Performance Measures, Incentives, and Rewards—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.
	• Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance—Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.
	• Considers Excessive Pressures—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.
	• Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate.
	COMMUNICATION AND INFORMATION
CC2.1	**COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Identifies Information Requirements—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.

(continued)

	• Captures Internal and External Sources of Data—Information systems capture internal and external sources of data.
	• Processes Relevant Data Into Information—Information systems process and transform relevant data into information.
	• Maintains Quality Throughout Processing—Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.
CC2.2	**COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.
	• Communicates With the Board of Directors—Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.
	• Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the information.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Communicates Responsibilities—Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.*

	• *Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters—Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.*
	• *Communicates Objectives and Changes to Objectives —The entity communicates its objectives and changes to those objectives to personnel in a timely manner.*
	• *Communicates Information to Improve Security Knowledge and Awareness—The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.*
	Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:
	• ***Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.***
	• ***Communicates System Objectives—The entity communicates its objectives to personnel to enable them to carry out their responsibilities.***
	• ***Communicates System Changes—System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.***
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.

(continued)

	• Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.
	• Communicates With the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.
	• Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.
	Additional point of focus that applies only to an engagement using the trust services criteria for confidentiality:
	• *Communicates Objectives Related to Confidentiality and Changes to Objectives— The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.*
	Additional point of focus that applies only to an engagement using the trust services criteria for privacy:
	• *Communicates Objectives Related to Privacy and Changes to Objectives—The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.*
	Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:
	• ***Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.***
	• ***Communicates System Objectives—The entity communicates its system objectives to appropriate external users.***

	• ***Communicates System Responsibilities—External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.***
	• ***Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters—External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.***
	RISK ASSESSMENT
CC3.1	**COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	Operations Objectives • Reflects Management's Choices—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.
	• Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	• Includes Operations and Financial Performance Goals—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.
	• Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.
	External Financial Reporting Objectives • Complies With Applicable Accounting Standards—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.
	• Considers Materiality—Management considers materiality in financial statement presentation.

(continued)

	• Reflects Entity Activities—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.
	External Nonfinancial Reporting Objectives • Complies With Externally Established Frameworks—Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.
	• Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.
	• Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits.
	Internal Reporting Objectives • Reflects Management's Choices—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.
	• Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.
	• Reflects Entity Activities—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.
	Compliance Objectives • Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.
	• Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Establishes Sub-objectives to Support Objectives—Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.*

CC3.2	**COSO Principle 7: 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 following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.
	• Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.
	• Involves Appropriate Levels of Management—The entity puts into place effective risk assessment mechanisms that involve appropriate levels of management.
	• Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
	• Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.*
	• *Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties—The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.*

(continued)

	• *Considers the Significance of the Risk—The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.*
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers Various Types of Fraud—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
	• Assesses Incentives and Pressures—The assessment of fraud risks considers incentives and pressures.
	• Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.
	• Assesses Attitudes and Rationalizations—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers the Risks Related to the Use of IT and Access to Information—The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.*
CC3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.

	• Assesses Changes in the Business Model—The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
	• Assesses Changes in Leadership—The entity considers changes in management and respective attitudes and philosophies on the system of internal control.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Assesses Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.*
	• *Assesses Changes in Vendor and Business Partner Relationships—The risk identification process considers changes in vendor and business partner relationships.*
	MONITORING ACTIVITIES
CC4.1	**COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations.
	• Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.
	• Establishes Baseline Understanding—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.
	• Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.
	• Integrates With Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions.

(continued)

	• Adjusts Scope and Frequency—Management varies the scope and frequency of separate evaluations depending on risk.
	• Objectively Evaluates—Separate evaluations are performed periodically to provide objective feedback.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers Different Types of Ongoing and Separate Evaluations—Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.*
CC4.2	**COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Assesses Results—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
	• Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.
	• Monitors Corrective Action—Management tracks whether deficiencies are remedied on a timely basis.
	CONTROL ACTIVITIES
CC5.1	**COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Integrates With Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.

	• Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
	• Determines Relevant Business Processes—Management determines which relevant business processes require control activities.
	• Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.
	• Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity.
	• Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, management selects and develops alternative control activities.
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
	• Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
	• Establishes Relevant Security Management Process Controls Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.

(continued)

	• Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.
CC5.3	**COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Establishes Policies and Procedures to Support Deployment of Management's Directives—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
	• Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.
	• Performs in a Timely Manner—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.
	• Takes Corrective Action—Responsible personnel investigate and act on matters identified as a result of executing control activities.
	• Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.
	• Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.
	Logical and Physical Access Controls
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 following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

	• *Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.*
	• *Restricts Logical Access—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 is restricted through the use of access control software and rule sets.*
	• *Identifies and Authenticates Users—Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely.*
	• *Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.*
	• *Manages Points of Access—Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.*
	• *Restricts Access to Information Assets—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.*
	• *Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure and software.*
	• *Manages Credentials for Infrastructure and Software—New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.*
	• *Uses Encryption to Protect Data—The entity uses encryption to supplement other measures used to protect data-at-rest, when such protections are deemed appropriate based on assessed risk.*
	• *Protects Encryption Keys—Processes are in place to protect encryption keys during generation, storage, use, and destruction.*

(continued)

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.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Controls Access Credentials to Protected Assets—Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.*
	• *Removes Access to Protected Assets When Appropriate—Processes are in place to remove credential access when an individual no longer requires such access.*
	• *Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.*
CC6.3	***The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Creates or Modifies Access to Protected Information Assets—Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.*
	• *Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets when an individual no longer requires access.*
	• *Uses Role-Based Access Controls—Role-based access control is utilized to support segregation of incompatible functions.*

CC6.4	***The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Creates or Modifies Physical Access—Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.*
	• *Removes Physical Access—Processes are in place to remove access to physical resources when an individual no longer requires access.*
	• *Reviews Physical Access—Processes are in place to periodically review physical access to ensure consistency with job responsibilities.*
CC6.5	***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.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Identifies Data and Software for Disposal—Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.*
	• *Removes Data and Software From Entity Control—Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.*
CC6.6	***The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

(continued)

	• *Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.*
	• *Protects Identification and Authentication Credentials—Identification and authentication credentials are protected during transmission outside its system boundaries.*
	• *Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.*
	• *Implements Boundary Protection Systems—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.*
CC6.7	***The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement and removal of information.*
	• *Uses Encryption Technologies or Secure Communication Channels to Protect Data—Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.*
	• *Protects Removal Media—Encryption technologies and physical asset protections are used for removable media (such as USB drives and back-up tapes), as appropriate.*
	• *Protects Mobile Devices—Processes are in place to protect mobile devices (such as laptops, smart phones and tablets) that serve as information assets.*

CC6.8	***The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts Application and Software Installation—The ability to install applications and software is restricted to authorized individuals.*
	• *Detects Unauthorized Changes to Software and Configuration Parameters—Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.*
	• *Uses a Defined Change Control Process—A management-defined change control process is used for the implementation of software.*
	• *Uses Antivirus and Anti-Malware Software—Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.*
	• *Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.*
	System Operations
CC7.1	***To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Uses Defined Configuration Standards—Management has defined configuration standards.*
	• *Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.*

(continued)

	• *Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.*
	• *Detects Unknown or Unauthorized Components—Procedures are in place to detect the introduction of unknown or unauthorized components.*
	• *Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.*
CC7.2	***The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.*
	• *Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.*
	• *Implements Filters to Analyze Anomalies—Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.*

	• *Monitors Detection Tools for Effective Operation—Management has implemented processes to monitor the effectiveness of detection tools.*
CC7.3	***The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Responds to Security Incidents—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.*
	• *Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.*
	• *Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.*
	Additional points of focus that apply only in an engagement using the trust services criteria for privacy:
	• *Assesses the Impact on Personal Information—Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.*
	• *Determines Personal Information Used or Disclosed—When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.*
CC7.4	***The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

(continued)

	• *Assigns Roles and Responsibilities—Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.*
	• *Contains Security Incidents—Procedures are in place to contain security incidents that actively threaten entity objectives.*
	• *Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.*
	• *Ends Threats Posed by Security Incidents—Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.*
	• *Restores Operations—Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.*
	• *Develops and Implements Communication Protocols for Security Incidents—Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.*
	• *Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.*
	• *Remediates Identified Vulnerabilities—Identified vulnerabilities are remediated through the development and execution of remediation activities.*
	• *Communicates Remediation Activities—Remediation activities are documented and communicated in accordance with the incident response program.*
	• *Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness on a periodic basis.*
	• *Periodically Evaluates Incidents—Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.*

	Additional points of focus that apply only in an engagement using the trust services criteria for privacy:
	• *Communicates Unauthorized Use and Disclosure—Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.*
	• *Application of Sanctions—The conduct of individuals and organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.*
CC7.5	***The entity identifies, develops, and implements activities to recover from identified security incidents.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.*
	• *Communicates Information About the Event—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).*
	• *Determines Root Cause of the Event—The root cause of the event is determined.*
	• *Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.*
	• *Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.*
	• *Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*

(continued)

	Change Management
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.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software and procedures) is used to support system availability and processing integrity.*
	• *Authorizes Changes—A process is in place to authorize system changes prior to development.*
	• *Designs and Develops Changes—A process is in place to design and develop system changes.*
	• *Documents Changes—A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.*
	• *Tracks System Changes—A process is in place to track system changes prior to implementation.*
	• *Configures Software—A process is in place to select and implement the configuration parameters used to control the functionality of software.*
	• *Tests System Changes—A process is in place to test system changes prior to implementation.*
	• *Approves System Changes—A process is in place to approve system changes prior to implementation.*
	• *Deploys System Changes—A process is in place to implement system changes.*
	• *Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.*
	• *Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.*

	• *Creates Baseline Configuration of IT Technology—A baseline configuration of IT and control systems is created and maintained.*
	• *Provides for Changes Necessary in Emergency Situations—A process is in place for authorizing, designing, testing, approving and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent timeframe).*
	Additional points of focus that apply only in an engagement using the trust services criteria for confidentiality:
	• *Protects Confidential Information—The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality.*
	Additional points of focus that apply only in an engagement using the trust services criteria for privacy:
	• *Protects Personal Information—The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.*
	Risk Mitigation
CC9.1	***The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Considers Mitigation of Risks of Business Disruption—Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during response, mitigation, and recovery efforts.*
	• *Considers the Use of Insurance to Mitigate Financial Impact Risks—The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.*

(continued)

CC9.2	***The entity assesses and manages risks associated with vendors and business partners.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Establishes Requirements for Vendor and Business Partner Engagements—The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.*
	• *Assesses Vendor and Business Partner Risks—The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.*
	• *Assigns Responsibility and Accountability for Managing Vendors and Business Partners—The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.*
	• *Establishes Communication Protocols for Vendors and Business Partners—The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.*
	• *Establishes Exception Handling Procedures From Vendors and Business Partners —The entity establishes exception handling procedures for service or product issues related to vendors and business partners.*
	• *Assesses Vendor and Business Partner Performance—The entity periodically assesses the performance of vendors and business partners.*
	• *Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—The entity implements procedures for addressing issues identified with vendor and business partner relationships.*
	• *Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.*
	Additional points of focus that apply only to an engagement using the trust services criteria for confidentiality:

	• *Obtains Confidentiality Commitments from Vendors and Business Partners—The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.*
	• *Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners—On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.*
	Additional points of focus that apply only to an engagement using the trust services criteria for privacy:
	• *Obtains Privacy Commitments from Vendors and Business Partners—The entity obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information.*
	• *Assesses Compliance with Privacy Commitments of Vendors and Business Partners—On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.*
	ADDITIONAL CRITERIA FOR AVAILABILITY
A1.1	***The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Measures Current Usage—The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.*
	• *Forecasts Capacity—The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.*

(continued)

	• *Makes Changes Based on Forecasts—The system change management process is initiated when forecasted usage exceeds capacity tolerances.*
A1.2	***The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services availability criteria, highlight important characteristics relating to this criterion:
	• *Identifies Environmental Threats—As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.*
	• *Designs Detection Measures—Detection measures are implemented to identify anomalies that could result from environmental threat events.*
	• *Implements and Maintains Environmental Protection Mechanisms— Management implements and maintains environmental protection mechanisms to prevent and mitigate against environmental events.*
	• *Implements Alerts to Analyze Anomalies—Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.*
	• *Responds to Environmental Threat Events—Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator back-up subsystem).*
	• *Communicates and Reviews Detected Environmental Threat Events—Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system, and actions are taken, if necessary.*
	• *Determines Data Requiring Backup—Data is evaluated to determine whether backup is required.*
	• *Performs Data Backup—Procedures are in place for backing up data, monitoring to detect back-up failures, and initiating corrective action when such failures occur.*

	• *Addresses Offsite Storage—Back-up data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.*
	• *Implements Alternate Processing Infrastructure—Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.*
A1.3	***The entity tests recovery plan procedures supporting system recovery to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Implements Business Continuity Plan Testing—Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*
	• *Tests Integrity and Completeness of Back-Up Data—The integrity and completeness of back-up information is tested on a periodic basis.*
	ADDITIONAL CRITERIA FOR CONFIDENTIALITY
C1.1	***The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.***
	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Identifies Confidential information—Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.*
	• *Protects Confidential Information From Destruction—Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.*

(continued)

C1.2	***The entity disposes of confidential information to meet the entity's objectives related to confidentiality.***
	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Identifies Confidential Information for Destruction—Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.*
	• *Destroys Confidential Information—Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.*
	ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY
PI1.1	***The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Identifies Information Specifications—The entity identifies information specifications required to support the use of products and services.*
	• *Defines Data Necessary to Support a Product or Service—When data is provided as part of a service or product or as part of a reporting obligation related to a product or service:* *(1) The definition of the data is available to the users of the data* *(2) The definition of the data includes the following information:* *— The population of events or instances included in the data* *— The nature of each element (for example, field) of the data (that is, the event or instance to which the data element relates, for example, transaction price of a sale of XYZ Corporation stock for the last trade in that stock on a given day)* *— Source(s) of the data*

	— *The unit(s) of measurement of data elements (for example, fields)* — *The accuracy/correctness/precision of measurement* — *The uncertainty or confidence interval inherent in each data element and in the population of those elements* — *The date the data was observed or the period of time during which the events relevant to the data occurred* — *The factors in addition to the date and period of time used to determine the inclusion and exclusion of items in the data elements and population* *(3) The definition is complete and accurate.* *(4) The description of the data identifies any information that is necessary to understand each data element and the population in a manner consistent with its definition and intended purpose (meta-data) that has not been included within the data.*
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.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Defines Characteristics of Processing Inputs—The characteristics of processing inputs that are necessary to meet requirements are defined.*
	• *Evaluates Processing Inputs—Processing inputs are evaluated for compliance with defined input requirements.*
	• *Creates and Maintains Records of System Inputs—Records of system input activities are created and maintained completely and accurately in a timely manner.*
PI1.3	***The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:

(continued)

	• *Defines Processing Specifications—The processing specifications that are necessary to meet product or service requirements are defined.*
	• *Defines Processing Activities—Processing activities are defined to result in products or services that meet specifications.*
	• *Detects and Corrects Production Errors—Errors in the production process are detected and corrected in a timely manner.*
	• *Records System Processing Activities—System processing activities are recorded completely and accurately in a timely manner.*
	• *Processes Inputs—Inputs are processed completely, accurately, and timely as authorized in accordance with defined processing activities.*
PI1.4	***The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Protects Output—Output is protected when stored or delivered, or both, to prevent theft, destruction, corruption, or deterioration that would prevent output from meeting specifications.*
	• *Distributes Output Only to Intended Parties—Output is distributed or made available only to intended parties.*
	• *Distributes Output Completely and Accurately—Procedures are in place to provide for the completeness, accuracy, and timeliness of distributed output.*
	• *Creates and Maintains Records of System Output Activities—Records of system output activities are created and maintained completely and accurately in a timely manner.*
PI1.5	***The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:

	• *Protects Stored Items—Stored items are protected to prevent theft, corruption, destruction, or deterioration that would prevent output from meeting specifications.*
	• *Archives and Protects System Records—System records are archived, and archives are protected against theft, corruption, destruction, or deterioration that would prevent them from being used.*
	• *Stores Data Completely and Accurately—Procedures are in place to provide for the complete, accurate, and timely storage of data.*
	• *Creates and Maintains Records of System Storage Activities—Records of system storage activities are created and maintained completely and accurately in a timely manner.*
	ADDITIONAL CRITERIA FOR PRIVACY
P1.0	**Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy**
P1.1	***The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates to Data Subjects—Notice is provided to data subjects regarding the following:* — *Purpose for collecting personal information* — *Choice and consent* — *Types of personal information collected* — *Methods of collection (for example, use of cookies or other tracking techniques)* — *Use, retention, and disposal* — *Access* — *Disclosure to third parties* — *Security for privacy* — *Quality, including data subjects' responsibilities for quality* — *Monitoring and enforcement* • *If personal information is collected from sources other than the individual, such sources are described in the privacy notice.*

(continued)

	• *Provides Notice to Data Subjects—Notice is provided to data subjects (1) at or before the time personal information is collected or as soon as practical thereafter, (2) at or before the entity changes its privacy notice or as soon as practical thereafter, or (3) before personal information is used for new purposes not previously identified.*
	• *Covers Entities and Activities in Notice—An objective description of the entities and activities covered is included in the entity's privacy notice.*
	• *Uses Clear and Conspicuous Language—The entity's privacy notice is conspicuous and uses clear language.*
P2.0	**Privacy Criteria Related to Choice and Consent**
P2.1	***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.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates to Data Subjects—Data subjects are informed (a) about the choices available to them with respect to the collection, use, and disclosure of personal information and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.*
	• *Communicates Consequences of Denying or Withdrawing Consent—When personal information is collected, data subjects are informed of the consequences of refusing to provide personal information or denying or withdrawing consent to use personal information for purposes identified in the notice.*
	• *Obtains Implicit or Explicit Consent—Implicit or explicit consent is obtained from data subjects at or before the time personal information is collected or soon thereafter. The individual's preferences expressed in his or her consent are confirmed and implemented.*

	• *Documents and Obtains Consent for New Purposes and Uses—If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the data subject is notified, and implicit or explicit consent is obtained prior to such new use or purpose.*
	• *Obtains Explicit Consent for Sensitive Information—Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.*
	• *Obtains Consent for Data Transfers—Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.*
P3.0	**Privacy Criteria Related to Collection**
P3.1	***Personal information is collected consistent with the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Limits the Collection of Personal Information—The collection of personal information is limited to that necessary to meet the entity's objectives.*
	• *Collects Information by Fair and Lawful Means—Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.*
	• *Collects Information From Reliable Sources—Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.*
	• *Informs Data Subjects When Additional Information Is Acquired—Data subjects are informed if the entity develops or acquires additional information about them for its use.*

(continued)

P3.2	***For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Obtains Explicit Consent for Sensitive Information—Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.*
	• *Documents Explicit Consent to Retain Information—Documentation of explicit consent for the collection, use, or disclosure of sensitive personal information is retained in accordance with objectives related to privacy.*
P4.0	**Privacy Criteria Related to Use, Retention, and Disposal**
P4.1	***The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Uses Personal Information for Intended Purposes—Personal information is used only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained unless a law or regulation specifically requires otherwise.*
P4.2	***The entity retains personal information consistent with the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Retains Personal Information—Personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.*

	• *Protects Personal Information—Policies and procedures have been implemented to protect personal information from erasure or destruction during the specified retention period of the information.*
P4.3	***The entity securely disposes of personal information to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Captures, Identifies, and Flags Requests for Deletion—Requests for deletion of personal information are captured, and information related to the requests is identified and flagged for destruction to meet the entity's objectives related to privacy.*
	• *Disposes of, Destroys, and Redacts Personal Information—Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.*
	• *Destroys Personal Information—Policies and procedures are implemented to erase or otherwise destroy personal information that has been identified for destruction.*
P5.0	**Privacy Criteria Related to Access**
P5.1	***The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Authenticates Data Subjects' Identity—The identity of data subjects who request access to their personal information is authenticated before they are given access to that information.*

(continued)

	• *Permits Data Subjects Access to Their Personal Information—Data subjects are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.*
	• *Provides Understandable Personal Information Within Reasonable Time—Personal information is provided to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any.*
	• *Informs Data Subjects If Access Is Denied—When data subjects are denied access to their personal information, the entity informs them of the denial and the reason for the denial in a timely manner, unless prohibited by law or regulation.*
P5.2	***The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates Denial of Access Requests—Data subjects are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.*
	• *Permits Data Subjects to Update or Correct Personal Information—Data subjects are able to update or correct personal information held by the entity. The entity provides such updated or corrected information to third parties that were previously provided with the data subject's personal information consistent with the entity's objective related to privacy.*
	• *Communicates Denial of Correction Requests—Data subjects are informed, in writing, about the reason a request for correction of personal information was denied and how they may appeal.*

P6.0	Privacy Criteria Related to Disclosure and Notification
P6.1	***The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates Privacy Policies to Third Parties—Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.*
	• *Discloses Personal Information Only When Appropriate—Personal information is disclosed to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject, unless a law or regulation specifically requires otherwise.*
	• *Discloses Personal Information Only to Appropriate Third Parties—Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.*
	• *Discloses Information to Third Parties for New Purposes and Uses—Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of data subjects.*
P6.2	***The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:
	• *Creates and Retains Record of Authorized Disclosures—The entity creates and maintains a record of authorized disclosures of personal information that is complete, accurate, and timely.*

(continued)

P6.3	***The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:
	• *Creates and Retains Record of Detected or Reported Unauthorized Disclosures—The entity creates and maintains a record of detected or reported unauthorized disclosures of personal information that is complete, accurate, and timely.*
P6.4	***The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Discloses Personal Information Only to Appropriate Third Parties—Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.*
	• *Remediates Misuse of Personal Information by a Third Party —The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*

P6.5	***The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Remediates Misuse of Personal Information by a Third Party—The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
	• *Reports Actual or Suspected Unauthorized Disclosures—A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of personal information.*
P6.6	***The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Remediates Misuse of Personal Information by a Third Party—The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
	• *Provides Notice of Breaches and Incidents—The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.*
P6.7	***The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:

(continued)

	• *Identifies Types of Personal Information and Handling Process—The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified.*
	• *Captures, Identifies, and Communicates Requests for Information—Requests for an accounting of personal information held and disclosures of the data subjects' personal information are captured, and information related to the requests is identified and communicated to data subjects to meet the entity's objectives related to privacy.*
P7.0	**Privacy Criteria Related to Quality**
P7.1	***The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Ensures Accuracy and Completeness of Personal Information—Personal information is accurate and complete for the purposes for which it is to be used.*
	• *Ensures Relevance of Personal Information—Personal information is relevant to the purposes for which it is to be used.*
P8.0	**Privacy Criteria Related to Monitoring and Enforcement**
P8.1	***The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates to Data Subjects—Data subjects are informed about how to contact the entity with inquiries, complaints, and disputes.*
	• *Addresses Inquiries, Complaints, and Disputes—A process is in place to address inquiries, complaints, and disputes.*

	• *Documents and Communicates Dispute Resolution and Recourse—Each complaint is addressed, and the resolution is documented and communicated to the individual.*
	• *Documents and Reports Compliance Review Results—Compliance with objectives related to privacy are reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.*
	• *Documents and Reports Instances of Noncompliance—Instances of noncompliance with objectives related to privacy are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.*
	• *Performs Ongoing Monitoring—Ongoing procedures are performed for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.*

Appendix A

Information for Service Organization Management

This appendix is nonauthoritative and is included for informational purposes only.

The purpose of this appendix is to assist service organization management with understanding its responsibilities in a SOC examination. It is also intended to provide helpful guidance to management when discharging those responsibilities.

Introduction and Background

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.

Examples of the types of services provided by service organizations are as follows:

- *Customer support.* Providing customers of user entities with online or telephonic post-sales support and service management. 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.
- *Enterprise 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.

- *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 (FinTech) services.* Providing financial services companies with IT-based transaction processing services. Examples of such transactions are loan processing, peer-to-peer lending, payment processing, crowdfunding, big data analytics, and asset management.

Although these relationships may increase revenues, expand market opportunities and reduce costs for the user entities and business partners, they also result in additional risks arising from interactions with the service organization and its system. Accordingly, the management of those 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.

To 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[1] 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® report is the result of an examination of whether (*a*) the description of the service organization's system presents the system that was designed and implemented in accordance with the description criteria, (*b*) the suitability of the design of controls would 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).[2,3] This examination is referred to as a *SOC 2® examination.*

---

[1] In this appendix, *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 appendix refers to "controls that provide reasonable assurance," it means the controls that make up the system of internal control.

[2] As discussed in paragraph 2.59, 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 service criteria.

[3] 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 1.31.

Because the informational needs of SOC 2® report users vary, there are two types of SOC 2® examinations and related reports:

- A type 1 examination is an examination of whether
  - — 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
  - — 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*.
- A type 2 examination also addresses the description of the system and the suitability of design of the controls, but it also 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 type 2 examination also includes a detailed description of the service auditor's[4] tests of controls and the results of those tests. A report on such an examination is referred to as a *type 2 report*.

Management may engage a service auditor to perform *either* a type 1 or a type 2 examination. Management may not engage a service auditor to examine and express an opinion on the description of the service organization's system and the suitability of design of certain controls stated in the description and to express an opinion on the operating effectiveness of other controls stated in the description.

Intended Users of a SOC 2® Report

A SOC 2® report, whether a type 1 or a type 2 report, is usually intended to provide report users with information about the service organization's system 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. For instance, the description of the service organization's system is 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.

---

[4] 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.

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. 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, management and the service auditor should agree on the intended users of the report (referred to as *specified parties*). 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,[5] and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls[6] 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

Specified parties that are likely to possess sufficient knowledge to understand a SOC 2® report may include service organization personnel, 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 user entities and business partners, and regulators who have sufficient knowledge and understanding of such matters.

Other parties may also have the requisite knowledge and understanding. 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. (If prospective users lack such knowledge and understanding, management may instead engage a service auditor to provide a SOC 3® report, as discussed later.)

Because of the knowledge that intended users need to understand the SOC 2® report, the service auditor's report is required to be restricted to specified parties who possess that knowledge.

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

---

[5] 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 these two methods for treating subservice organizations.

[6] In the July 2015 version of this guide, these controls were referred to as "controls expected to be implemented at carved-out subservice organizations."

and understanding required to understand the SOC 2® report. In that case, management may engage a service auditor to examine and express an opinion on the effectiveness of controls within a service organization system in a SOC 3® examination. A SOC 3® report is ordinarily appropriate for general users. (See the section titled "SOC 3® Examination.")

Overview of a SOC 2® Examination

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.

A service auditor performs a SOC 2® examination in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*,[7] and AT-C section 205, *Examination Engagements*. Those standards establish performance and reporting requirements for the SOC 2® examination. According to those standards, an attestation examination is predicated on the concept that a party other than the practitioner (the responsible party) makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria. An *assertion* is any declaration or set of declarations about whether the subject matter is in accordance with (or based on) the criteria. The AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* provides guidance on performing and reporting in a SOC 2® examination.

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. In addition, the service auditor is required by the attestation standards to request a written assertion from management. Management's written assertion 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.

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

[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.

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

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.

Table 1-1[9]

Contents of a SOC 2® Report

Type 1 Report	*Type 2 Report*
1. Description of the system as of a point in time in accordance with the description criteria	1. 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

[9] This table can also be found in chapter 1, "Introduction and Background."

Contents of a SOC 2® Report—*continued*

Type 1 Report	*Type 2 Report*
3. The service auditor's opinion about whether *a.* the description of the service organization's system as fof 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	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, *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

Difference Between Privacy and Confidentiality

Some individuals consider effective privacy practices to be the same as effective practices over confidential information. Privacy applies only to personal information,[10] whereas confidentiality applies to various types of sensitive information.[11] Therefore, a SOC 2® examination that includes the trust

[10] 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).

[11] 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.

services privacy criteria encompasses the service organization's specific processes that address each of the following, as applicable:

- Notice of the service organization's privacy commitments and practices
- 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

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.

Criteria for a SOC 2® Examination

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*,[12] includes the criteria used to prepare and evaluate the description of the service organization's system.
- *Trust services criteria*. TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*,[13] 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.

Description Criteria[14]

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, DC section 200 also includes implementation

---

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

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

[14] The description criteria presented in supplement A, "2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report," (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*, as discussed in the following footnote. 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*, in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are codified as DC section 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*.

(continued)

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 should carefully consider the facts and circumstances of the entity and its environment in actual situations when applying the description criteria.

The description criteria in DC section 200 were promulgated by the Assurance Services Executive Committee (ASEC), 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 description criteria are published by the AICPA and made available to the public, they are considered available to report users. Therefore, the description criteria are both suitable and available for use in a SOC 2® engagement.

Trust Services Criteria[15]

The trust services criteria in TSP section 100 are used to evaluate the suitability of design and operating effectiveness of controls related to one or more of the trust services categories (security, availability, processing integrity, confidentiality, and privacy). The engaging party, typically service organization management, may choose to engage the service auditor to report on controls related to one or more of these categories.

Service organization management evaluates the suitability of design and operating effectiveness of controls stated in the description to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to the trust services category or categories included within the scope of the examination. Such criteria are referred to as the *applicable trust services criteria*. For example, in a SOC 2® 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, would be the applicable trust services criteria.

(footnote continued)

When preparing a description of the service organization's system as of December 15, 2018, or prior to that date (type 1 examination) or a description for periods ending as of December 15, 2018, or prior to that date (type 2 examination), either the 2018 description criteria or the 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain available in DC section 200A through December 31, 2019. During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

[15] The 2017 trust services criteria are codified in TSP section 100. The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. Until that date, service auditors may use either the 2016 trust services criteria or the 2017 trust services criteria as the evaluation criteria in a SOC 2® examination. After that date, the 2016 trust services criteria will be considered superseded. During the transition period, management and the service auditor should identify in the SOC 2® report whether the 2017 or 2016 trust services criteria were used.

In addition, the 2014 trust services criteria will continue to be codified in TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

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* (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.

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 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.

The criterion for determining, in a type 2 examination, 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 whether manual controls were applied by individuals who have the appropriate competence and authority.

The trust services criteria in TSP section 100 were promulgated by the ASEC. The ASEC has determined that the trust services criteria are both suitable and available for use in a SOC 2® examination.

Categories of Criteria

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.

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 service categories (common criteria) and

- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

For example, if the SOC 2® examination is only on availability, the controls should address all the common criteria and the additional specific criteria for availability.

Common Criteria

The common criteria presented in supplement B, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (CC1–CC5) are organized into the following classifications:

a. Control environment (CC1 series)
b. Communication and information (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 sub-classifications: logical and physical access controls [CC6 series], system operations [CC7 series], change management [CC8 series], and risk mitigation [CC 9 series].)

Table 1-2 identifies the trust services criteria to be used when evaluating the design or operating effectiveness of controls for each of the trust services categories. As shown in that table, the common criteria constitute the complete set of criteria for the security category. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of (*a*) the common criteria (labeled in the table in supplement B and (*b*) the criteria applicable to the specific trust services category or categories addressed by the examination, which are labeled in the table in supplement B as follows:

a. Availability (A series)
b. Processing integrity (PI series)
c. Confidentiality (C series)
d. Privacy (P series)

Table 1-2[16]

Criteria for Evaluating the Design and Operating Effectiveness of Controls

Trust Services Category	*Common Criteria*	*Additional Category-Specific Criteria*
Security	X	
Availability	X	X
Processing integrity	X	X
Confidentiality	X	X
Privacy	X	X

Because each system and the environment in which it operates are unique, the combination of risks that would prevent a service organization from achieving

[16] This table can also be found in chapter 1.

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 the applicable trust services criteria are met, which would mitigate those risks.

Using the Trust Services Criteria to Evaluate Suitability of Design and Operating Effectiveness in a SOC 2® Examination. The trust services criteria presented in TSP section 100 may be 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.

The Service Organization's Service Commitments and System Requirements

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.

Service organization management is responsible for establishing its service commitments and 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

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 request from its customers.

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
- System edits that restrict the values accepted for system input, which are defined in application design documents
- 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])

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).

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 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. 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.

SOC 2® Examination That Addresses Additional Subject Matters and Additional Criteria

Management may engage the service auditor to examine and report on subject matter in addition to the description of the service organization's system in accordance with the description criteria and the suitability of design and operating effectiveness of controls based on the applicable trust services criteria. In that case, the service auditor would also examine and report on whether the additional subject matter is presented in accordance with the additional suitable criteria used to evaluate it. Table 1-3 provides examples of additional subject matters and additional criteria that may be used to evaluate them.

Table 1-3[17]

Additional Subject Matter and Additional Criteria

What Additional Information Might Be Included in the SOC 2® Report?	*What Are the Subject Matters?*	*What Are Suitable Criteria Relevant to the Subject Matters?*
Information on the physical characteristics of a service organization's facilities (for example, square footage)	A detailed description of certain physical characteristics of a service organization's facilities that includes items such as the square footage of the facilities	Criteria to evaluate the presentation of the description of the physical characteristics of the facilities
Information about historical data regarding the availability of computing resources at a service organization	Historical data related to the availability of computing resources	Criteria to evaluate the completeness and accuracy of the historical data
Information about how controls at a service organization help meet the organization's responsibilities related to the security requirements of HIPAA	Compliance with the HIPAA security requirements	Security requirements set forth in the HIPAA Administrative Simplification (Code of Federal Regulations, Title 45, Sections 164.308–316)

[17] This table can also be found in chapter 1.

Additional Subject Matter and Additional Criteria—*continued*

What Additional Information Might Be Included in the SOC 2® Report?	*What Are the Subject Matters?*	*What Are Suitable Criteria Relevant to the Subject Matters?*
Information about how controls at a service organization address the Cloud Security Alliance's Cloud Controls Matrix	Controls related to security at a cloud service provider	Criteria established by the Cloud Security Alliance's Cloud Controls Matrix relevant to the security of a system

A SOC 2® engagement that includes additional subject matters and additional criteria such as that described in the table is predicated on service organization management providing the service auditor with the following:

- An appropriate description of the subject matter
- A description of the criteria identified by management used to measure and present the subject matter
- If the criteria are related to controls, a description of the controls intended to meet the control-related criteria
- An assertion by management regarding the additional subject matter or criteria

SOC 3® Examination

To market its services to prospective customers of the system, a service organization may want to provide them with a SOC 2® report. However, some of those prospective customers (system users) may not have sufficient knowledge about the system, which might cause them to misunderstand the information in the report. Consequently, distribution of the SOC 2® report for general marketing purposes is likely be inappropriate. In this situation, a SOC 3® report, which is a general use report, may be more 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 more general user needs.

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[18] 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

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

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.

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 tests of controls and the results thereof.[19]

Other Types of SOC Examinations: 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 and system- or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the AICPA enables the introduction of new internal control examinations that may be performed (*a*) for other types of organizations, in addition to service organizations, and (*b*) on either system-level or entity-level controls of such organizations. The following are designations for four such examinations in the SOC suite of services:

1. SOC 1®—SOC for Service Organizations: ICFR[20]
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

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,* 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. The controls addressed in AT-C section 320 are those that a service organization implements to prevent, or detect and correct, misstatements[21] in the information it provides to user entities. A service organization's controls are relevant to a user entity's internal control over financial reporting when they are part of the user entity's information and communications component of internal control maintained by the service

---

[19] 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, *Examination Engagements*, 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.

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

[21] A *misstatement* is a difference between the measurement or evaluation of the subject matter by the responsible party and the proper measurement or evaluation of the subject matter based on the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions.

organization.[22] Such an examination is known as a *SOC 1® examination*, and the resulting report is known as a *SOC 1® report.*

Service organizations frequently receive requests from user entities for these reports because they 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 existing user entities (for example, existing customers of the service organization), their financial statement auditors, and management of the service organization. The 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.

SOC for Cybersecurity

Cybersecurity has become a top concern for boards of directors and senior executives of many entities throughout the country, regardless of their size or the industry in which they operate. In addition, governmental 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.

For those reasons, entities have begun requesting practitioners to examine and report on a description of the 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. The performance and reporting requirements for such an examination are found in AT-C section 105 and AT-C section 205. The AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* contains interpretive application guidance for practitioners performing these engagements.

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

[22] 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 the auditing standards with which a service auditor should comply.

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.

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). The AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* contains description criteria and trust services criteria for security, availability, and confidentiality, which may be used in the cybersecurity risk management examination.

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.

Management Responsibilities in a SOC 2® Examination Prior to Engaging the Service Auditor

Prior to engaging a service auditor to perform a SOC 2® examination, service organization management 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 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
    - — Determining whether subservice organizations, if any, are to be addressed in the report using the inclusive method or the carve-out method

  - If a subservice organization is to be presented using the inclusive method, obtaining agreement from subservice 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 analyzing 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 of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria

To increase the likelihood that the description and service auditor's report will be useful to report users, service organization management may discuss some or all of these matters with intended users prior to engaging the service auditor.

Defining the Scope of the Examination

Identifying the Services

The scope of a SOC 2® engagement is defined by the services that the service organization provides to user entities. Services involve the performance of a function on behalf of the user entities. Services may be provided in conjunction with the provision of goods either through lease or sale and may be difficult to distinguish from the lease or sale. For example, maintenance services may be provided in conjunction with the sale of equipment, whereas warranty work performed on the same equipment may not be considered a service but rather a part of the purchase of the equipment. Services may also be dependent on the provision of equipment from the service organization to the user entity. For example, the provision of security monitoring services may require user entities to install the service organization's proprietary software on computer servers in the user entity's network. The services addressed by a SOC 2® examination are usually common to many of its user entities and specified in written agreements between the service organization and the user entities.

Often, service organizations bundle multiple services together as incentives to user entities or to provide the individual services more efficiently and effectively. When the service organization wishes to include only a portion of commonly bundled services in a SOC 2® report, management should consider whether the portion of the services is an appropriate subject matter. Factors to consider include the following:

- Is there a reasonable basis for evaluating the portion of the services to be covered by the scope of the report? For example, a service organization that provides software-as-a-service solutions would likely conclude that it is not appropriate to exclude the testing of software prior to implementation from the scope of services.

However, a service organization that provides software development services, software testing services, and implementation services as separate offerings, each having their own processes and procedures, may conclude that the software development services alone are an appropriate subject matter for a SOC 2® report.

- Will the intended report users understand which services are included in the scope of the SOC 2® report and which are not? If there is a likelihood that report users will conclude that all services are covered in the scope of the examination when only a portion of the services are covered, report users may misunderstand the results of the examination.

When defining the services to be covered by the SOC 2® report, management may find it useful to consider how services are presented in agreements with user entities and how the services are described in service documentation. These agreements may also establish requirements for the service organization to have a SOC 2® engagement. In such instances, the services to be covered may be explicitly stated in the agreement.

Identifying the System

In the SOC 2® examination, a system is defined as the following:

> 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.

The italicized terms are defined as follows:

- *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 supports 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 output 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 prepared

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).

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.

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.

In identifying the system used to provide the services, management may need to consider processes and procedures used to provide the services that may be performed by different business units or functional areas; however, not all processes related to the services are part of the system used to provide the services. For example, the accounting function used to bill user entities for the services is not a part of the system used to deliver the services.

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

In a SOC 2® engagement, the trust services criteria are used to evaluate the suitability of design and operating effectiveness of controls relevant to one or more of the trust services categories of security, availability, processing integrity, confidentiality, and privacy. These categories relate to areas of concern for report users; however, not all services are subject to the same level of concern for each category. When determining the scope of the SOC 2® examination, management determines which categories are likely to be of interest to report users and includes them within the scope of the examination. For example, security and availability may be of concern to user entities of a service organization providing IT infrastructure collocation services; however, processing integrity is unlikely to be of concern to them. Written agreements may

provide information on which category or categories should be included within the scope of the SOC 2® examination.

Period Covered by the Examination

Service organization management is responsible for determining the time frame to be covered by the description of the service organization's system, its assertion, and, consequently, the service auditor's examination. In a type 1 examination, the time frame is as of a specific 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.

For SOC 1® examinations, user entities usually have very explicit needs with respect to the period covered by the examination. Those needs usually do not exist for a SOC 2® report. However, a type 2 report should cover a period of time that is sufficient for the service auditor to obtain sufficient appropriate evidence about the suitability of design and operating effectiveness of the controls. Beyond that consideration, the frequency and the period covered by a SOC 2® report is a business decision of management. Many service organizations use the same period of time for their SOC 1® and SOC 2® examinations because that is often the most efficient approach.

Identifying Subservice Organizations

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. When controls at a 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, 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 company that owns the service organization.

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 services 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.

If the service organization's controls alone achieve its service commitments and system requirements, or if the service organization's monitoring of the vendor's services and controls is sufficient to achieve its service commitments and system requirements, the services provided by a vendor are not likely to be relevant to the SOC 2® examination.

Service organization management is responsible for determining whether it uses a subservice organization. Making that determination is not always easy, as illustrated by the following examples:

- *A vendor that is responsible for performing quarterly maintenance on a service organization's backup power system in an examination that addresses availability.* This vendor would not be considered a subservice organization if the service organization implements its own controls over the vendor's services and vendor controls over its maintenance activities are not 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 for availability.
- *A vendor that provides data center hosting services.* If that vendor is responsible for monitoring server capacity and usage and for projecting future capacity demands based on historical trends, controls at the vendor may be needed for the service organization to achieve its availability commitments based on the applicable trust services criteria for availability. On the other hand, controls at the vendor may not be necessary if the service organization independently performs high-level capacity monitoring activities and reviews the future capacity demands projected by the vendor for appropriateness.

In some instances, a service organization may stipulate in its contract with the vendor that the vendor perform certain controls that the service organization believes are necessary to address the risks related to the vendor's services. For example, a service organization may outsource its application development testing to a vendor and contractually specify that certain controls be executed by the vendor. The service organization designates a service organization employee to oversee the outsourced services, and that employee compares the 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 the vendor before changes to the application are approved by the vendor and submitted to the service organization for user acceptance testing. In this instance, the controls at the vendor may not be 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.

If the vendor is a subservice organization, the service organization's description of its system would include the information set forth in description criterion DC7 in DC section 200, depending on whether the inclusive or carve-out method is used with respect to the subservice organization.

Determining Whether to Use the Inclusive or Carve-Out Method

If the service organization uses a subservice organization, management is responsible for determining whether to carve out or include the subservice organization's controls within the scope of the examination. For that reason, it is important that management 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 (1) the nature of the services performed by the subservice organization; (2) 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 (3) 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 (*a*) the nature of the service provided by the subservice organization and (*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. (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.)

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.

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.

Although the inclusive method provides more information for report users than the carve-out method, the inclusive method may not be appropriate or feasible in all cases. Management may determine that the carve-out method is most practical in the following circumstances:

a. The challenges entailed in implementing the inclusive method, including the extensive planning and communication required among the service auditor, the service organization, and the subservice organization, are sufficiently onerous that it is not practical to use the inclusive method.

b. The service auditor is not independent of the subservice organization. (When the inclusive method is used, the SOC 2® examination covers the service organization and the subservice organization, and the service auditor must be independent of both entities.)

c. A type 1 or type 2 service auditor's report on the subservice organization, which meets the needs of report users, is available.

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

In some cases, the subservice organization's services and controls have a pervasive effect on the service organization's system. In these circumstances, management would consider whether use of the carve-out method may result in a description of the service organization's system that is so limited that it is unlikely to be useful to the intended users of the report. When making this determination, the following factors may be helpful:

- The significance of the portion of the system functions performed by the subservice organization
- The complexity of the services and the types of controls that would be expected to be implemented by the subservice organization
- The extent to which the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria depends on controls at the subservice organization
- The number of applicable trust services criteria that would not be met if the types of controls expected to be implemented at the subservice organization were not implemented
- The ability of the intended users of the report to obtain sufficient appropriate evidence about the design and, in a type 2 examination, the operating effectiveness of controls at the subservice organization

In situations in which the subservice organization's services and controls have a pervasive effect on the service organization's system, management would not be able to use the carve-out method.

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 previously as they relate to the subservice organization. Accordingly, prior to engaging the service auditor, management and the service auditor discuss 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 and the suitability of the design 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.

Identifying Complementary Subservice Organization Controls

As discussed earlier, a subservice organization exists when management identifies certain risks that it expects to be addressed by controls implemented by that subservice organization. When the carve-out method is used, and controls performed by the subservice organization are necessary, in combination with the service organization's controls, to provide reasonable assurance that one

or more of the service organization's service commitments and system requirements were achieved, such controls are referred to as *complementary subservice organization controls* (CSOCs).[23]

Examples of CSOCs include the following:

- Controls relevant to the completeness and accuracy of transaction processing on behalf of the service organization
- Controls relevant to the completeness and accuracy of specified reports provided to and used by the service organization
- Logical access controls relevant to the processing performed for the service organization

Service organization management is required to disclose in its description the types of CSOCs that the subservice organization is assumed to have implemented. In some cases, management may request the service auditor's assistance when determining how to present the CSOCs in the description. For example, the service auditor can provide examples of CSOC disclosures made by others and can make recommendations to improve the presentation of the CSOCs in the description.

Identifying Complementary User Entity Controls and User Entity Responsibilities

Usually, user entities must perform specific activities in order 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 service and do not affect the ability of the service organization to achieve its service commitments and system requirements. These activities are referred to as *user entity responsibilities*. However, in some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the user entity performing certain activities in a defined manner. In these instances, the service organization expects the user entity to implement necessary controls and to perform them completely and accurately in a timely manner. Such controls are referred to as *complementary user entity controls* (CUECs).

A service organization's controls are usually able to provide reasonable assurance that the service organization's service commitments or system requirements were achieved without the implementation of CUECs because the service organization restricts its service commitments and system requirements to those matters that are its responsibility and that it can reasonably perform. Consider, for example, 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 limits the service organization's responsibilities because the criterion requires

[23] In the July 2015 version of this guide, those controls were referred to as *controls expected to be implemented at carved-out subservice organizations.*

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 that inadvertently includes employees who should not have been included, the service organization has still met CC6.2. 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, identifying the authorized users and communicating that information to the service organization are not considered CUECs.

In other situations, a control may be necessary for 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 criterion. 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 at the user entity to protect the components of the service organization's system located at the user entity.

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

In addition to controls that the service organization expects at the subservice organization, 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 the subservice organization has a SOC 2® examination, such activities may be identified in the section of its description that describes CUECs. Such activities may also be described in user documentation published by the subservice organization or the agreement between the service organization and subservice organization. For example, a service organization that outsources aspects of its technology infrastructure to a subservice organization may obtain a type 1 or type 2 SOC 2® report from the subservice organization and discover that the subservice organization's description of its system includes the following CUEC:

> User entities should have controls in place to restrict access to system resources and applications to appropriate user entity personnel.

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

- 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.

Agreeing on the Terms of the Engagement

The attestation standards require the service organization and the service auditor to agree on, and document in a written communication such as an engagement letter, the terms of the engagement with the engaging party. A written agreement 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. For that reason, service organization management acknowledges these responsibilities in an engagement letter or other suitable form of written communication.

The engagement letter 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 American Institute of Certified Public Accountants

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

If the service auditor plans to use internal auditors to provide direct assistance, prior to doing so, the service auditor will also request written acknowledgment from service organization management that internal auditors providing direct assistance will be allowed to follow the service auditor's instructions and that management will not intervene in the work the internal auditor performs for the service auditor. If service organization management is the engaging party, it is likely that this matter will also be included in the engagement letter.

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

Management Responsibilities During the Examination

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
- 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 service organization will not intervene in the work the internal auditor performs 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 are relevant to the description of the service organization's system and assertion
  - Access to additional information that the service auditor may request from management for the examination
  - 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 intentional acts that could adversely affect the presentation of the description of the service organization's system, the suitability of design of its controls, or, in a type 2 examination, the operating effectiveness of controls

- Any 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 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 could have a significant effect on management's assertion

Preparing the Description of the Service Organization's System in Accordance With the Description Criteria

The description of the service organization's system 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.

Service organization management is responsible for preparing the description of the system that was designed and implemented in accordance with the description criteria in DC section 200. Generally, management prepares the description from documentation supporting the system of internal control and system operations, as well from consideration of the policies, processes, and procedures (controls) within the system used to provide the services. Although the description is generally narrative in nature, there is no prescribed format for the description. In addition, flowcharts, matrices, tables, graphics, context diagrams, or a combination thereof, may be used to supplement the narratives contained within the description.

Additionally, the description can be organized in a variety of different ways. 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). Alternatively, it may be organized by components of the system (infrastructure, software, people, data, and processes and procedures) and 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 commitments and system requirements and by disclosures of the design, implementation, and operation of controls to address those risks.

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 or the services provided by the system, particularly if certain aspects of those services are not relevant to the report users or are beyond the scope of the SOC 2® examination. For example, a service organization's processes related to billing for the services provided to user entities are unlikely to be relevant to report users. Similarly, although the description may include procedures within both manual and automated systems by which services are provided, the description need not necessarily disclose every step in the process.

Ordinarily, a description of a service organization's system in a SOC 2® examination is presented in accordance with the description criteria when it does the following:

- Describes the system that the service organization has implemented (that is, placed in operation) to provide the services
- Includes information about each description criterion, to the extent it is relevant to the system being described
- Does not inadvertently or intentionally omit or distort information that is likely to be relevant to report users' decisions

Although the description should 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.

A description that (*a*) states or implies that certain IT components exist when they do not, (*b*) states or implies that certain processes and controls have been implemented when they are not being performed, or (*c*) contains statements that cannot be objectively evaluated (for example, advertising puffery) is not presented in accordance with the description criteria.

When evaluating whether the description is presented in accordance with the description criteria, service organization management should consider the 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. Because the implementation guidance does not address all possible situations, management should consider the specific facts and circumstances of the service organization when evaluating the description against the description criteria.

Determining whether the description of a service organization's system is presented in accordance with the description criteria also involves evaluating whether each control stated in the description has been implemented. Controls have been implemented when they have been placed in operation rather than existing only in the description.

Materiality Considerations When Preparing the Description in Accordance With the Description Criteria

As previously discussed, applying the description criteria requires judgment. One of those judgments involves the informational needs of report users. For most SOC 2® reports, there is a broad range of specified parties. Therefore, the

description is intended to meet the common informational needs of the specified parties and does not ordinarily include information about every aspect of the system that may be considered important to each individual report user. However, an understanding of the perspectives and information needs of the broad range of intended SOC 2® report users is necessary to determine whether the description is presented in accordance with the description criteria and is sufficient to meet their needs. As discussed in chapter 1, "Introduction and Background," users of a SOC 2® report are expected to have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide them, among other matters. (See section titled "Intended Users of the SOC 2® Report" in chapter 1.)

Because the description presents primarily nonfinancial information, materiality considerations are mainly qualitative in nature and center around whether there are misstatements, or omissions, in the information disclosed that could, individually or in the aggregate, reasonably be expected to influence the decisions of intended users of the SOC 2® report.

Examples of qualitative factors ordinarily considered when determining whether the description is presented in accordance with the description criteria include the following:

- Whether the description of the service organization's system includes the significant aspects of system processing
- Whether the description is prepared at a level of detail likely to be meaningful to report users
- Whether each of the relevant description criteria in supplement A, "2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report," has been addressed without using language that omits or distorts the information
- Whether the characteristics of the presentation are appropriate, given that the description criteria allow for variations in presentation

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 and 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. The description includes such information because it is likely to be relevant to report users and, therefore, such information would be considered 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 tape as a control, but it has not identified physical security controls over the tape storage location as a control because management has concluded that the 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 material or 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.

Having a Reasonable Basis for the Assertion

Service organization management is responsible for having a reasonable basis for its assertion about the description and the 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. (The procedures performed by the service auditor during a SOC 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.)

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 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.

If service organization management determines the risks associated with 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 the those users effectively address the identified risks. Such monitoring controls may include a combination of the following:

- Testing controls at the subservice organization by members of the service organization's internal audit function
- Reviewing and reconciling output reports
- Holding periodic discussions with the subservice organization personnel and evaluating subservice organization performance against established service level objectives and agreements
- Making site visits to the subservice organization
- Inspecting a type 2 SOC 2® report on the subservice organization's system

- Monitoring external communications, such as complaints from user entities relevant to the services performed by the subservice organization

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.

Service organization management may document 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.

If management does not have reasonable basis for its assertion, or if sufficient appropriate evidence to support the basis is unlikely to be available, the service auditor is unable to accept or continue the SOC 2® examination.

Providing the Service Auditor With a Written Assertion[24]

The attestation standards require the service auditor to request a written assertion from the responsible party that addresses all the subject matters in the SOC 2® examination. Specifically, the assertion addresses 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. Service organization management may use any language in its written assertion as long as it addresses management's conclusions about the description, the suitability of controls, and, in a type 2 examination, the operating effectiveness of controls.

Management usually attaches the assertion to the description. Segregating the assertion from the description clarifies that the assertion is not part of the description.

If management refuses to provide the service auditor with a written assertion, the attestation standards require the service auditor to withdraw from the engagement when withdrawal is possible under applicable laws and regulations. If law or regulation does not allow the service auditor to withdraw, the service auditor is required to disclaim an opinion.

Modifying Management's Assertion

As previously discussed, management provides the service auditor with a written assertion at the beginning of the SOC 2® examination. However, during the engagement, the service auditor may identify deficiencies or deviations that may cause the service auditor to qualify the opinion. Management's written

[24] If the service organization uses a subservice organization and elects the inclusive method, subservice organization management is also a responsible party. Accordingly, subservice organization management also needs to provide written assertions and representations to the service auditor. 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.

assertion is generally expected to align with the service auditor's report by reflecting the same modifications as in the service auditor's report.

Service organization management is also required to provide the service auditor with written representations at the conclusion of the engagement. (See the section titled "Providing the Service Auditor With Written Representations" that follows.)

Providing the Service Auditor With Written Representations

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.

For those reasons, written representations obtained from service organization management 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.

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 will request the representations from subservice organization management as well.

Appendix B

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 AICPA introduced the term *system and organization controls* (SOC) to refer to the suite of services 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 the 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, *Examination Engagements*, and the 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 the 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, *Common Concepts Applicable to All Attestation Engagements*, because they apply to all attestation engagements. In addition, a practitioner performing a SOC 1® examination is also required to comply with the requirements in AT-C section 205.

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

The following table identifies differences between SOC 1®, SOC 2®, and SOC 3® examinations and related reports:

	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,*[2] contains the criteria for evaluating the description of the service organization's system. Supplement A of this guide presents that criteria. TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*,[3] contains the criteria for evaluating the design and operating effectiveness of the controls. Supplement B of this guide presents that criteria.	TSP section 100 , *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, contains the criteria for evaluating the effectiveness of controls. Supplement B of this guide presents that criteria.
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 were 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' system operated effectively throughout the specified period to achieve those control objectives	**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*
	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	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 *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	
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 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	Interested parties

(continued)

	SOC 1® Examination	*SOC 2® Examination*	*SOC 3® Examination*
		• 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	

Appendix C

Illustrative Comparison of a SOC 2® Examination and Related Report With the Cybersecurity Risk Management Examination and Related Report

This appendix is nonauthoritative and is included for informational purposes only.

The following table compares the SOC 2® examination and related report with a cybersecurity risk management examination and related report. Within the SOC 2® examination and the cybersecurity risk management examination columns, certain text is set in bold to highlight key distinctions between the two types of examinations.

	***SOC 2®* Examination**[1]	***Cybersecurity Risk Management Examination***[2,3]
What is the purpose of the report?	To provide **specified users** (who have sufficient knowledge and understanding of the service organization and its system as discussed later in the table) 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 **general users** with useful information about an entity's cybersecurity risk management program for making informed decisions

(continued)

[1] For illustrative purposes, this table focuses specifically on a type 2 SOC 2® report, which includes both an opinion on the suitability of design and operating effectiveness of controls.

[3] The 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. The AICPA intends to develop a vendor supply chain guide to provide guidance for practitioners engaged to examine and report on system controls at a manufacturer or distributer. The vendor supply chain guide is expected to be issued in 2018.

[3] In a SOC 2® examination, when the entity 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. Those concepts are defined and discussed in this guide.

In the cybersecurity risk management examination, however, 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 service organization. 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.

	SOC 2® **Examination**	***Cybersecurity Risk Management Examination***
Who are the intended users?	Management of the service organization and specified parties **who have sufficient knowledge and understanding of the service organization and its system**	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
Under what professional standards and implementation guidance is the examination performed?	AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*, in AICPA *Professional Standards*	AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*, in AICPA *Professional Standards*
	The AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*	The AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*
Who is the responsible party?	**Service organization** management	Management of an **entity**
Is the report appropriate for general use or 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 regulators who have sufficient knowledge and understanding of the following:**[4]	**Appropriate for general use** [5]

[4] Because the report is only appropriate for users who possess such knowledge and understanding, the SOC 2® report is restricted to the use of such specified users.

[5] The term *general use* refers to 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	*Cybersecurity Risk Management Examination*
	• **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**	

(continued)

	SOC 2® **Examination**	***Cybersecurity Risk Management 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 cybersecurity risk management program** based on the description criteria
	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 based on the applicable trust services criteria relevant to security, availability, processing integrity, confidentiality, or privacy	The effectiveness of controls within the cybersecurity risk management 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*[6]	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*
	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.[7] contains the **criteria for evaluating the design and operating effectiveness of controls (applicable trust services criteria)**.	The trust services criteria for security, availability, and confidentiality included in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Such criteria are suitable for use as **control criteria**.[8]

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

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

[8] 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**	***Cybersecurity Risk Management Examination***
What are the contents of the report?	A description of the **service organization's system** 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 service auditor's[9] 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 **In a type 2 report, a description of the service auditor's tests of controls and the results of those tests**	A description of the **entity's cybersecurity risk management program** A written assertion by 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 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

[9] The practitioner in a SOC 2® examination is referred to as a *service auditor*.

Appendix D

Appendix D-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 and Complementary User Entity Controls)***
Appendix D-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 D-3	***Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation***
Appendix D-4	***Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)***

Appendix D-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 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* (AICPA, *Description Criteria*) (description criteria).[1] The description

[1] The description criteria presented in this document (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,* in a SOC 2® report. 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*, in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide

(continued)

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,* (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

---

(footnote continued)

Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) (2015 description criteria) are codified as DC section 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*.

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2 examination), either the 2018 description criteria or 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

[2] The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

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.***

Illustrative Independent Service Auditor's Type 2 Report

Independent Service Auditor's Report[3]

To: 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* (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* (AICPA, *Trust Services Criteria*).[5]

---

[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.

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.

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 American Institute of Certified Public Accountants. 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 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*]

[*Service auditor's city and state*]

[*Date of the service auditor's report*]

Appendix D-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* (AICPA, *Description Criteria*), (description criteria).[1] The description is

[1] The description criteria presented in this document (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,* in a SOC 2® report. The 2018 description criteria are codified as DC section 200, *2018 Description Criteria*

(continued)

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* (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 for XYZ to achieve XYZ's 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.

(footnote continued)

for a Description of a Service Organization's System in a SOC 2® Report, in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are codified as DC section 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*.

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2 examination), either the 2018 description criteria or 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

[2] The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

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 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* (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* (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[3]

To: 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* (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* (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

[3] The report may also be titled "Report of Independent Service Auditors."

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 American Institute of Certified Public Accountants. 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 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*]

[*Service auditor's city and state*]

[*Date of the service auditor's report*]

Appendix D-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, implements, and operates 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[1]

To: 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* (AICPA, *Description Criteria*), (description criteria)[2] and

---

[1] The report may also be titled "Report of Independent Service Auditors."

[2] The description criteria presented in this document (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,* in a SOC 2® report. 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*, in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are codified as DC section 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*.

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2

(continued)

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* (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 American Institute of Certified Public Accountants.

Attestation standards established by the American Institute of Certified Public Accountants 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

---

(footnote continued)

examination), either the 2018 description criteria or 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

[3] The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

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 suitability 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.

Appendix D-4

Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)

This appendix is nonauthoritative and is included for informational purposes only.

Although this guide specifies the components of a SOC 2® report and the information to be included in each component, it is not specific about the format for SOC 2® reports. Service organizations and service auditors may organize and present the required information in a variety of formats. The format of the illustrative type 2 report presented in this appendix is not meant to be prescriptive but, rather, illustrative. The illustrative report contains all the components of a service auditor's type 2 report; however, for brevity, it does not include everything that might be described in a type 2 report. Ellipses (...) or notes to readers indicate places where detail has been omitted.

The trust services categories being reported on, the controls specified by the service organization, and the tests performed by the service auditor in this appendix are presented for illustrative purposes only. They are not intended to represent the categories that would be addressed in every type 2 engagement or the controls or tests of controls that would be appropriate for all service organizations. The trust services categories being reported on, the controls a service organization would include in its description, and the tests of controls a service auditor would perform for a specific type 2 examination will vary based on the specific facts and circumstances of the engagement.

In the following illustrative type 2 report, XYZ Service Organization has engaged the service auditor to examine and report on the description of the service organization's transportation management system and its controls relevant to security 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 has included information in section 5, "Other Information Provided by XYZ Service Organization That Is Not Covered by the Service Auditor's Report," which is not a part of the description or the service auditor's examination.

Report on XYZ Service Organization's Description of Its Transportation Management System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period January 1, 20X1, to December 31, 20X1

CONTENTS

Section 1—Assertion of XYZ Service Organization Management

Section 2—Independent Service Auditor's Report

Section 3—XYZ Service Organization's Description of Its Transportation Management System

- Services Provided
- Principal Service Commitments and System Requirements
- Components of the System Used to Provide the Services
  - Infrastructure
  - Software
  - People
  - Data
  - Processes and Procedures
- Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring
  - Control Environment
    - Management Philosophy
    - Security Management
    - Security Policies
    - Personnel Security
    - Physical Security and Environmental Controls
    - Change Management
    - System Monitoring
    - Problem Management
    - Data Backup and Recovery
    - System Account Management
  - Risk Assessment Process
  - Information and Communication Systems
  - Monitoring Controls
  - Changes to the System During the Period

Section 4—Trust Services Category, Criteria, Related Controls, and Tests of Controls

- Applicable Trust Services Criteria Relevant to Security

Section 5—Other Information Provided by XYZ Service Organization That Is Not Covered by the Service Auditor's Report

Section 1—Assertion of XYZ Service Organization Management

Illustrative Assertion by Service Organization Management

[*XYZ Service Organization's Letterhead*]

Assertion of XYZ Service Organization Management

We have prepared the accompanying description in section 3 titled "XYZ Service Organization's Description of Its Transportation Management 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* (AICPA, *Description Criteria*), (description criteria).[1] The description is intended to provide report users with information about the transportation management system that may be useful when assessing the risks arising from interactions with XYZ Service Organization's (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 (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).[2]

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. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to

---

[1] The description criteria presented in this document (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,* in a SOC 2® report. 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*, in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are codified as DC section 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*.

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2 examination), either the 2018 description criteria or 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

[2] The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

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.

Section 2—Independent Service Auditor's Report

Independent Service Auditor's Report[3]

To: XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying description in section 3 titled "XYZ Service Organization's Description of its Transportation Management System" throughout the period January 1, 20XX, to December 31, 20XX, (description)[4] 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* (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 (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information included in section 5, "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 the 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, the suitability of the design of controls, and the operating effectiveness of the controls to achieve XYZ's service commitments and system requirements based on the applicable 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. In section 1, XYZ has provided its 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

---

[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.

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 American Institute of Certified Public Accountants. 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 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 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 presented in section 4, "Trust Services Security Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

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. 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.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of XYZ, user entities of XYZ's transportation management 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 transportation management 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*]
[*Service auditor's city and state*]
[*Date of the service auditor's report*]

Section 3—XYZ Service Organization's Description of Its Transportation Management System

Note to Readers: *The following system description is for illustrative purposes only and is not meant to be prescriptive. For brevity, the illustration does not include everything that might be described in the description of the service organization's system. Ellipses (...) or notes to readers indicate places where detail has been omitted from the illustration.*

Services Provided

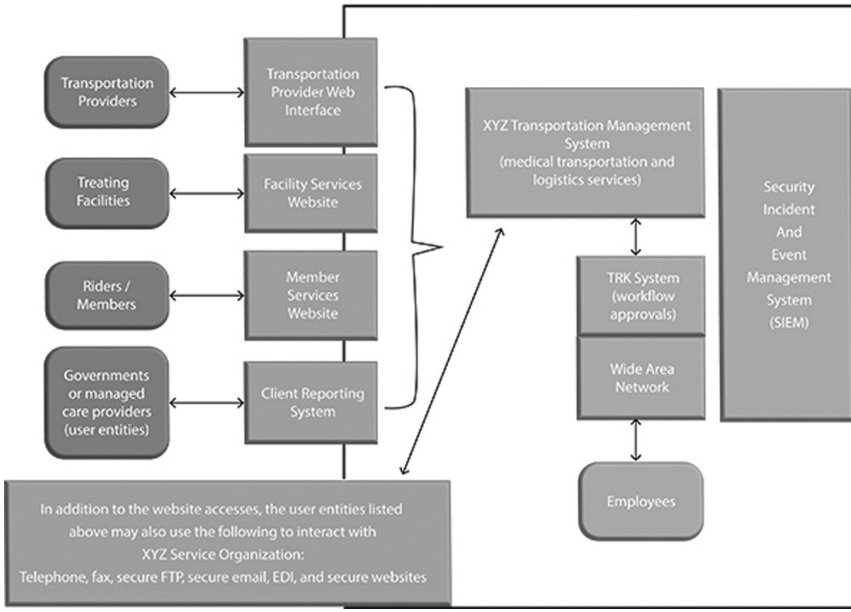
XYZ Service Organization (XYZ) provides medical transportation (MT) services throughout the United States. The Company was founded in 19XX to provide MT services to Medicaid recipients.

XYZ's core application, Transportation Management System (TMS), is a multiuser, transaction-based application suite that enables the processing and delivery of transportation and logistics services. The TMS enables processing of the following tasks related to MT trips:

- Capturing data for transportation providers, governments, and managed care providers (user entities), treating facilities, and riders
- Determining rider eligibility
- Providing gate keeping and ride authorization
- Managing complaints and verifying compliance with transportation agreements
- Managing transportation providers
- Reconciling billing to completed rides
- Providing operational, management, and ad hoc reports
- Providing data reporting in a variety of formats

Trips are tracked through the order cycle, from initial ride assignment to completion or reassignment of the ride, and by payments. Transportation providers send XYZ daily trip information, including information about trips completed or cancelled (or no-shows) and weekly driver logs, which are entered into the TMS. System-generated reports provide supporting documentation for trips, including date, transportation provider, rider, and actual trip via a unique job number.

Information is shared with user entities by telephone, fax, secure electronic exchange (FTP [file transfer protocol], email, EDI [electronic data interchange]), and secured websites.



Principal Service Commitments and System Requirements

XYZ designs its processes and procedures related to TMS to meet its objectives for its MT services. Those objectives are based on the service commitments that XYZ makes to user entities, the laws and regulations that govern the provision of MT services, and the financial, operational, and compliance requirements that XYZ has established for the services. The MT services of XYZ are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which XYZ operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the TMS that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

XYZ establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in XYZ's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and

data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the TMS.

Components of the System Used to Provide the Services

Infrastructure

The TMS runs on Microsoft Windows file servers using a wide area network.

Employees access the application either through their desktop on company-supplied computers or through a Citrix Access Gateway. Data communications between offices are encrypted with Cisco virtual private networking (VPN) technology using Advanced Encryption Standard 256-bit encryption to protect data and intra-company communications.

The TMS uses the IBM DB2 relational database management system. These database servers and file servers are housed in XYZ's secured network operations centers (NOCs).

Software

The TMS is a Microsoft Windows client-server application developed and maintained by XYZ's in-house software engineering group. The software engineering group enhances and maintains the TMS to provide service for the company's transportation providers, governments and managed care providers (user entities), treating facilities, and riders. XYZ's software is not sold on the open market.

The TMS tracks information in real time. The information is immediately stored in the database and is accessible for daily operations, service authorization, trip scheduling, provider reimbursement, agency monitoring, and report generation. The information can be retrieved, reviewed, and reported as needed to create the history of approvals and denials for any rider. Information can be retrieved by rider identification number, rider name, trip date, facility attended, and transportation provider.

External websites are supplied to supplement XYZ's ability to communicate and exchange information with transportation providers, governments and managed care providers (user entities), treating facilities, and riders. Each website targets a specific audience and is designed to address their business needs. These include a site for the transportation providers, governments and managed care providers, treating facilities, and riders.

The XYZ transportation provider web interface is a multiuser, web-based application that helps to manage the flow of information between XYZ and the transportation providers. This website allows transportation providers to enter and retrieve certain information about trips they were assigned by XYZ. It also provides some specific performance reports to help them manage their work with XYZ. To access the site, transportation providers must sign up for the site and fill out certain EDI forms.

The XYZ facility services website supports transportation requests from treating facilities on behalf of their clients. The purpose of the site is to provide a

means to request trips and to manage trip requests online without the need to call an XYZ call center. The facility services website allows a treating facility to enter a single trip or standing order request for review and approval by an XYZ facility representative, look up and view trip requests, modify or update pending requests, and withdraw pending requests.

The XYZ member services website is like the facility services website, except its focus is on the riders. After a rider has successfully logged in, he or she is able to request new trip reservations, view pending requests and processed reservations, edit pending requests, withdraw pending requests, and cancel existing reservations. Requests are placed in a request queue within the TMS database for review by call center personnel through the TMS.

The XYZ client reporting interface is provided as a service to XYZ's government agencies and managed care providers (user entities). This interface allows them to monitor basic statistics of their business and resolve simple questions and complaints. Summary reports of trip volume, complaints, and utilization are available in addition to detailed reports for single trips, single complaints, and rider eligibility.

People

XYZ has a staff of approximately 500 employees organized in the following functional areas:

- *Corporate*. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources, and transportation provider relations. These individuals use the TMS primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for XYZ's user entities.
- *Operations*. Staff that administers the scheduling and administration of transportation providers and riders. They provide the direct day-to-day services, such as transportation reservation intake, trip distribution to transportation providers, quality assurance monitoring, medical facility support, service claims adjudication, transportation network support, and reporting.
    - — Customer service representatives take phone calls directly from riders to arrange transportation. These requests are entered into the TMS and initiate the life cycle of a trip.
    - — Transportation coordinators use the TMS to assign trips to transportation providers. They also manage rerouting and dispensing work from the TMS to the transportation providers on daily trip lists via fax. Transportation managers maintain the transportation provider network database, including updates for training, violations, screenings, and other compliance measures.
    - — Quality assurance (or utilization review) employees use reports generated by the TMS to select samples of trips that are tested for contractual compliance and to

monitor for fraud and abuse. They also take complaints from riders, facilities, and transportation providers and work them to resolution, using tools within the TMS.

- The facility staff manages the facility database for the TMS. They also maintain the transportation standing orders within the system and take single trip requests from facilities only.
- The claims staff receives requests for payment and adjudicates these claims in the software. This includes invoice management, trip verification, and billing support.
- A reports manager typically uses the TMS to produce contract-level specific reports for XYZ's user entities.

- *IT*. Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom.

  - The help desk group provides technical assistance to the TMS users.
  - The infrastructure, networking, and systems administration staff typically has no direct use of the TMS. Rather, it supports XYZ's IT infrastructure, which is used by the software. A systems administrator will deploy the releases of the TMS and other software into the production environment.
  - The software development staff develops and maintains the custom software for XYZ. This includes the TMS, supporting utilities, and the external websites that interact with the TMS. The staff includes software developers, database administration, software quality assurance, and technical writers.
  - The information security staff supports the TMS indirectly by monitoring internal and external security threats and maintaining current antivirus software.
  - The information security staff maintains the inventory of IT assets.
  - IT operations manage the user interfaces for the TMS. This includes processing user entity–supplied membership and eligibility files, producing encounter claims files, and other user-oriented data (capitation files, error reports, remittance advice, and so on).
  - Telecom personnel maintain the voice communications environment, provide user support to XYZ, and resolve communication problems. This group does not directly use the TMS, but it provides infrastructure support as well as disaster recovery assistance.

Data

Data, as defined by XYZ, constitutes the following:

- Master transportation file data
- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Transaction processing is initiated by the receipt of a trip or standing order request. This request typically comes directly from a rider or treating facility by telephone or via the websites, or it may arrive by fax from a treating facility. After the trip is completed, the transportation provider sends XYZ paper documents with daily trip information, including information about completed trips, cancellations or no-shows, and weekly driver logs, all of which is entered into the system's verification module; a portion of this trip completion information may be entered on the XYZ transportation provider web interface.

Output reports are available in electronic PDF, comma-delimited value file exports, or electronically from the various websites. The availability of these reports is limited by job function. Reports delivered externally will only be sent using a secure method—encrypted email, secure FTP, or secure websites—to transportation providers, treating facilities, and governments or managed care providers using XYZ-developed websites or over connections secured by trusted security certificates. XYZ uses Transport Layer Security to encrypt email exchanges with government or managed care providers, facility providers, and transportation providers.

Processes and Procedures

Management has developed and communicated to transportation providers, governments and managed care providers, treating facilities, and riders procedures to restrict logical access to the TMS. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response

- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The security category and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in section 4 of this report. Although the applicable trust services criteria and related controls are included in section 4, they are an integral part of XYZ's description of the TMS.

Control Environment

Management Philosophy

XYZ's control environment reflects the philosophy of senior management concerning the importance of security of medical transportation and logistics data and information. XYZ's Security Steering Committee meets quarterly and reports to the board annually. The committee, under the direction of the XYZ board, oversees the security activities of XYZ. The committee members are from each of the business lines. The committee is charged with establishing overall security policies and procedures for XYZ. The importance of security is emphasized within XYZ through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, XYZ has taken into consideration the relevance of controls to meet the relevant trust criteria.

Security Management

XYZ has a dedicated information security team consisting of a security officer and a senior security specialist responsible for management of information security throughout the organization. They hold positions on the Security Steering Committee and maintain security credentials and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing XYZ's information security policies. The information security policy is reviewed annually by the security officer, CIO, and vice president of operations, and it is approved by the Security Steering Committee.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.

Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

Security Policies

The following security policies and related processes are in place for the TMS:

- Data classification and business impact assessment
- Selection, documentation, and implementation of security controls
- Assessment of security controls
- User access authorization and provisioning
- Removal of user access
- Monitoring of security controls
- Security management

Application TRK is installed to enhance the workflow and approval process in support of the policies. This application enables tracking of

- changes to data classification;
- additions, modifications, or deletions of users;
- changes to authority levels in access approvals;
- tests of new security components prior to installation; and
- reviews of significant security monitoring events.

Personnel Security

Background checks are performed on new information security employees, who are also required to review and acknowledge their receipt of relevant security policies. The new positions are supported by job descriptions. Once employed, employees are subject to XYZ's procedures for accessing systems and sanctions for violating XYZ's information security policy. Employees are instructed to report potential security incidents to the help desk.

XYZ's business associate agreement instructs user entities and transportation providers to notify their respective account representative if they become aware of a possible security breach.

Physical Security and Environmental Controls

The TMS is located in XYZ's NOCs. NOC access is monitored by video surveillance and on-site personnel, and it is controlled through the use of card reader systems. Access to the NOC is limited to authorized personnel based on job function, and physical security access permissions are reviewed quarterly by the security administration team.

XYZ's NOCs employ UPS power systems, air conditioning systems, fire detection and suppression systems, and environmental monitoring and alert notification systems.

Change Management

XYZ has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The IT management team meets weekly to review and schedule changes to the IT environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.

XYZ has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

XYZ uses a standardized server build checklist to help secure its servers, and it conducts monthly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with XYZ's patch management process.

System Monitoring

The security administration team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed daily by the security administration team using a security incident and event monitoring (SIEM) product. Additionally, the security administration team has developed and will review the following SIEM reports:

- Failed object level access
- Daily IDS or IPS attacks
- Critical IDS or IPS alerts
- Devices not reporting in the past 24 hours
- Failed login detail
- Firewall configuration changes
- Windows policy changes
- Windows system shutdowns and restarts
- Security events requiring further investigation are tracked using a help desk ticket and monitored until resolved

Problem Management

Security incidents and other IT-related problems are reported to the help desk. Issues are tracked using a help desk ticket and monitored until resolved.

Data Backup and Recovery

XYZ uses data replication and tapes to back up its data files and software. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized personnel.

System Account Management

XYZ has implemented role-based security to limit and control access within the TMS. Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel. XYZ's transportation providers, governments and managed care providers (user entities), treating facilities, and riders are approved for access by an authorized user. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to

verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

The human resources department provides IT personnel with an employee termination report every two weeks. IT reconciles the termination report with current access privileges to determine if access has been appropriately removed or disabled. Dormant network accounts are disabled after 90 days of inactivity, and dormant TMS accounts are disabled after 45 days of inactivity.

Administrative access to Active Directory, Unix, and TMS servers and databases is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users to the TMS, as well as to the facility services, transportation provider, member services, and client reporting websites. Password parameters consist of the following:

- Passwords contain a minimum of six characters, including one non-alphanumeric character.
- Passwords expire every 120 days for non-privileged accounts and 60 days for privileged accounts.
- Log-on sessions are terminated after three failed log-on attempts.
- Users cannot reuse the last three passwords (five passwords for privileged accounts).

Risk Assessment Process

XYZ regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security based on the applicable trust services criteria set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information security team assesses security risks on an ongoing basis. This is done through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.

An IT strategic plan is developed annually by the CIO and is communicated to and approved by senior management and the Security Steering Committee. As part of this plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed.

Senior management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on XYZ's security policies.

Changes in security threats and risks are reviewed by XYZ, and updates to existing control activities and information security policies are performed as necessary.

Information and Communication Systems

XYZ has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These

include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

XYZ uses checklists to help facilitate the upload of user (rider or member) information, such as encounter data, trip report, and client complaints, to the appropriate repository (for example, a portal or secure FTP folder) in accordance with the user's instructions.

Monitoring Controls

In addition to the daily oversight, monthly vulnerability assessments, and use of SIEM, management provides further security monitoring through the internal audit department, which performs periodic audits to include information security assessments.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how the TMS is used to provide the service during the period from January 1, 20XX, through December 31, 20XX.

Section 4—Trust Services Category, Criteria, Related Controls, and Tests of Controls

Note to Readers: *Although the applicable trust services criteria, related controls, and management responses to deviations, if any, are presented in this section, they are an integral part of XYZ's description of its transportation management system throughout the period January 31, 20X1, to December 31, 20X1. XYZ's controls and test of controls presented in this section are for illustrative purposes and, accordingly, are not all-inclusive and may not be suitable for all service organizations and examinations.*

Applicable Trust Services Criteria Relevant to Security

The trust services criteria relevant to security address the need for information and systems to be 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 service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of

i. *information* during its collection or creation, use, processing, transmission, and storage and

ii. *systems* that use electronic information to process, transmit or transfer, and store information to enable the achievement of XYZ's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
Control Environment			
CC1.1 The entity demonstrates a commitment to integrity and ethical values.	XYZ has documented the code of business conduct and ethical standards which are reviewed, updated if applicable, and approved by the board of directors and senior management annually.	Inspected the code of business conduct and ethical standards of XYZ noting the conduct and standards outlines the service organization's commitments to integrity and ethical values and that the conduct and standards were updated and approved by the board of directors and senior management within the examination period.	No exceptions noted.
	Personnel, including contractors, are required to read and accept the code of business conduct and ethical standards upon their hire and formally reaffirm them annually thereafter. Agreements are established with service providers and business partners (governments or managed care providers and transportation providers) that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	For a selection of new hires including contract hires, inspected the code of business conduct and ethical standards signed and determined that the conduct and the standards were acknowledged by each hire selected. For a selection of current personnel, including contractors, inspected the code of business conduct and ethical standards signed and determined that the conduct and the standards were acknowledged annually by each person selected. For a selection of agreements with the service providers and business partners, inspected the agreements and determined that the agreement outlined XYZ's requirements, including terms, conditions, and responsibilities for the service providers and business partners.	Two of 45 new hires selected, did not sign the conduct and standards acknowledge-ment.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Management monitors personnel compliance with the code of business conduct and ethical standards through monitoring of customer and workforce member complaints and the use of an anonymous third-party administered ethics hotline. XYZ's code of business conduct includes a sanctions policy for personnel who violate the code of business conduct. The sanctions policy is applied to personnel who violate the code of business conduct.	Inspected XYZ's website and test dialed the hotline number provided and determined that an anonymous third-party administered hotline is available. Inspected XYZ's code of business conduct and determined that it included a sanctions policy for personnel who violate the code of business conduct. For a selection of customer and workforce member complaints logged via the third-party administered hotline, inspected the related documentation and determined that personnel who violated the code of business conduct were sanctioned as per the policy.	No exceptions noted.
	Prior to employment, personnel are verified against regulatory screening databases, including at a minimum, credit, criminal, drug, and employment checks.	For a selection of new hires, inspected the background checks and determined that selected personnel successfully completed background checks including, credit, criminal, drug and employment checks prior to being hired by XYZ.	No exceptions noted.
	Before a third party is engaged by XYZ, the third-party personnel undergo background screening. A background check includes, at a minimum, credit, criminal, drug, and employment checks.	For a selection of third-party personnel engaged by XYZ, inspected the background checks and determined that selected third-party personnel successfully completed background checks including, credit, criminal, drug and employment checks prior to being engaged by XYZ.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
CC1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The board of directors are appointed to act on behalf of the shareholders. Roles and responsibilities of the board of directors as outlined in the Board of Directors' Charter are segregated from the roles and responsibilities of management. The board of directors understand and acknowledge the Board of Directors' Charter to accept its oversight responsibilities in relation to established requirements and expectations.	Inspected the Board of Directors' Charter and determined that the board of directors are appointed to act on behalf of the shareholders and the roles and responsibilities are segregated from the roles and responsibilities of management. Inspected the board of directors' acknowledgement of the Board of Directors' Charter to accept its oversight responsibilities in relation to established requirements and expectations.	No exceptions noted.
	The Board of Directors' Charter includes the minimum background and skills required of board of directors. During the annual board meeting, the background and skills of each board member is compared to the background and skills noted in the Board of Directors' Charter.	Inspected the Board of Directors' Charter and determined that the minimum background and skills required of board of directors is documented. For the annual board meeting, inspected the meeting minutes and determined that the background and skills of each board member was compared to the background and skills noted in the Board of Directors' Charter.	No exceptions noted.
	The board of directors consist of majority of independent members as per the Board of Directors' Charter to maintain independence from management.	Inspected the Board of Directors' Charter and determined that it notes the board of directors should consist of majority of independent members. Inspected the board of directors' structure and determined that the board of directors consisted of majority of independent members.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ has a Security Steering Committee governed by the Security Steering Committee Charter that provides support to the board of directors. The Security Steering Committee Charter includes roles and responsibilities relevant to security.	Inspected the Security Steering Committee structure and determined that a Security Steering Committee is in place. Inspected the Security Steering Committee Charter and determined that it included roles and responsibilities relevant to security.	No exceptions noted.
CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	XYZ management and the board of directors evaluate its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revise these when necessary to support the achievement of objectives.	Inspected the annual business planning and risk assessment documentation and determined that organizational structure, reporting lines, authorities, and responsibilities were revised.	No exceptions noted.
	Job descriptions are reviewed by XYZ management on an annual basis for needed changes and where job duty changes are required necessary changes to these job descriptions are also made to enable execution of authorities and responsibilities and flow of information to manage the activities of XYZ.	Inspected the annual business planning and risk assessment documentation and determined that organizational structure, reporting lines, authorities, and responsibilities were revised.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at the various levels of the organization and requirements relevant to security. Personnel are required to sign a copy of their job description to acknowledge their understanding of their responsibilities. Reporting relationships and organizational structures are reviewed periodically by senior management and the board of directors as part of organizational planning and adjusted as needed based on changing commitments and requirements.	Inspected the organizational structure and job descriptions and determined that organizational structure, reporting lines, authorities, and responsibilities were documented taking into consideration segregation of duties as necessary relevant to security. For a selection of personnel hired or transferred to a new role during the period, obtained the file copy of their job description and determined that the employees had acknowledged their understanding of their responsibilities. Inspected the annual business planning and risk assessment documentation and determined that organizational structure, reporting lines, authorities, and responsibilities were revised.	No exceptions noted.
	The security commitments and obligations of transportation providers, governments and managed care providers (user entities), treating facilities, and riders are posted on XYZ's websites and the web interface and included in business associate agreements. Roles and responsibilities for external party interaction and activity monitoring are defined in written job descriptions and communicated to	Inspected XYZ websites, web interface, and the standard business associate agreement and determined that the security commitments and obligations of user entities, treating facilities, and riders are posted on XYZ's websites and the web interface and included in business associate agreements. For a selection of user entities, transportation providers, governments	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	personnel. Personnel are required to sign a copy of their job description to acknowledge their understanding of their responsibilities.	and treating facilities, inspected the signed business associate agreements and compared those to the standard agreements for consistency. For a selection of personnel hired or transferred to a new role with roles that requires interaction with the external parties during the period, obtained the file copy of their job description and determined that the employees had acknowledged their understanding of their responsibilities.	
CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Job requirements are documented in the job descriptions and candidates', whether an employee, contractor, or vendor employee, abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process to support the achievement of objectives. The experience and training of candidates, whether an employee, contractor, or vendor employee, for employment of transfer are evaluated before they assume the responsibilities of their position to support the achievement of objectives. Existing personnel are evaluated at least annually.	For a selection of new hires, whether an employee, contractor, or vendor employee, and transfers, whether an employee, contractor, or vendor employee, who have transferred internally, inspected the personnel file and determined that job requirements were documented in the job descriptions. For a selection of new hires, whether an employee, contractor, or vendor employee, and transfers, whether an employee, contractor, or vendor employee, who have transferred internally, inspected the personnel file and determined that offer letter and management notes were maintained evidencing that the selected personnel were evaluated before they assume the responsibilities of their position.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
		For a selection of personnel, whether an employee, contractor, or vendor employee, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings or decision to terminate the employment.	
	Personnel competence across XYZ and in outsourced service providers is measured against established policies and practices as part of the annual evaluation process or when new outsourced service provider relationships are established to support the achievement of XYZ's service commitments and system requirements. Any shortcomings noted during the evaluation are addressed with action items and reevaluated in the following year's evaluation process or sooner.	For a selection of personnel, whether an employee, contractor, or vendor employee, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings or decision to terminate the employment. For a selection of outsourced service providers, including existing and new providers, inspected the annual service provider risk assessments performed and determined that external service provider performance and risks were assessed, including action items for any shortcomings as well as follow-up on prior year's action items as necessary.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Management establishes requisite skillsets for personnel, whether an employee, contractor, or vendor employee, and provides continued training about its commitments and requirements for personnel to support the achievement of objectives. Management monitors compliance with training requirements.	Obtained the dates of and attendance sheets for the annual security training, as well as the quarterly security compliance updates for employees and determined that employees had signed the attendance sheet for training sessions and updates on the specified dates. For a selection of personnel, obtained the dates of and attendance sheets for role-specific trainings and determined that the employee, contractor, or vendor employee selected had signed the attendance sheet for training sessions and updates on the specified dates. For a selection of personnel not present during the training dates, inspected management's training related documentation and determined that the selected personnel were required to take the training subsequently within the examination period.	No exceptions noted.
	During its ongoing and periodic business planning, business continuity planning and budgeting process, management and the board of directors evaluate the need for additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	Inspected XYZ's annual business planning, business continuity planning and budgeting related documentation and determined that XYZ continually evaluated its need for additional tools and resources as well as contingency plans for assignments of responsibility important for internal control.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Prior to employment, personnel, including contractors and vendor employees, are verified against regulatory screening databases, including at a minimum, credit, criminal, drug, and employment checks. For personnel with responsibility important for internal control, such back ground checks are re-performed every two years.	For a selection of new hires, including contractors and vendor employees, inspected the background checks and determined that selected personnel successfully completed background checks including, credit, criminal, drug and employment checks prior to being hired by XYZ. For a selection of personnel with responsibility important for internal control, inspected the background checks and determined that selected personnel successfully completed background checks including, credit, criminal, drug and employment checks every two years.	No exceptions noted.
CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	XYZ management and the board of directors perform annual performance evaluations to communicate and hold individuals accountable for performance of internal control responsibilities. The performance evaluation is signed by the manager and employee. Corrective actions, including training or sanctions, as necessary. Each XYZ department, such as Software Development, Information Security, Infrastructure, Networking and Systems Administration, IT Operations, Help Desk, Human Resources, Legal, Compliance, Internal Audit, Finance, Customer	For a selection of personnel, whether an employee, contractor, or vendor employee, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings or decision to terminate the employment, and whether evaluations were signed by the manager and the employee. For a selection of weekly department meetings that impacted security criteria, inspected the meeting minutes and determined that department's progress	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Support, IT Operations, hold periodic (weekly) meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of department's responsibilities.	is monitored and measured by respective department heads, including escalation or taking of corrective action as necessary.	
	Management and the board of directors establish measurable goals and performance evaluation criteria, including, incentives, other rewards, and sanctions appropriate for responsibilities at all levels of XYZ, considering the achievement of both short-term and longer-term objectives. Established short-term and longer-term XYZ goals and performance evaluation, reward and sanctions criteria for XYZ executives are reviewed and approved annually by the Compensation Committee.	For a selection of roles, inspected XYZ's documented goals, performance evaluation criteria and compensation matrix including incentives and rewards and determined that a formal process has been implemented for performance measures, incentives and rewards and that the goals documented for selected roles included both short-term and longer-term goals that aligned with XYZ's short-term and longer-term goals. Inspected the annual Total Executive Compensation Package and determined that the Compensation Committee approved the package.	No exceptions noted.
	Management and the board of directors establish measurable goals and performance evaluation criteria, taking into consideration pressures associated with the achievement of objectives. XYZ personnel with internal control responsibility are not rewarded based on number of exceptions noted or lack thereof by the external auditor. Established short-term	For a selection of roles, inspected XYZ's documented goals, performance evaluation criteria and compensation matrix including incentives and rewards and determined that a formal process has been implemented for performance measures, incentives and rewards and that the goals documented for selected roles considers	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	and longer-term XYZ goals and performance evaluation, reward and sanctions criteria for XYZ executives are reviewed and approved annually by the Compensation Committee.	excessive pressures or conflicting goals and evaluation criteria. Inspected the annual Total Executive Compensation Package and determined that the Compensation Committee approved the package.	
	Management and the board of directors evaluate performance of internal control responsibilities, providing rewards and sanctions appropriate for responsibilities, considering the achievement of both short-term and longer-term objectives.	For a selection of personnel, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings and that rewards or disciplines documented were consistent with the goals and performance evaluation criteria established by.	No exceptions noted.
Information and Communication			
CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	XYZ performs assessment at least annually to identify the information required and expected to support the internal control and the achievement of XYZ's service commitments and system requirements. XYZ's most valuable and sensitive digital data and mission-critical systems, "crown jewels" are identified during the assessment, including internal and external sources of data.	Inspected XYZ's annual assessment and determined that it identifies the information required to support internal controls and the achievement of XYZ's service commitments and system requirements, including identification of most valuable data and mission critical systems, i.e., "crown jewels" whether those are internal or external to XYZ.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ performs assessment at least annually to identify key information system processes that process relevant data into information to support the internal control and the achievement of XYZ's service commitments and system requirements.	Inspected XYZ's annual assessment and determined that it identifies the key information system processes that process relevant data into information required to support internal controls and the achievement of XYZ's service commitments and system requirements.	No exceptions noted.
	XYZ has implemented various processes and procedures relevant to security to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. XYZ has logical and physical security, change management, incident monitoring, and data classification, integrity, and retention controls, as necessary, with checks and balances woven into each applicable process to ensure quality of processing.	Inspected XYZ's documented policies and procedures as it relates to security of most valuable data and mission critical systems and determined that those document XYZ's internal controls for producing, timely, current, accurate, complete, accessible, protected, verifiable and retained information, as applicable. [Also refer to controls and service auditor's tests of controls under CC4 through CC9.]	No exceptions noted.
CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system, is provided to personnel to carry out their responsibilities.	Inspected XYZ's intranet and determined that documented policies and procedures as it relates to security of most valuable data and mission critical systems is available to internal personnel on the intranet.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ management and the board of directors meet quarterly and annually to communicate information needed to fulfill their roles with respect to the achievement of XYZ's service commitments and system requirements. XYZ has incident response policies and procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management and the board of directors as necessary.	For a selection of quarters and the year, inspected the quarterly and annual board meeting minutes and determined that those minutes documented discussion of key items with respect to the achievement of XYZ's service commitments and system requirements, including, progress, delays, risks, challenges related to those key items as applicable. Inspected XYZ's documented Incident Response policies and procedures and determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to the Board, as necessary.	No exceptions noted.
	XYZ has anonymous third-party administered whistle-blower hotlines available to internal and external users. Management monitors customer and workforce member complaints reported via the hotlines.	Inspected XYZ's website and test dialed the hotline number provided and determined that an anonymous third-party administered hotline is available. For a selection of customer and workforce member complaints logged via the third-party administered hotline, inspected the related documentation and determined that personnel who violated the code of business conduct were sanctioned as per the policy.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ holds quarterly and annual Board meetings. In addition, for communication of an unforeseen event, incident response policies and procedures are in place that includes escalation plan based on the nature and severity of the incident to senior management and the board of directors as necessary.	For a selection of quarters and the year, inspected the quarterly and annual board meeting minutes and determined that those documented discussion of key items with respect to the achievement of XYZ's service commitments and system requirements, including, progress, delays, risks, challenges related to those key items as applicable. Inspected XYZ's documented incident response policies and procedures and determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to the Board, as necessary.	No exceptions noted.
	XYZ's security commitments are communicated to external users (governments or managed care providers and transportation providers), as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities. The responsibilities of internal users whose roles affect system operation are communicated to those parties. Responsibilities and policies and procedures posted on XYZ's intranet are updated as necessary.	Inspected XYZ's intranet, customer portal, and websites and determined that documented responsibilities, policies and procedures as they relate to security commitments and responsibilities are available to internal personnel on the intranet and external personnel on XYZ's websites and customer portals as applicable. For a selection of responsibilities, policies and procedures posted on the intranet, inspected the documents and determined that history of changes with the date of change was documented.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Internal and external users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected XYZ's documented incident response policies and procedures and determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to the Board, as necessary.	No exceptions noted.
	Changes to XYZ's commitments and system requirements are communicated to internal and external users, vendors, and other third parties (governments or managed care providers and transportation providers) whose services are part of the system.	Inspected XYZ's intranet, customer portal, and websites and determined that documented responsibilities, policies and procedures as it relates to security commitments and responsibilities are available to internal personnel on the intranet and external personnel on XYZ's websites and customer portals as applicable, and that those responsibilities, policies and procedures documented history of changes with the date of change. For a selection of agreements with the service providers and business partners, inspected the agreements and determined that the agreement outlined XYZ's requirements, including terms, conditions, and responsibilities for the service providers and business partners and that signed addendum to agreements were also maintained when changes to commitments and requirements occurred, as necessary.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Management provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Management monitors compliance with security training requirements. XYZ also provides user guides, security alerts and known issues on its websites and customer portal with information to improve security knowledge and awareness.	Obtained the dates of and attendance sheets for the annual security training, as well as the quarterly security compliance updates for employees and determined that employees had signed the attendance sheet for training sessions and updates on the specified dates. For a selection of personnel not present during the training dates, inspected management's training related documentation and determined that the selected personnel were required to take the training subsequently within the examination period. Inspected XYZ's customer portal and websites and determined that user guides and history of security alerts and known issues with information to improve security knowledge and awareness was available.	No exceptions noted.
	XYZ posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, and data on its intranet for internal users and on the internet for external users.	Inspected XYZ's intranet and internet descriptions of XYZ's system, system boundaries, and system processes and determined that the description addressed infrastructure, software, people, processes and procedures, and data for the in-scope technology and locations.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Agreements are established with service providers and business partners (governments or managed care providers and transportation providers) that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	For a selection of agreements with the service providers and business partners, inspected the agreements and determined that the agreement outlined XYZ's requirements, including terms, conditions, and responsibilities for the service providers and business partners.	No exceptions noted.
	Planned changes to system components are reviewed, scheduled, and communicated to management as part of the weekly IT maintenance process. Planned changes to system components are communicated to external users (governments, managed care providers, and transportation providers) via the XYZ's website.	For a selection of weeks, inspected weekly IT maintenance schedules and communications and determined that planned system changes were included and had been reviewed and signed off by IT management. Inspected XYZ's customer portal and determined that it published a calendar of upcoming system changes existed and that it communicated upcoming changes and their impact on users, if any.	No exceptions noted.
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	XYZ has incident response policies and procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management, the board of directors and external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties as necessary.	Inspected XYZ's documented incident response policies and procedures and determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to senior management, the board of directors and external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties as necessary.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ has made available contact email and phone numbers on its website and customer portal to customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, including anonymous third-party administered whistle-blower hotlines. Management monitors customer and workforce member complaints reported via the hotlines, emails and phones.	Inspected XYZ's customer portal and websites and determined that contact email and phone numbers are available to customers and external users on the customer portal and websites. Inspected XYZ's website and test dialed the hotline number provided and determined that an anonymous third-party administered hotline is available. For a selection of customer and workforce member complaints logged via the third-party administered hotline, inspected the related documentation and determined that personnel who violated the code of business conduct were sanctioned as per the policy.	No exceptions noted.
	The Legal, Compliance, and Internal Audit departments meets with the board of directors quarterly to provide relevant information resulting from assessments conducted by internal and external parties. In addition, any significant information security related findings noted as part of XYZ's financial audits are communicated by the external auditor to the Audit Committee during quarterly and annual meetings.	For a selection of quarters and the year, inspected the quarterly and annual board meeting minutes and determined that the Legal, Compliance and Internal Audit departments presents an executive summary of all external and internal audit findings for the quarter including copies of the audit reports to the Board, and that significant information security related findings noted by the external auditors were also communicated by the external auditor to the Audit Committee.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, and data on its intranet for internal users and on the internet for external users.	Inspected XYZ's intranet and internet descriptions of XYZ's system, system boundaries, and system processes and determined that the description addressed infrastructure, software, people, processes and procedures, and data for the in-scope technology and locations.	No exceptions noted.
	XYZ's security commitments are communicated to external users, as appropriate. Agreements are established with service providers and business partners (governments or managed care providers and transportation providers) that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	Inspected XYZ's customer portal and websites and determined that documented responsibilities as it relates to security commitments and responsibilities are available to external personnel. For a selection of agreements with the service providers and business partners, inspected the agreements and determined that the agreement outlined XYZ's requirements, including terms, conditions, and responsibilities for the service providers and business partners.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
Risk Assessment			
CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	XYZ management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the board of directors. The objectives incorporate the service commitments and system requirements of the MT services and TMS. Assessed risks are reviewed quarterly to identify changes in underlying threats or in the environment that would require an update to assessed risks.	Inspected the annual risk assessment documentation to determine whether the risk assessment process included consideration of the MT service commitments and TMS system requirements. Inspected documentation for two of the three quarterly reviews of the risk assessment to determine whether the reviews included evaluation of identified changes in laws and regulations and changes to contractual commitments.	No exceptions noted.
	XYZ subscribes to an external reporting service that identifies changes to laws and regulations relating to MT services for the jurisdictions in which it operates. Reported changes are evaluated by personnel within the General Counsel's Office for their impact and the evaluations are communicated to senior management and are incorporated into the risk assessment and review process.	Obtained the monthly reports of changes in laws and regulations received from the external reporting service. For a sample of changes reported, obtained the evaluation of the changes by General Counsel Office personnel and the communication of the evaluation to senior management to determine whether the changes assessed for their impact on the TMS system. Inspected documentation of the use of the evaluation in the subsequent annual risk assessment and quarterly risk assessment reviews.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Contracts personnel within the General Counsel's Office maintain a database of contract terms and commitments. Updates of or modifications to standard contractual terms and commitments are approved by the Chief Operating Officer prior to contract approval. Updates and modifications to contractual terms and commitments are incorporated into the risk assessment and review process.	For a sample of updates to standard contract terms and new contracts with terms that differed from the standard contractual terms, inspected the entry in the contract terms and commitments databased to determine whether the changes were recorded completely and accurately. For a sample of changes to the contract terms and commitments database, inspected documentation of the Chief Operating Officer's approval of the change prior to contract execution. For a sample of changes to the contract terms and commitments database, Inspected documentation of the consideration of the change in the subsequent annual risk assessment and quarterly risk assessment reviews.	No exceptions noted.
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.	Monthly, XYZ's Security Steering Committee meets to discuss strategy and operations, financial results, risk considerations, and other factors critical to the business.	Inspected a sample of minutes from monthly Security Steering Committee meetings to determine whether organizational strategy and operations, financial results and risk considerations critical to the business were discussed.	No exceptions noted.
	A quarterly risk assessment is performed to identify risks arising from external and internal sources and the effectiveness of these controls are shared with executive management and the audit committee.	Inspected the annual risk assessment to determine whether risks arising from external and internal sources and effectiveness of controls to mitigate those risks were identified and communicated.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	An overview of the annual risk assessment is presented to the audit committee as well as used to help establish the annual audit plan.	Inspected a sample of minutes and meeting agendas from the audit committee meetings to determine whether an overview of the risk assessment was communicated.	No exceptions noted.
	The information security team assess and responds to security risks on an ongoing basis through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.	Inspected a sample of minutes and meeting agendas from monthly information security team meetings to determine whether security risks and vulnerabilities were identified, assessed, and analyzed by management.	No exceptions noted.
	XYZ has a defined information classification scheme for the labeling and handling of data. XYZ classifies data into four levels: public, internal use, confidential, and protected.	Inspected the data classification policy to determine whether there is a documented classification scheme for labeling and handling data. For a sample of data files and databases, obtain the relevant data dictionary and compared the data classification per the contents of the data dictionary, the data classification scheme, and the data classification of the file/database.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services.	Inspected the annual risk assessment and a sample of completed vendor questionnaires during the calendar year to determine whether an organizational assessment of risk was performed prior to the acquisition or outsourcing of dedicated information security services.	No exceptions noted.
	A company-wide risk assessment is performed annually by management and includes the following: *a.* Determining business objectives, entity, subsidiary, division, operating unit, and functional levels. *b.* Evaluating the effect of environmental, regulatory, and technological changes on XYZ's system security *c.* Involving appropriate levels of management. *d.* Analyzing risks associated with the threats *e.* Identifying threats to operations, including security threats, using information technology asset records *f.* Identifying threats to operations, including threats from vendors, business partners, and other parties. *g.* Determining a risk mitigation strategy	Inspected the annual risk assessment documentation to determine whether they included the significant aspects of operations.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
CC3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management conducts a periodic fraud risk assessment to identify the various ways that fraud and misconduct can occur, including how management might engage in inappropriate actions, and maintains documentation of this assessment.	Inspected the fraud risk assessment documentation to determine whether management periodically evaluated and assessed the various ways fraud and misconduct can occur and that documentation of the assessment was maintained.	No exceptions noted.
	The board, audit committee and management review the XYZ's compensation and performance evaluation programs annually to identify potential incentives and pressures for employees to commit fraud.	Inspected the fraud risk assessment documentation to determine whether compensation and performance evaluation programs were reviewed annually by the board, audit committee and management.	No exceptions noted.
	XYZ has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	Inspected the fraud risk assessment documentation and internal audit plan to determine whether measures were established to protect against unauthorized and unwell acquisition, use or disposal of assets.	No exceptions noted.
	Management uses information technology tools including security systems, fraud detection and monitoring systems, and incident tracking systems to identify and manage fraud risk.	Inspected the fraud risk assessment documentation to determine whether management considered threats and vulnerabilities from the use of IT and access to information.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
CC3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.	XYZ, through its ongoing an annual risk assessment process, evaluates changes in: *a.* the regulatory, economic, and physical environment in which XYZ operates. *b.* the business environment, including industry, competitors, regulatory environment, and consumers. *c.* the potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. *d.* the management and respective attitudes and philosophies on the system of internal control. *e.* XYZ's systems and changes in the technology environment. *f.* vendor and business partner relationships.	Inspected the annual risk assessment documentation to determine that management identified the need for new controls to address risks that were not adequately addressed by existing controls. Inspected a sample of system change requests to determine that management followed the change management process for new controls identified.	No exceptions noted.
Monitoring Activities			
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.	The internal audit department performs periodic audits to include information security assessments.	Inspected the internal audit plan for the calendar year and noted it included information security assessments.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Internal audit annual plans include a risk analysis of all significant operating and reporting areas of XYZ as a means to prioritize audit efforts for the year.	Inspected the internal audit plan and risk analysis documentation and noted that the significant operating and reporting areas of XYZ were assessed to prioritize audit efforts for the year.	No exceptions noted.
	XYZ developed, documented, and maintained a baseline configuration of the internal control system.	Inspected the baseline configuration documentation and noted that the design and current state of the internal control system was used to establish a baseline for ongoing and separate evaluations.	No exceptions noted.
	XYZ provides training, as well as annual performance reviews, for internal audit personnel.	Obtained the dates of and attendance sheets for the annual training, as well as the annual performance reviews for internal audit personnel. Determined whether employees had signed the attendance sheet for training sessions and updates on the specified dates.	No exceptions noted.
	On a quarterly basis, internal audit performs an assessment of the audit plan and scope to identify potential changes impacting XYZ's risk profile.	Inspected the quarterly internal audit plan assessment and noted that the internal audit plan and scope was assessed to identify potential changes impacting XYZ's risk profile.	No exceptions noted.
	An internal audit department exists that is independent of management.	Inspected the organizational chart of XYZ noting the organizational chart described functional areas and reporting structures within functional areas and that reporting hierarchies were defined and appropriately segregated.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Internal audit personnel perform audit procedures using a formal methodology, document their procedures and results in working papers, and prepare an audit report summarizing the procedures performed and the findings from those procedures.	Inspected internal audit methodology and ascertained that the methodology, including requirements for planning, execution, and reporting, and based on standards established by a professional organization. For an XYZ internal audit, inspected documentation and ascertained that the documentation complied with the defined methodology.	No exceptions noted.
	Internal audit developed audit programs that include a mix of manual and automated controls, as well as preventive and detective controls, to mitigate risks identified during the risk assessment process.	Inspected a sample of audit programs during the calendar year to determine whether control activities to mitigate identified risks included a mix of manual, automated, detective and preventive controls.	No exceptions noted.
	Internal audit developed audit programs that include various levels of management.	Inspected a sample of audit programs during the calendar year to determine whether control activities applied various levels of management.	No exceptions noted.
	The XYZ's Security Steering Committee reviews reports from regulators or other third parties to determine whether they indicate possible deficiencies in internal control.	Inspected a sample of minutes from quarterly Security Steering Committee meetings to determine whether regulatory or other third-party reports were reviewed for possible internal control deficiencies.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
CC4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Complete reports of deficiencies in internal control from internal and external sources are provided to the board and audit committee. The board and audit committee work with management to suggest appropriate remediation and follow up to ensure that proper controls have been established.	Inspected minutes from the annual board meeting and audit reports to determine whether deficiencies in internal control and external sources were reported to the board and audit committee.	No exceptions noted.
	XYZ has established a practice that requires all deficiencies rated as serious threats to be reported to senior management and to the board or audit committee.	Inspected minutes from the annual board meeting to determine whether the audit committed reported deficiencies rated as serious threats were reported to the board.	No exceptions noted.
	The board and/or audit committee track the status of all deficiencies that have been rated as a serious threat to the organization until satisfactorily resolved.	Inspected the deficiency tracking matrix to determine whether deficiencies rated as serious threats to the organization were tracked to resolution by the board and/or audit committee.	No exceptions noted.
Control Activities			
CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	Obtained and inspected the annual risk assessment documentation to determine that new controls were implemented for any risks not adequately addressed by existing controls. Inspected a sample of system change requests to determine that the change management process was followed.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	As part of the risk assessment, management assessed the environment, complexity, nature and scope of its operations when developing control activities to mitigate the risks.	Obtained and inspected the risk assessment documentation to determine whether management assessed the environment, complexity, nature and scope of its operations when developing control activities to mitigate the risks	No exceptions noted.
	When management identifies the need for new controls, management considers a mix of control activities, included both manual and automated controls and preventive and detective controls.	Obtained and inspected the risk assessment documentation to determine whether management considered a mix of control activities to mitigate the identified risks.	No exceptions noted.
	XYZ has designed application-enforced segregation of duties to define what privileges are assigned to users within applications.	Inspected the access control policy to determine whether application controls were designed to enforce segregation of duties to users within applications.	No exceptions noted.
CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.	As part of the IT strategic plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed.	Inspected the annual IT strategic plan documentation to determine whether IT risk affecting the organization and recommended courses of action were identified and discussed.	No exceptions noted.
	Management developed a list of control activities to manage the technology infrastructure risks identified during the annual risk assessment process.	Inspected the risk assessment, internal audit plan and audit program for the calendar year to determine whether management developed and implemented control activities over the technology infrastructure.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Management developed a list of control activities to manage the security access management risks identified during the annual risk assessment process.	Inspected the risk assessment, internal audit plan and audit program for the calendar year to determine whether management developed and implemented control activities designed to restrict technology access rights to authorized users commensurate with their job responsibilities and protect corporate assets from external threats.	No exceptions noted.
	XYZ employs organization-defined tailored acquisition strategies and procurement methods for the purchase, development, and maintenance of information systems, system components, or information system services from technology suppliers.	Inspected the procurement policy manual to determine whether management employed acquisition strategies and procurement methods for the purchase, development, and maintenance of information systems, system components, or information system services from technology suppliers.	No exceptions noted.
CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	XYZ's policy and procedure manuals address controls over significant aspects of operations. Policy sections include *a.* security requirements for authorized users; *b.* data classification and associated protection, access rights, retention, and destruction requirements; *c.* risk assessment; *d.* access protection requirements; *e.* user provisioning and deprovisioning; *f.* responsibility and accountability for security;	Inspected the policy and procedure manuals to determine whether they included section headings that addressed controls over the significant aspects of system operations.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	g. responsibility and accountability for system changes and maintenance; *h.* change management; *i.* complaint intake and resolution; *j.* security and other incidents identification, response and mitigation; *k.* security training; *l.* handling of exceptions and situations not specifically addressed in policies; *m.* commitment and requirement identification and compliance measurement; and *n.* information sharing and disclosure.		
	The XYZ's Security Steering Committee is charged with establishing, maintaining, and enforcing the overall security policies and procedures.	Inspected a sample of minutes from quarterly Security Steering Committee meetings to determine whether the committee was charged with establishing, maintaining, and enforcing the overall security policies and procedures.	No exceptions noted.
	Monthly service level assessments are performed by the functional heads of each department. These assessments include evaluation of the operation of key controls.	Inspected a sample of minutes from monthly departmental and management committee meetings to determine whether the evaluation of the operation of key controls were performed by department heads.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Assessments are reviewed at monthly departmental meetings and require the development of corrective action plans for control weaknesses.	Inspected a sample of minutes from monthly departmental and management committee meetings to determine whether the corrective action plans for control weaknesses were reviewed by department heads and the management committee.	No exceptions noted.
	XYZ has written job descriptions specifying the responsibilities and the academic and professional requirements for key job positions. Human resources personnel screen internal and external job applicant qualifications based on the defined requirements within the job description. Transcripts are obtained to evidence educational attainment, and job references are checked to validate experience.	For a sample of positions, inspected written job descriptions to determine whether the job descriptions included responsibilities and academic and professional requirements. For a sample of employees, inquired of the employees about their understanding of their job responsibilities, academic qualifications, and professional certifications and compared their responses for consistency to the documented responsibilities, and academic and professional requirements documented in the job description applicable to their position. For a sample of new employees and employees who have transferred internally, inspected the personnel file to determine whether transcripts were obtained, and job references were checked.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ's policy and procedure manuals are reviewed annually by the CIO, Vice President of Operations, and the Security Officer for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.	Inspected the policy and procedure manuals to ascertain whether policies and procedures had been updated for changes in the risk mitigation strategy. Inspected documentation of the annual review of the policy and procedures manuals by the CIO, Vice President of Operations, and the Security Officer.	No exceptions noted.
Logical and Physical Access			
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 service organization monitors all system components through an automated management interface to log, track, and maintain all inventory components.	Inspected the automated inventory management tool to determine that the tool is in place to monitor the system components. Inspected information system inventory records from the inventory management tool to determine that the tool was providing necessary information to manage assets.	No exceptions noted.
	XYZ permits remote access to production systems by authorized employees only with multi-factor authentication (MFA) over encrypted virtual private network (VPN) connection.	Observed a remote login session to determine that MFA VPN was required to access the production network.	No exceptions noted.
	In-scope system components require unique username and passwords (or authorized SSH keys) prior to authenticating users.	Inspected login attempts to determine that the in-scope system components required authentication measures for users.	No exceptions noted.
	End user and server workload network traffic is segmented to support isolation.	Inspected the network diagram and configurations to determine that customer environments and data are segmented.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected access review documentation for sample of quarters to determine that an access review was performed for in-scope system components and that tickets were created to remove inappropriate access.	No exceptions noted.
	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. SSL certificates are used at the entry-point firewalls to information assets to establish access control rules.	Inspected the data classification policy to determine that procedures existed around classifying and protecting confidential information. Inspected the SSL certificates for verification, issuance, signature algorithm, and validity date.	No exceptions noted.
	Passwords for in-scope system components are configured according to the XYZ's policy, which (*a*) requires eight-character minimum and 90-day password changes; (*b*) is complexity enabled; and (*c*) locks users out of the system after five invalid attempts.	Inspected in-scope system components to determine that passwords were configured according to company policy.	No exceptions noted.
	The configuration management policy requires that all system changes undergo formal documentation, review, and authorization.	Inspected the configuration management policy to determine that all changes to the system are to be configuration controlled, approved, and a risk analysis is performed.	No exceptions noted.
	Databases housing sensitive customer data are encrypted at rest.	Inspected database configurations to determine that databases were encrypted at rest.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Encryption keys used by integrated services are encrypted themselves with a unique master key.	Inspected the configuration for the encryption process to determine that encryption activities use an acceptable cryptographic algorithm.	No exceptions noted.
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.	Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.	Inspected access requests forms for a sample of new hires that received access to the in-scope system components to determine that an access provisioning request was approved prior to access being provisioned.	No exceptions noted.
	A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active user listing to determine that terminated employees did not retain access to the in-scope system and platforms after their separation. Inspected termination tickets for a sample of terminated employees during the review period to determine that access was revoked within 24 hours as a part of the termination process.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected access review documentation for sample of quarters to determine that an access review was performed for in-scope system components and that tickets were created to remove inappropriate access.	No exceptions noted.
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Asset owners periodically review access to ensure continued appropriateness.	Interviewed asset owners and inspected documentation to determine that appropriate procedures are in place to remove or modify application access as needed.	No exceptions noted.
	A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active user listing to determine that terminated employees did not retain access to the in-scope system and platforms after their separation. Termination tickets for a sample of terminated employees during the review period to determine that access was revoked within 24 hours as a part of the termination process.	No exceptions noted.
	XYZ establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles.	Inspected the access control policy to determine that the role-based access scheme was employed to organize information system and network privileges into roles.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ tracks and monitors privileged role assignments on a continuous basis through automated mechanisms.	Tested a sample of the automated mechanisms and their configuration settings, alerts, and reports to determine that the mechanisms are operating as intended.	No exceptions noted.
CC6.4 The entity restricts physical access to facilities and protected information assets (for XYZ, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Access to the data centers requires a documented access request form and manager approval prior to access being provisioned.	Inspected access requests forms for a sample of new hires that received access to the data centers to determine that an access provisioning request was approved prior to access being provisioned.	No exceptions noted.
	A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active user listing to determine that terminated employees did not retain access to the data centers after their separation. Termination tickets for a sample of terminated employees during the review period to determine that access was revoked within 24 hours as a part of the termination process.	No exceptions noted.
	Access to the data centers is reviewed quarterly by management.	Inspected a sample of physical access reviews completed by management to determine that physical access to the data centers was reviewed on a quarterly basis.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
CC6.5 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.	Formal data retention and disposal procedures are in place to guide the secure disposal of the company's and customers' data.	Inspected data retention and disposal procedures to determine that they were in place.	No exceptions noted.
	Prior to removal from company facilities, all digital media is completely degaussed and sanitized to remove any data and software.	Examined media sanitization records for an agreed-upon sample of digital information system media to be sanitized to determine that measures are being applied to sanitize digital media prior to disposal.	No exceptions noted.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined.	Inspected the firewall configurations and rulesets employed within the environment to determine that the permit rules aligned with the specified networking protocols permitted for inbound network traffic.	No exceptions noted.
	The company has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information over public networks.	Inspected TLS settings to determine that transmission of confidential and/or sensitive information over public networks was encrypted.	No exceptions noted.
	XYZ permits remote access to production systems by authorized employees only with multi-factor authentication (MFA) over encrypted virtual private network (VPN) connection.	Observed a remote login session to determine that MFA VPN was required to access the production network.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Intrusion detection systems are used to provide continuous monitoring of the XYZ's network and prevention of potential security breaches.	Inspected intrusion detection system configurations to determine that continuous monitoring of the XYZ's network and early prevention of potential security breaches were in place.	No exceptions noted.
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The information system restricts the ability of users to transmit, move, or remove system information to other information systems or networks.	Inspected the system and communications protection policy and procedures and associated system configuration settings to determine that the information system restricts the ability of users to transmit, move, or remove system information.	No exceptions noted.
	Secure file transfer protocols (SFTP) are deployed for transmission of confidential and/or sensitive information over public networks.	Inspected SFTP configurations to determine that SFTP was used for the transmission of confidential and/or sensitive information over public networks.	No exceptions noted.
	Removable media to be used for customer or system data is encrypted and sanitized prior to connecting such devices to the information system.	Inspected the information system media protection policy and procedures and media sanitization records to determine that removable media is encrypted and sanitized prior to use.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Mobile device access to production systems is permitted by authorized devices only with multi-factor authentication (MFA) over encrypted virtual private network (VPN) connection.	Observed a remote login session to determine that MFA VPN was required to access the production network. Inspected the MFA VPN configurations to determine whether user identification numbers, names, and passwords are required. Observed an employee attempt to access the system through the VPN software and ascertained that user identification numbers, names, and passwords are required to gain access.	No exceptions noted.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Only authorized system administrators are able to install software on system devices. Unauthorized use or installation of software is explicitly covered in the employee handbook and Rules of Behavior.	Inspected the rules of behavior and the employee handbook and verified that the policies prohibit installation of software by users, and installation is limited to system administrators.	No exceptions noted.
	The security center monitoring system logs and alerts system administrators of software installation or attempted software installation.	Inspected documentation describing the current configuration settings for a sample of the automated mechanisms to determine that these mechanisms are configured as required. Tested the automated mechanisms and their configuration settings by creating a simulated unauthorized installation to determine that these mechanisms are operating as intended.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements.	Inspected the change management procedures to determine that procedures were in place to govern the modification and maintenance of production systems and addressed security and availability requirements.	No exceptions noted.
	Anti-malware technology is deployed for environments commonly susceptible to malicious attack. This software is used to scan assets prior to being placed into production.	Inspected screenshots of anti-malware software configurations (virus definition update, scan schedule, notifications, and evidence that software is deployed on all servers) to determine that anti-virus was updated routinely, logged, and installed on all production servers.	No exceptions noted.
	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests.	Inspected installed software inventory for use of logging and monitoring software. For a sample of logging and monitoring software from the inventory, obtained the operations log for a sample date from each sample item selected to determine whether the monitoring software was operational.	No exceptions noted.
System Operations			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Baseline configurations are retained within the configuration manager tool for roll back capability anytime an approved configuration change is made. Baseline configurations are reviewed and updated annually, when required due to reviews and system changes, and anytime integral system components are added.	Inspected the configuration manager tool to determine that baseline configurations are retained and up to date for applicable system changes.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	Inspected IT infrastructure monitoring tool configurations and an XYZ notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
	XYZ utilizes a configuration monitoring tool that notifies management of changes to production system.	Inspected alert configurations settings and an XYZ alert to determine that a configuration monitoring tool monitored and alerted management of changes to production.	No exceptions noted.
	Automated mechanisms are used to continuously detect the addition of unauthorized components/devices into the system. The configuration monitoring tool logs all changes in status to network switch ports. Any attempt to insert or install a component immediately sends an alert to the monitoring tool and creates a ticket.	Inspected configuration settings for the monitoring tool and an XYZ alert to determine that a configuration monitoring tool monitored and alerted management of any unauthorized components.	No exceptions noted.
	Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected internal and external vulnerability scans for a sample of quarters to determine that internal and external vulnerability scans were performed quarterly and remediation plans were developed to remediate all critical and high vulnerabilities.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	User entities are provided with instructions for communicating potential security breaches to the information security team.	Inspected the instructions provided to user entities to determine whether they include protocols for communicating potential security breaches.	No exceptions noted.
	When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.	Inspected the written incident management procedures to determine whether the procedures include a process for handling the security incident.	No exceptions noted.
	Security incidents are reported to the help desk and tracked through to resolution. Incidents that may affect security compliance are reported to the security compliance officer.	Selected a sample of security incidents logged in the incident tracking system and inspected documentation to determine whether the incident was tracked within a help desk ticket until resolution. Inspected a sample of security incidents logged in the incident tracking system and associated communications to the security officer that may affect security compliance to determine whether the incidents were reported to the security officer.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Intrusion detection systems are used to provide continuous monitoring of the XYZ's network and prevention of potential security breaches.	Inspected intrusion detection system configurations to determine that continuous monitoring of the XYZ's network and early prevention of potential security breaches were in place.	No exceptions noted.
	All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.	Inspected the most recent risk assessment to determine that threats and changes were formally identified and assessed on an annual basis.	No exceptions noted.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	XYZ has developed security incident response policies and procedures that are communicated to authorized users. A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.	Inspected incident response policies and procedures to determine that an incident response plan was documented and communicated to authorized users. Inspected the most recent risk assessment to determine that threats and changes were formally identified and assessed on an annual basis.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	A technician or administrator responsible for security incident tickets follows a process of analyzing the security incident. The process begins with detailing what specific attack occurred, which system(s) were affected and what happened during the attack. Next the root cause is determined and the event is given a classification to assign the level of impact of the event. The impact level is based on guidelines detailed in the procedures.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Management has established defined roles and responsibilities to oversee implementation of information security policies including incident response.	Inspected security policies to determine the company has established defined roles and responsibilities to oversee implementation of the incident response plan.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	The containment phase ensures that all other interconnections to the system were not affected by the security incident.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	An assessment of the incident response to better handle future incidents is performed through analysis after-action reports or the mitigation of exploited vulnerabilities to prevent similar incidents in the future.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	Daily incremental and weekly full backups are configured for the databases.	Observed backup configuration to determine that daily incremental and weekly full backups were configured for the databases.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected internal and external vulnerability scans for a sample of quarters to determine that internal and external vulnerability scans were performed quarterly and remediation plans were developed to remediate all critical and high vulnerabilities.	No exceptions noted.
	A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.	Inspected the most recent risk assessment to determine that threats and changes were formally identified and assessed on an annual basis.	No exceptions noted.
	XYZ incorporates lessons learned from ongoing incident response activities into incident response procedures accordingly. If changes are required, necessary changes are made to the policy and procedures and redistributed according to all responsible organizations and key personnel.	Inspected the incident response plan to determine that the document has been reviewed and revised every year and changes were incorporated from prior incidents and associated lessons learned.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	Software updates related to flaw remediation are tested for effectiveness and potential side effects on the system before installation. All software updates and patches are tested by creating a virtual instance of the environment and running the tests associated with the software update and/or patch. An ability to rollback is implemented during software updates and/or patching.	Inspected the configuration management policy to determine that all changes including patches/updates are configuration controlled through virtual instance testing and rollback capability. Inspected a sample of patch updates to determine that patches were tested in accordance with the configuration management policy prior to being placed into production.	No exceptions noted.
	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	A technician or administrator responsible for security incident tickets follows a process of analyzing the security incident. The process begins with detailing what specific attack occurred, which system(s) were affected and what happened during the attack. Next the root cause is determined and the event is given a classification to assign the level of impact of the event. The impact level is based on guidelines detailed in the procedures.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	An assessment of the incident response to better handle future incidents is performed through analysis after-action reports or the mitigation of exploited vulnerabilities to prevent similar incidents in the future.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	XYZ incorporates lessons learned from ongoing incident response activities into incident response procedures accordingly. If changes are required, necessary changes are made to the policy and procedures and redistributed according to all responsible organizations and key personnel.	Inspected the incident response plan to determine that the document has been reviewed and revised every year and changes were incorporated from prior incidents and associated lessons learned.	No exceptions noted.
	Annual testing of the incident response plan is performed using tabletop exercises and simulations to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned from tabletop exercises are used to implement changes to reflect effective procedures when handling incidents.	Inspected documentation for the most recent incident response plan review to determine that the plan was tested within the past year, and that drills conducted to imitate incidents were resolved and service availability was restored. Inspected the incident response plan for revision because of the testing performed.	No exceptions noted.
	XYZ has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.	Inspected the security and systems methodology policy to determine whether it includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Security administration team approval of changes is required prior to implementation.	Inspected change documentation from system-generated list of system changes to determine whether the changes were approved by security administration prior to implementation.	No exceptions noted.
Change Management			
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.	XYZ has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	Inspected the systems development life cycle (SDLC) methodology to determine that it governed the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	No exceptions noted.
	XYZ's software and infrastructure change management process requires that change requests are: • Authorized • Formally documented • Tested prior to migration to production • Reviewed and approved	Inspected a sample of change requests to determine that changes were: • Authorized • Formally documented • Tested prior to migration to production • Reviewed and approved • Tracked through completion	No exceptions noted.
	Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements.	Inspected the change management procedures to determine that procedures were in place to govern the modification and maintenance of production systems and addressed security and availability requirements.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ requires all changes, including maintenance activities, to be documented in the help desk application and tracked from initiation through deployment and validation.	Inspected a sample of change requests to determine that changes were: • Authorized • Formally documented • Tested prior to migration to production • Reviewed and approved • Tracked through completion	No exceptions noted.
	Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected internal and external vulnerability scans for a sample of quarters to determine that internal and external vulnerability scans were performed quarterly and remediation plans were developed to remediate all critical and high vulnerabilities.	No exceptions noted.
	Baseline configurations are retained within the configuration manager tool for roll back capability anytime an approved configuration change is made. Baseline configurations are reviewed and updated annually, when required due to reviews and system changes, and anytime integral system components are added.	Inspected the configuration manager tool to determine that baseline configurations are retained and up to date for applicable system changes.	No exceptions noted.
	XYZ maintains a documented change management and patch management process.	Inspected the change and patch management policies to determine whether there are documented policies and procedures.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Servers are reviewed monthly by the security administration team to determine if required vendor security patches have been applied by comparing patches applied per system configuration reports to the vendor's list of current patches released.	For a sample of months, inspected management's server review documentation to determine whether the security administration team had completed the review of the patches applied to the vendor's list of current patches released. For any missing patches identified, inspected the change request created by the security administration team and the change record to ascertain that the identified patches were applied.	No exceptions noted.
	XYZ contracts with third parties to conduct monthly security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management. Management develops a plan of action for each recommendation and follows up on open recommendations monthly.	For a sample of months, inspected the security review and vulnerability assessment reports to determine whether the assessments were performed, communicated, and addressed by management.	No exceptions noted.
	XYZ prepares a root cause analysis for high severity incidents. Based on the root cause analysis, change requests are prepared, and XYZ's risk management process and relevant risk management data is updated to reflect the planned incident response.	Inspected the root cause analysis for high severity incidents to determine whether the risk management process and relevant risk management data was updated to reflect the planned incident response.	No exceptions noted.
	XYZ maintains a formally documented change management process. Changes to hardware, operating system, and system software are authorized, tested (when applicable), and approved by appropriate personnel prior to implementation.	Inspected the change management policy for hardware, operating system, and system software to determine whether procedures are formally documented, including procedures over authorization, testing (when	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
		applicable), and approval prior to implementation. Inspected change documentation from system-generated list of system changes to determine whether the changes were authorized, tested, and approved prior to implementation.	
	Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.	Inspected documentation of the system infrastructure architecture to determine whether a separate development or test environment existed from the production environment. Inspected the access list to the change management tools to determine whether access to migrate changes to production was appropriate based on job responsibilities and that developers did not have the ability to migrate changes into production. Inspected change documentation from system-generated list of system changes to determine whether the changes were authorized, tested, and approved prior to implementation.	No exceptions noted.
	Emergency changes follow the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, all necessary approvals are obtained and documented.	Inspected change documentation from system-generated list of program changes for a sample of emergency changes to determine whether the changes were approved.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed. The risk management program includes the use of insurance to minimize the financial impact of any loss events.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. Inspected the most recent risk assessment to determine that threats and changes were formally identified and assessed on an annual basis.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.	The risk management program includes the use of insurance to minimize the financial impact of any loss events.	Inspected the risk management policy to determine that the program includes cyber insurance for potential loss events.	No exceptions noted.
	Formal information sharing agreements are in place with related parties and vendors. These agreements include the scope of services and security commitments applicable to that entity.	Inspected contracts for a sample of new vendors added during the audit period to determine that agreements included scope of services and security commitments.	No exceptions noted.
	A vendor risk assessment is performed for all vendors on an annual basis that have access to confidential data or impact the security of the system.	Inspected vendor risk assessment documentation for a sample of vendors to determine that a risk assessment was performed within the past year.	No exceptions noted.

(continued)

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	Management has established defined roles and responsibilities to oversee implementation of information security policies.	Inspected security policies to determine XYZ has established defined roles and responsibilities to oversee implementation of information security policies.	No exceptions noted.
	XYZ has documented and communicated security policies that define the information security rules and requirements for the service environment.	Inspected the security policies to determine that they address applicable information security requirements including communication of service issues. Observed the XYZ's intranet to determine that security policies are published and communicated to employees and relevant third parties.	No exceptions noted.
	An annual risk assessment is performed by management and includes the following: *a.* Determining business objectives, entity, subsidiary, division, operating unit, and functional levels *b.* Evaluating the effect of environmental, regulatory, and technological changes on the TMS system security *c.* Involving appropriate levels of management. *d.* Analyzing risks associated with the threats *e.* Identifying threats to operations, including security threats, using information technology asset records *f.* Identifying threats to operations, including threats from vendors, business partners, and other parties *g.* Determining a risk mitigation strategy	Inspected the annual risk assessment documentation to determine whether they included the significant aspects of operations.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of XYZ Service Organization's Controls*	*Service Auditor's Tests of Controls*	*Results of Service Auditor's Tests of Controls*
	XYZ has clauses in its agreements with vendors and business partners to terminate relationships when necessary. Vendor and business partner access is removed upon termination through a termination checklist and access is revoked within 24 hours as part of the termination process.	Inspected a listing of terminated vendors and compared the vendor employee listing to the active user listing to determine that terminated vendor employees did not retain access to the in-scope system and platforms after their separation. Inspected termination tickets for a sample of terminated vendors during the review period to determine that vendor employee access was revoked within 24 hours as a part of the termination process.	No exceptions noted.

Section 5—Other Information Provided by Example Service Organization That Is Not Covered by the Service Auditor's Report

Note to Readers: *The service organization may wish to attach to the description of the service organization's system, or include in a document containing the service auditor's report, information in addition to its description. The following are examples of such information*:

- *Future plans for new systems*
- *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 when such responses have not been subject to procedures by the service auditor*

For brevity, an example is not provided.

Appendix E

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* (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* (AICPA, *Trust Services Criteria*).[2]

---

[1] The description criteria presented in this document (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*, in a SOC 2® report. The 2018 description criteria are codified as DC section 200 in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are codified as DC section 200A.

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2 examination), either the 2018 description criteria or 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

[2] The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality*,

(continued)

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.

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[3]

To: 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* (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 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* (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

---

(footnote continued)

and Privacy (2016), and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

[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.

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 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 of 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. 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 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 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 achieved 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*]

[*Service auditor's city and state*]

[*Date of the service auditor's report*]

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 relevant to security, availability, confidentiality, and privacy were achieved. 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 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* (AICPA, *Trust Services Criteria*).[1] 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.

---

[1] The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

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.

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

Note to Readers: *The following description of the boundaries of the system is for illustrative purposes only and is not meant to be prescriptive. For brevity, the illustration does not include everything that might be described in a description of the boundaries of the service organization's system.*

XYZ Service Organization's Description of the Boundaries of Its Transportation Management System

Services Provided

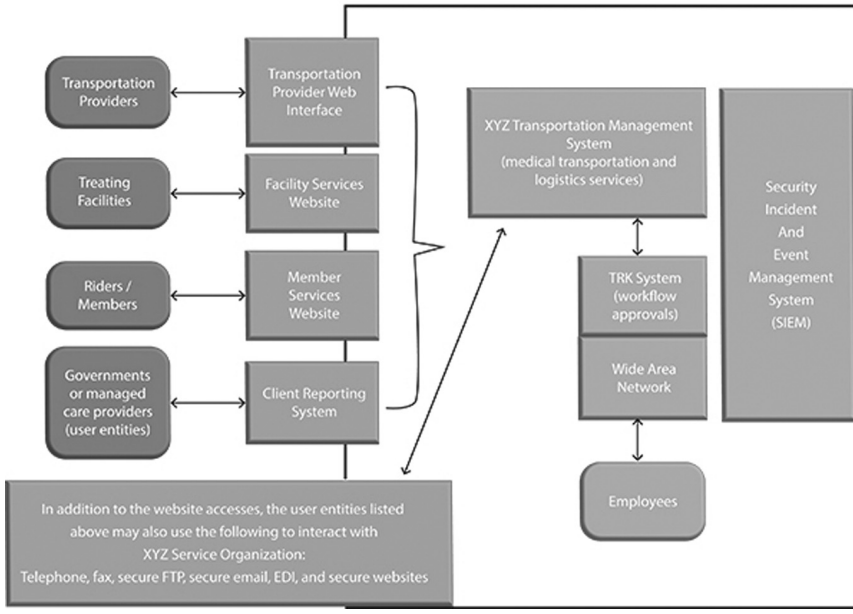
XYZ Service Organization (XYZ) provides medical transportation (MT) services throughout the United States. The Company was founded in 19XX to provide MT services to Medicaid recipients.

XYZ's core application, Transportation Management System (TMS), is a multiuser, transaction-based application suite that enables the processing and delivery of transportation and logistics services. The TMS enables processing of the following tasks related to MT trips:

- Capturing data for transportation providers, governments, and managed care providers (user entities), treating facilities, and riders
- Determining rider eligibility
- Providing gate keeping and ride authorization
- Managing complaints and verifying compliance with transportation agreements
- Managing transportation providers
- Reconciling billing to completed rides
- Providing operational, management, and ad hoc reports
- Providing data reporting in a variety of formats

Trips are tracked through the order cycle, from initial ride assignment to completion or reassignment of the ride, and by payments. Transportation providers send XYZ daily trip information, including information about trips completed or cancelled (or no-shows) and weekly driver logs, which are entered into the TMS. System-generated reports provide supporting documentation for trips, including date, transportation provider, rider, and actual trip via a unique job number.

Information is shared with user entities by telephone, fax, secure electronic exchange (FTP [file transfer protocol], email, EDI [electronic data interchange]), and secured websites.



Infrastructure

The TMS runs on Microsoft Windows file servers using a wide area network.

Employees access the application either through their desktop on company-supplied computers or through a Citrix Access Gateway. Data communications between offices are encrypted with Cisco virtual private networking (VPN) technology using Advanced Encryption Standard 256-bit encryption to protect data and intra-company communications.

The TMS uses the IBM DB2 relational database management system. These database servers and file servers are housed in XYZ's secured network operations centers (NOCs).

Software

The TMS is a Microsoft Windows client-server application developed and maintained by XYZ's in-house software engineering group. The software engineering group enhances and maintains the TMS to provide service for the company's transportation providers, governments and managed care providers (user entities), treating facilities, and riders. XYZ's software is not sold on the open market.

The TMS tracks information in real time. The information is immediately stored in the database and is accessible for daily operations, service authorization, trip scheduling, provider reimbursement, agency monitoring, and report generation. The information can be retrieved, reviewed, and reported as needed to create the history of approvals and denials for any rider. Information can be

retrieved by rider identification number, rider name, trip date, facility attended, and transportation provider.

External websites are supplied to supplement XYZ's ability to communicate and exchange information with transportation providers, governments and managed care providers (user entities), treating facilities, and riders. Each website targets a specific audience and is designed to address their business needs. These include a site for the transportation providers, governments and managed care providers, treating facilities, and riders.

The XYZ transportation provider web interface is a multiuser, web-based application that helps to manage the flow of information between XYZ and the transportation providers. This website allows transportation providers to enter and retrieve certain information about trips they were assigned by XYZ. It also provides some specific performance reports to help them manage their work with XYZ. To access the site, transportation providers must sign up for the site and fill out certain EDI forms.

The XYZ facility services website supports transportation requests from treating facilities on behalf of their clients. The purpose of the site is to provide a means to request trips and to manage trip requests online without the need to call an XYZ call center. The facility services website allows a treating facility to enter a single trip or standing order request for review and approval by an XYZ facility representative, look up and view trip requests, modify or update pending requests, and withdraw pending requests.

The XYZ member services website is like the facility services website, except its focus is on the riders. After a rider has successfully logged in, he or she is able to request new trip reservations, view pending requests and processed reservations, edit pending requests, withdraw pending requests, and cancel existing reservations. Requests are placed in a request queue within the TMS database for review by call center personnel through the TMS.

The XYZ client reporting interface is provided as a service to XYZ's government agencies and managed care providers (user entities). This interface allows them to monitor basic statistics of their business and resolve simple questions and complaints. Summary reports of trip volume, complaints, and utilization are available in addition to detailed reports for single trips, single complaints, and rider eligibility.

People

XYZ has a staff of approximately 500 employees organized in the following functional areas:

- *Corporate*. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources, and transportation provider relations. These individuals use the TMS primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for XYZ's user entities.
- *Operations*. Staff that administers the scheduling and administration of transportation providers and riders. They provide the direct day-to-day services, such as transportation reservation intake, trip distribution to transportation providers, quality

assurance monitoring, medical facility support, service claims adjudication, transportation network support, and reporting.

- — Customer service representatives take phone calls directly from riders to arrange transportation. These requests are entered into the TMS and initiate the life cycle of a trip.
- — Transportation coordinators use the TMS to assign trips to transportation providers. They also manage rerouting and dispensing work from the TMS to the transportation providers on daily trip lists via fax. Transportation managers maintain the transportation provider network database, including updates for training, violations, screenings, and other compliance measures.
- — Quality assurance (or utilization review) employees use reports generated by the TMS to select samples of trips that are tested for contractual compliance and to monitor for fraud and abuse. They also take complaints from riders, facilities, and transportation providers and work them to resolution, using tools within the TMS.
- — The facility staff manages the facility database for the TMS. They also maintain the transportation standing orders within the system and take single trip requests from facilities only.
- — The claims staff receives requests for payment and adjudicates these claims in the software. This includes invoice management, trip verification, and billing support.
- — A reports manager typically uses the TMS to produce contract-level specific reports for XYZ's user entities.

- *IT*. Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom.

  - — The help desk group provides technical assistance to the TMS users.
  - — The infrastructure, networking, and systems administration staff typically has no direct use of the TMS. Rather, it supports XYZ's IT infrastructure, which is used by the software. A systems administrator will deploy the releases of the TMS and other software into the production environment.
  - — The software development staff develops and maintains the custom software for XYZ. This includes the TMS, supporting utilities, and the external websites that interact with the TMS. The staff includes software developers, database administration, software quality assurance, and technical writers.

- — The information security staff supports the TMS indirectly by monitoring internal and external security threats and maintaining current antivirus software.
- — The information security staff maintains the inventory of IT assets.
- — IT operations manage the user interfaces for the TMS. This includes processing user entity–supplied membership and eligibility files, producing encounter claims files, and other user-oriented data (capitation files, error reports, remittance advice, and so on).
- — Telecom personnel maintain the voice communications environment, provide user support to XYZ, and resolve communication problems. This group does not directly use the TMS, but it provides infrastructure support as well as disaster recovery assistance.

Data

Data, as defined by XYZ, constitutes the following:

- Master transportation file data
- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Transaction processing is initiated by the receipt of a trip or standing order request. This request typically comes directly from a rider or treating facility by telephone or via the websites, or it may arrive by fax from a treating facility. After the trip is completed, the transportation provider sends XYZ paper documents with daily trip information, including information about completed trips, cancellations or no-shows, and weekly driver logs, all of which is entered into the system's verification module; a portion of this trip completion information may be entered on the XYZ transportation provider web interface.

Output reports are available in electronic PDF, comma-delimited value file exports, or electronically from the various websites. The availability of these reports is limited by job function. Reports delivered externally will only be sent using a secure method—encrypted email, secure FTP, or secure websites—to transportation providers, treating facilities, and governments or managed care providers using XYZ- developed websites or over connections secured by trusted security certificates. XYZ uses Transport Layer Security to encrypt email exchanges with government or managed care providers, facility providers, and transportation providers.

Processes and Procedures

Management has developed and communicated to transportation providers, governments and managed care providers, treating facilities, and riders procedures to restrict logical access to the TMS. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

Attachment B

Principal Service Commitments and System Requirements

XYZ designs its processes and procedures related to TMS to meet its objectives for its MT services. Those objectives are based on the service commitments that XYZ makes to user entities, the laws and regulations that govern the provision of MT services and the financial, operational and compliance requirements that XYZ has established for the services. The MT services of XYZ are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which XYZ operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the TMS that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

XYZ establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in XYZ's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.

In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the TMS.

Illustrative Independent Service Auditor's SOC 3® Report

Independent Service Auditor's Report[2]

To: 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* (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 service 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 whether 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 American Institute of Certified Public Accountants. 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.

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

[2] The report may also be titled "Report of Independent Service Auditors."

- 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.

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*]

[*Service auditor's city and state*]

[*Date of the service auditor's report*]

Appendix G

Appendix G-1	***Illustrative Management Representation Letter for Type 2 Engagement***
Appendix G-2	***Illustrative Management Representation Letter for Type 1 Engagement***

Appendix G-1

Illustrative Management Representation Letter for Type 2 Engagement

This appendix is nonauthoritative and is included for informational purposes only.

Illustrative Management Representation Letter for Type 2 Engagement

[*Service Organization's Letterhead*]
[*Date*][1]
[*Service Auditor's Name*]
[*Address*]

In connection with your engagement to report on [*name of service organization*]'s (service organization) description of its [*type or name of*] system entitled "[*name of service organization*'s *description*]" throughout the period [*date*] to [*date*] (description)[2] 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* (AICPA, *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 [*name of 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* (AICPA, *Trust Services Criteria*), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description presents the system that was designed and implemented throughout the period [*date*] to [*date*] in accordance with the description criteria and whether the controls stated in the description were suitably designed and operating effectively throughout the period [*date*] to [*date*] to provide reasonable assurance that [*name of service organization*]'s service commitments and system requirements were achieved based on the applicable trust services criteria.

We confirm, to the best of our knowledge and belief, as of [*date of this letter*], the following representations made to you during your examination:[3]

1. We reaffirm our assertion attached to the description.
2. We have evaluated the presentation of the description in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls stated therein to

[1] This representation letter should be dated as of the date of the service auditor's report.

[2] The title of the description of the service organization's system included in management's representation letter should be the same as the title used in the description of the service organization's system, in management's assertion, and in the service auditor's report.

[3] If management does not provide one or more of the written representations requested by the service auditor, the service auditor should discuss the matter with management, evaluate the effect of such exclusions on the examination, and take appropriate action, which may include disclaiming an opinion or withdrawing from the examination.

provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and all relevant matters have been considered and reflected in our evaluation and in our assertion.

3. We have disclosed to you any of the following of which we are aware:
    a. Misstatements (including omissions) in the description
    b. Instances in which controls were not suitably designed and implemented
    c. Instances in which controls did not operate effectively or as described
    d. Any communications from regulatory agencies, user entities, or others affecting the presentation of the description or the suitability of the design or operating effectiveness of the controls stated therein, including communications received between the end of the period addressed in our description and the date of your report
    e. All other known matters contradicting the presentation of the description or the suitability of the design or operating effectiveness of the controls stated therein or contradicting our assertion
4. We acknowledge responsibility for our assertion and for
    a. the presentation of the description in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
    b. selecting the trust services category or categories to be included within the scope of the examination and determining that they are appropriate for our purposes.
    c. stating the applicable trust services criteria and related controls in the description.
5. We have disclosed to you any known events subsequent to the period covered by the description up to the date of this letter that would have a material effect on the presentation of the description or on the suitability of the design or operating effectiveness of the controls stated therein or on our assertion.
6. We have disclosed to you any changes in the controls that are likely to be relevant to report users occurring through the date of this letter.
7. We have provided you with all information and access that is relevant to your examination and to our assertion.
8. We believe the effects of uncorrected misstatements, if any, are immaterial, individually and in the aggregate, to the presentation of the description in accordance with the description criteria or to the suitability of the design or operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

9. We have responded fully to all inquiries made to us by you during the examination.
10. We have disclosed to you any of the following of which we are aware:
    a. Actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the presentation of the description or the suitability of the design or operating effectiveness of the controls stated therein
    b. Instances of noncompliance with laws and regulations or uncorrected misstatements attributable to the service organization that may affect one or more user entities
    c. All identified system incidents that resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements during the [*period of time covered by the description*]

[*Add any other representations about matters the service auditor deems appropriate or matters relevant to special circumstances, such as industry-specific matters*.]

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The examination was designed for the purpose of expressing an opinion about whether, in all material respects, the description is presented in accordance with the description criteria and whether 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 also understand that the opinion was based on your examination and that the procedures performed in the examination were limited to those that you considered necessary.

_____

[*Name and title of appropriate member of management*]

_____

[*Name and title of appropriate member of management*]

_____

[*Name and title of appropriate member of management*]

Appendix G-2

Illustrative Management Representation Letter for Type 1 Engagement

This appendix is nonauthoritative and is included for informational purposes only.

Illustrative Management Representation Letter for Type 1 Engagement

[*Service Organization's Letterhead*]
[*Date*][1]
[*Service Auditor's Name*]
[*Address*]

In connection with your engagement to report on [*name of service organization*]'s (service organization) description of its [*type or name of*] system entitled "[*name of service organization*'s description]" as of [*date*] (description)[2] based on the description 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* (AICPA, *Description Criteria*), and the suitability of the design of controls stated in the description as of [*date*] to provide reasonable assurance that [*name of 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* (AICPA, *Trust Services Criteria*), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion on whether the description presents the system that was designed and implemented as of [*date*] in accordance with the description criteria and whether the controls stated in the description were suitably designed to provide reasonable assurance that [*name of service organization*]'s service commitments and system requirements were achieved based on the applicable trust services criteria, if the controls operated effectively as of [*date*].

We confirm, to the best of our knowledge and belief, as of [*date of this letter*], the following representations made to you during your examination:[3]

1. We reaffirm our assertion attached to the description.
2. We have evaluated the presentation of the description in accordance with the description criteria and the suitability of the design of the controls stated therein to provide reasonable assurance

---

[1] This representation letter should be dated as of the date of the service auditor's report.

[2] The title of the description of the service organization's system included in management's representation letter should be the same as the title used in the description of the service organization's system, in management's assertion, and in the service auditor's report.

[3] If management does not provide one or more of the written representations requested by the service auditor, the service auditor should discuss the matter with management, evaluate the effect of such exclusions on the examination, and take appropriate action, which may include disclaiming an opinion or withdrawing from the examination.

that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and all relevant matters have been considered and reflected in our evaluation and in our assertion.

3. We have disclosed to you any of the following of which we are aware:
    a. Misstatements (including omissions) in the description
    b. Instances in which controls were not suitably designed and implemented
    c. Instances in which controls did not operate effectively or as described
    d. Any communications from regulatory agencies, user entities, or others affecting the presentation of the description or the suitability of the design or operating effectiveness of the controls stated therein, including communications received between [*as of date of the description*] and the date of your report
    e. All other known matters contradicting the presentation of the description and the suitability of the design or operating effectiveness of the controls stated therein or contradicting our assertion
4. We acknowledge responsibility for our assertion and for
    a. the presentation of the description in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
    b. selecting the trust services category or categories to be included within the scope of the examination and determining that they are appropriate for our purposes.
    c. stating the applicable trust services criteria and related controls in the description.
5. We have disclosed to you any known events subsequent to the period covered by the description up to the date of this letter that would have a material effect on the presentation of the description or on the suitability of the design or operating effectiveness of the controls stated therein or on our assertion.
6. We have disclosed to you any changes in the controls that are likely to be relevant to report users occurring through the date of this letter.
7. We have provided you with all information and access that is relevant to your examination and to our assertion.
8. We believe the effects of uncorrected misstatements, if any, are immaterial, individually and in the aggregate, to the presentation of the description in accordance with the description criteria or to the suitability of the design or operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

9. We have responded fully to all inquiries made to us by you during the examination.
10. We have disclosed to you any of the following of which we are aware:
    a. Actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the presentation of the description or the suitability of the design or operating effectiveness of the controls stated therein
    b. Instances of noncompliance with laws and regulations or uncorrected misstatements attributable to the service organization that may affect one or more user entities
    c. 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 [*date of description*]

[*Add any other representations about matters the service auditor deems appropriate or matters relevant to special circumstances, such as industry-specific matters*.]

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The examination was designed for the purpose of expressing an opinion about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein 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. We also understand that the opinion was based on your examination and that the procedures performed in the examination were limited to those that you considered necessary.

_____

[*Name and title of appropriate member of management*]

_____

[*Name and title of appropriate member of management*]

_____

[*Name and title of appropriate member of management*]

Appendix H

Performing and Reporting on 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, *Examination Engagements*,[2] of the attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with the 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, review, compilation, management consulting, tax, or other professional services

---

[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.

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

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 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. 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 Engagements Other Than Audits or Reviews of Historical Financial Information*, and AT-C sections 105, *Concepts Common to All Attestation Engagements,* and 205, *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://www.aicpa.org/content/dam/aicpa/interestareas/frc/auditattest/downloadabledocuments/attest-clarity/differences-between-isae-3000-at-c-105-and-205.pdf.

---

[4] *Frequently Asked Questions: General ethics questions* issued by the AICPA Professional Ethics Division as of May 1, 2017. https://www.aicpa.org/interestareas/professionalethics/resources/tools/downloadabledocuments/ethics-general-faqs.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–.66 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 Report

To: 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* (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* (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 have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

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*]

[*Service auditor's city and state*]

[*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 Description of Controls and Their Design and Operating Effectiveness

To: 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* (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* (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[5] 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.

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

[5] ISQC I, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements*.

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 I

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,* and TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, of 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 a computer, its operating system, a network, or other elements.

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, who 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 who works with another company who 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 (1) the nature of the services performed by the subservice organization; (2) 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 (3) 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. Controls that service organization management assumed, in the design of the service organization's system, would be implemented by 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 are achieved.

complementary user entity controls. Controls that service organization management assumed, in the design of the service organization's system, would be implemented by user entities and 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 (1) processing integrity or availability of systems or (2) 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 his or her information, consent is the individual's way of giving permission for the use or disclosure. Consent may be affirmative (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" his or her 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 help 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 the subject matter.

cybersecurity objectives. The objectives that an entity establishes to address the cybersecurity risks that could otherwise threaten the achievement of the entity's overall business objectives.

cybersecurity risk management examination. An examination engagement to report on whether (*a*) management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (*b*) the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria. A cybersecurity risk management examination is performed in accordance with the attestation standards and the AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*.

cybersecurity risk management examination report. The end product of the cybersecurity risk management examination, which includes management's description of the entity's cybersecurity risk management program, management's assertion, and the practitioner's report.

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 release, transfer, provision of access to, 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 and (*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. (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 relevant to meeting the common needs of the broad range of SOC 2® report users.

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.

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 the 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 control.

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.

Index of Pronouncements and Other Technical Guidance

A

Title	*Paragraphs*
AT-C Section	
105, *Concepts Common to All Attestation Engagements*	1.15, 1.24, 1.29, 1.64, 1.70–.72, 1.74–.76, 2.01, 2.32, 2.43, 2.45, 2.47, 2.49, 2.57, 2.75, 2.96, 2.102, 2.124, 2.155–.157, 3.09, 3.167, 3.221–.222
205, *Examination Engagements*	1.15, 1.52–.53, 1.64, 1.70, 1.72, 2.02, 2.26, 2.51, 2.66, 2.68, 2.70–.73, 2.92–.96, 2.101–.102, 2.104, 2.111, 2.121, 2.125–.126, 2.143, 2.152, 2.157–.158, 2.160, 2.165–.166, 3.04–.05, 3.64, 3.66, 3.70, 3.74, 3.78–.79, 3.121, 3.141, 3.158, 3.165, 3.176, 3.178–.181, 3.183, 3.186, 3.201, 3.209–.210, 3.212, 3.215–.216, 3.222, 3.225, 4.04, 4.31, 4.33–.34, 4.36, 4.43–.45, 4.48, 4.54, 4.57–.58, 4.61, 4.100–.102, 4.115–.116, Table 4-3 at 4.32, Table 4-4 at 4.116
320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*	1.60
706, *Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs in the Independent Auditor's Report*	4.90
Audit and Accounting Guides (AAG)	
Audit Sampling	3.143, 3.173
Reporting on an Entity's Cybersecurity Risk Management Program and Controls	1.66
Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)	1.61

C

Title	*Paragraphs*
Code of Professional Conduct	1.73, 2.57
ET section 1.200.001, "Independence Rule"	1.73, 2.36
ET section 1.210, "Conceptual Framework Approach"	2.36
ET section 1.297, "Independence Standards for Engagements Performed in Accordance With Statements on Standards for Attestations Engagements"	2.36
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	
Internal Control-Integrated Framework	1.33, 1.43

D

Title	*Paragraphs*
DC Section 200, *2018 Description Criteria for Description of a Service*	1.27

Q

Title	*Paragraphs*
QC Section 10, *A Firm's System of Quality Control*	1.74–.75, 2.31

T

Title	*Paragraphs*
TSP Section 100, *Criteria, And Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy*	1.27, 1.56, Supplement B

Subject Index

A

ACCEPTING A SOC 2® EXAMINATION ENGAGEMENT 2.01–.90
- Agreeing on terms of engagement ..... 2.32, ... 2.70–.90
- Changes in terms of examination 2.75–.78
- Competence of engagement team members 2.39–.42
- Engagement acceptance and continuance 2.31–.34
- Independence of service auditor ..... 2.05, ... 2.35–.38
- Management of service organization's responsibilities 2.03–.29
- Preconditions of SOC 2® engagement 2.43–.65
- Service auditor's responsibilities ... 2.30, 2.74
- Written assertion and representations request of service organization management 2.66–.69

ADDITIONAL SUBJECT MATTERS AND CRITERIA, ADDRESSING IN SOC 2® EXAMINATION ..... 1.50–.54, ... Table 1–3 at 1.50

ADVERSE OPINION 3.29, 4.14, 4.54–.55

ALERT PARAGRAPH, SERVICE AUDITOR'S REPORT ..... 4.34, Table 4-3 at 4.32

ANALYTICS 3.117, 3.143

APPLICABLE TRUST SERVICES CRITERIA. *See also* trust services criteria .... 1.05, ... 1.16, 1.32, 3.92–.94, 4.77, ... Table 1-2 at 1.41, ... Table 4-4 at 4.116, Supplement B

ASSURANCE SERVICES EXECUTIVE COMMITTEE (ASEC) 1.29, 1.36, 2.57

AUDIT EVIDENCE
- Evaluating 3.182–.189
- Concluding on sufficiency and appropriateness of 4.05–.09

AUDIT OPINION. *See* opinion

AUDIT SAMPLING, TESTS OF CONTROLS 3.142–.146, 3.173, 4.19

AUTOMATED CONTROLS, TESTS OF ... 3.138

AVAILABILITY
- Applicable trust services criteria ..... Table 1-2 ..... at 1.41, Supplement B
- Boundaries of the system and 1.22
- Defined 1.37
- In description of the system 3.26, 3.34
- Service organization controls relevant to 1.04, 3.149

B

BOUNDARIES OF SERVICE ORGANIZATION'S SYSTEM
- Areas covered by 1.21–.23
- Distinguishing between SOC 1®, SOC 2®, and SOC 3® engagements and related reports ..... 2.45, Appendix B
- Identifying controls outside of 3.32
- Management's assertion in SOC 3® report 2.167, 4.112–.114
- Planning the examination 2.75, 2.113

BUSINESS PARTNERS
- Prospective 1.10
- Relationship to service organizations 1.01–.04
- Risk consideration 3.147–.151
- As specified parties of a SOC 2® report 1.09

C

CARVE-OUT METHOD
- CSOCs. *See* complementary subservice organization controls
- Defined 2.12
- Description of the system, contents of ... 3.42
- Disclosures related to subservice organizations 3.46–.54
- Management responsibilities for use of 2.12–.16
- Materiality related to 3.77
- Service auditor's report ..... 4.32, ... 4.39–.41, Appendix D-1
- Suitability of design of controls, evaluating 3.86, 3.99–.100, 3.152

CHANGES TO CONTROLS
- Evaluating and testing 2.58, 3.140–.141
- Omission from description of the system 4.72

CHANGES TO THE SYSTEM
- Omission of relevant changes in description 4.72
- During the period ..... 3.55–.56, 3.62, ... 3.108, 3.140–.141
- Between periods 3.57–.58

COMMITMENTS TO USER ENTITIES. *See* service commitments and system requirements

COMMON CRITERIA. *See also* trust services criteria ..... 1.39–.43, Table 1-2 at 1.41

COMPETENCE
- Engagement Team Members 2.39–.42
- Internal audit function ..... 2.132, 2.139-.144, ... 2.146, 3.166

COMPETENCE—continued
- Other practitioner 2.156
- Performance of controls .....3.79, 3.98, ... 3.102, 3.106
- Specialists 2.160-.161, 3.178
- Written representations 3.209, 3.222

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)
- Disclosures related to carve-out subservice organizations 3.46–.54
- Identification of 2.17–.19
- Omission from description of the system, illustrative separate paragraphs 4.74
- In separate SOC 2® report analysis 2.114
- Service auditor's report ..... 4.32, 4.39–.41, ... Table 4-3 at 4.32, Appendix D
- Tests of controls 3.152–.155

COMPLEMENTARY USER ENTITY CONTROLS (CUECS)
- Disclosure of 3.36-.41, 3.88–.91
- Identification of 2.20–.25
- Omitted from description of the system, illustrative separate paragraph 4.73
- In a separate SOC 2® report analysis ...2.114
- Service auditor's report ..... 4.32, 4.36–.38, ... Appendix D, Table 4-3 at 4.32
- SOC 3® engagement 2.171
- Suitability of design of controls, evaluating 3.86,

CONFIDENTIALITY
- Applicable trust services criteria .....Table 1-2 ..... at 1.41, Supplement B
- Boundaries of the system and 1.23
- Defined 1.37
- Privacy distinguished from 1.25–.26
- Service organization controls relevant to 1.04

CONTROLS. *See also* trust services categories; trust services criteria
- Changes to, evaluating and testing .....2.58, ... 3.140–.141
- Comparing description to implementation 3.22–.23
- Controls that did not operate during the period 3.156
- CSOCs. *See* complementary subservice organization controls
- CUECs. *See* complementary user entity controls
- Deficiencies in. *See* deficiencies in controls
- In description of service organization's system .....3.30–.32, 3.163, ... Table 3-1 at 3.30
- Design of. *See* suitability of design of controls
- Effectiveness of. *See* operating effectiveness of controls
- Consideration of entity-level controls in planning the examination 2.127–.131
- System description, evaluating 3.12–.23
- Management's responsibility for ... 2.04, 2.26

CONTROLS—continued
- Not implemented but included in description, illustrative separate paragraph 4.70
- Not operating during the period 4.86–.88
- Omission of relevant changes in description of the system 4.72
- Operating effectiveness of. *See* operating effectiveness of controls
- Planning the examination 2.110, 2.113
- Risk assessment 2.125–.126
- Service auditor's recommendations for improving 4.94
- Subservice organizations .....2.06–.10, ... 3.43–.54
- Suitability of design. *See* suitability of design of controls
- Tests of. *See* tests of controls
- User entities reviewing 1.04

CRITERIA. *See* description criteria; trust services criteria

CSOCs. *See* complementary subservice organization controls

CUECs. *See* complementary user entity controls

CYBERSECURITY RISK MANAGEMENT EXAMINATION AND REPORT .....1.63–.68, Appendix C

D

DATA
- Reliability of, in tests of controls 3.121–.130
- As system component 1.20

DATE OF SERVICE AUDITOR'S REPORT. *See also* periods ..... Table 4-3 at 4.32, ... Table 4-4 at 4.116

DEFICIENCIES IN CONTROLS. *See also* deviations
- Communicating incidents of 3.193–.196
- Defined 3.10, 3.101–.102
- Effect on third parties 3.163
- Entity-level controls 2.129–.130
- Evaluating results of procedures 3.185
- Forming the opinion 4.10–.12
- Identifying and evaluating 3.70–.71
- Modifications to management assertions due to 3.228, 4.38
- Occurring during the original, extended, or modified period 2.87–.90, 3.132–.133
- Operating effectiveness of controls 4.85
- Suitability of design of controls 3.101–.105, 4.79–.82
- Testing for 3.185–.189

DEFINITIONS .....Appendix I

DESCRIPTION CRITERIA ..... Supplement A
- Assessing suitability of 2.57–.58
- Disclosures about service commitments and system requirements 3.24-3.26
- System incidents 3.33–.35
- User entity responsibilities and CUECs 3.36-.41, 4.37
- Disclosures related to subservice organization 3.38, 3.42, 3.47
- Significant changes to service organization's system 3.55–.58, 3.108
- Description's requirements for meeting 3.17–.19
- Evaluating against description of the system 3.20–.23
- Generally 1.05, 1.15–.17, 1.27–.30
- Materiality considerations 3.72–.78
- Misstated or misleading information 3.67
- In SOC 2® report ..... Table 1-1 at 1.18

DESCRIPTION OF SERVICE ORGANIZATION'S SYSTEM
- Boundaries. *See* boundaries of the system
- Qualitative factors 3.163
- Changes to the system occurring between periods covered by type 2 exam ... 3.57–.58
- Confidentiality or privacy principle in 3.59
- Controls. *See* controls
- Criteria for evaluating. *See* description criteria
- CUECs and user entity responsibilities 3.36–.41
- Entity-level controls disclosures in 2.131
- Evaluating results of procedures 3.183–.189
- Generally 1.07, 3.12–.23
- Information not covered by the service auditor's report 4.95–.104
- Management's responsibility for ... 1.16, 2.26, ... 2.117
- Materiality consideration. *See also* material misstatement, risk of 3.07, 3.72–.78
- Misstated or misleading description, considering 3.64–.68
- Misstatements, identifying and evaluating 3.10, 3.69–.71
- Performing a SOC 2® examination ... 3.12–.78
- Planning the examination ..... 2.113, ... 2.116–.117
- Procedures to obtain evidence about 3.59–.63
- Service commitments and system requirements 2.59–.65, 3.24–.29
- Significant changes to the system during period covered by type 2 exam ... 3.55–.56, ... 3.62, 3.108
- Subsequent event effects 3.214–.219
- Subservice organization considerations ..... 2.11–.16, 2.24–.25, ... 3.42–.54, 4.75
- System incident disclosures 3.33–.35
- Uncorrected misstatements and deficiencies 4.10–.12

DESIGN OF CONTROLS. *See* suitability of design of controls

DEVIATIONS
- Changes in terms of engagement 2.76
- Defined 3.10
- Discovery of uncorrected errors ..... 3.193, ... 3.203
- Effect on suitability of design of controls 3.163
- Evaluating results of procedures 3.185
- Identifying and evaluating 3.157-3.160
- Materiality concept in disclosing 4.16
- As result of intentional acts 3.163, 3.190
- Reporting ..... 4.15–.22, Table 4-1 at 4.15

DISCLAIMER OF OPINION
- Change in terms of examination 2.78
- Independence of service auditor and 2.38
- For other information service organization appends to report 4.104
- Service auditor's report ..... 4.61–.67, ... Appendix D-3
- Written representation issues ..... 3.211, ... 4.66-4.67

DOCUMENTATION. *See also* service auditor's report; written assertions; written representations
- Management's risk assessment ..... 2.55, ... 2.119, 3.97
- Performing a SOC 2® examination 3.221–.225

E

EFFECTIVENESS OF CONTROLS. *See* operating effectiveness of controls; suitability of design of controls

EMPHASIS-OF-MATTER PARAGRAPHS, IN SERVICE AUDITOR'S REPORT 4.89–.90

ENGAGEMENT LETTER 2.27, 2.70, 2.74

ENGAGING PARTY
- Signing of engagement letter 2.74
- Written representation when not responsible party 3.212

ENTERPRISE IT OUTSOURCING SERVICES, DEFINED 1.02

EVIDENCE. *See* audit evidence

EXPECTED KNOWLEDGE OF SPECIFIED PARTIES 1.08–.13

EXTENDING OR MODIFYING THE PERIOD COVERED BY THE EXAMINATION 2.79–.90

F

FINANCIAL TECHNOLOGY (FINTECH) SERVICES 1.02

FRAUD CONSIDERATION
- Operating effectiveness of controls evaluation 3.162
- Planning the examination 2.122
- Responding to and communicating known or suspected fraud 3.190–.196
- Suitability of design of controls evaluation 3.86, 3.162
- Written representations about fraud 3.203

H

HEALTH CARE CLAIMS MANAGEMENT AND PROCESSING, DEFINED 1.02

I

INCLUSIVE METHOD
- Defined 2.12
- Description of the system, contents of 3.43–.45
- Design of controls for subservice organization, evaluating 3.81
- Illustrative service auditor's report ..... Appendix D-2
- Management responsibilities in deciding on 2.12–.16
- Operating effectiveness of controls for subservice organization, evaluating 3.81
- Planning considerations for using 2.96–.103
- Subservice organization's management responsibilities 2.28

INDEPENDENCE OF SERVICE AUDITORS
- Accepting a SOC 2® examination engagement 2.05, 2.35–.38
- Other practitioner consideration 2.156
- Specialist, use of 2.162–.163
- Subservice organizations consideration 2.15, 2.37

INFRASTRUCTURE, DEFINED 1.20

INHERENT RISK, DEFINED 2.124

INTENDED USERS. *See also* user entities
- Business partners 1.01–.04, 1.09, 1.10,
- Description criteria as based on informational needs of 3.67
- In engagement acceptance and continuance 2.47–.48
- Expected knowledge of 1.08–.13
- Auditor report considerations 1.07–.13
- Need for subservice organization information 3.48
- Service auditor's evaluation of design of controls to serve 3.163

INTERNAL AUDIT FUNCTION, USING WORK OF 3.166–.177
- Direct assistance from ..... 3.176–.177, ... 4.24–.26
- Evaluating adequacy of work of ... 3.170–.174

INTERNAL AUDIT FUNCTION, USING WORK OF—continued
- Including in terms of engagement 2.72
- Management's responsibility to assist in service auditor's use of 2.26
- Nature, timing, and extent of procedures 3.168
- Operating effectiveness of controls 3.169
- Planning to use 2.112, 2.132–.153
- Professional judgment of service auditor in 2.145–.147, 3.170, 3.175
- Reperformance testing in ... 3.167–.168, 4.26
- Reporting on results of tests of controls 4.23–.27

INTERNAL CONTROL OVER FINANCIAL REPORTING (SOC 1® EXAMINATION) .... 1.60–.61, Appendix B

IT PROCESSING, TESTS OF AUMOMATED CONTROLS 3.138

L

LAWS OR REGULATIONS, COMPLIANCE WITH
- Noncompliance issues in examination ..... 2.122, 3.158, 3.163, ... 3.190–.196
- Service organizations objectives and 1.44
- Written representations 3.201

M

MANAGED SECURITY, DEFINED 1.02

MANAGEMENT ASSERTIONS. *See also* written assertions
- Additional subject matters and criteria ... 1.51
- Components of ..... 1.16, Table 1-1 at 1.18
- Illustrative examples ..... Appendix D, ... Appendix E, Appendix F
- Modification due to misstatements or deficiencies 3.226–.229, 4.38
- Reasonable basis for, determining ..... 2.26, ... 2.49–.56
- SOC 3® report 1.56, 4.111, 4.112–.114
- Subsequent event effects 3.213–.219

MANAGEMENT OF SERVICE ORGANIZATION
- Additional subject matters and criteria for service auditor 1.51
- Agreement with service auditor on intended users 1.08
- Changes to the system during the period 3.62
- Communication of user entity responsibilities 3.38–.41
- Description of the system from ... 1.16, 2.26, ... 2.117
- Design of controls 3.80
- Disclosure requirements to service auditor 2.26
- Distribution of service auditor's report by 1.13, 4.91–.93

MANAGEMENT OF SERVICE ORGANIZATION—continued
- Information for ..... Appendix A
- Privacy disclosures 2.61
- Response to deviations in tests of controls 4.20–.21
- Responsibilities in SOC 2® examination .... 1.16, 1.32, 1.45, 2.03–.29, ... 2.117, 3.13, Appendix A, ... Table 4-3 at 4.32
- Responsibilities in SOC 3® examination 2.167–.171
- Risk identification by 1.42, 2.26, 2.52–.53
- Role in use of other practitioner 2.157
- Changes in terms of engagement ..... 2.75, ... 4.57
- Subservice organization evaluation by 2.98
- Written representations. *See* written representations

MANAGEMENT OF SUBSERVICE ORGANIZATION
- Identification of controls for implementation 2.24–.25
- Responsibilities of 2.28, 2.101

MANAGEMENT OF USER ENTITY OR BUSINESS PARTNER, INTEREST IN SERVICE ORGANIZATION'S CONTROLS. *See also* user entities 1.01–.04

MATERIAL DEFICIENCIES
- Extended or modified period covered by examination 2.88
- Operating effectiveness of controls 4.83–.88
- Suitability of design of controls 4.79–.82

MATERIAL MISSTATEMENT, RISK OF
- Concluding on sufficiency and appropriateness of evidence 4.05–.06
- Considering uncorrected description misstatements and deficiencies ..... 4.10, ... 4.68–.78
- Due to fraud. *See* fraud consideration
- Modified opinion type ..... Table 4-4 at 4.47
- Performing the examination 3.01–.04
- Planning the examination ..... 2.111, ... 2.120–.126
- Revising the risk assessment 3.181

MATERIALITY
- Adverse opinion basis 4.54–.55
- Description of service organization's system 3.07, 3.72–.78
- Evaluating suitability of design and operating effectiveness of controls 3.161-3.165
- Considerations during planning ... 2.104–.109
- Reporting results of tests of controls 4.16
- In responding to assessed risks and planning procedures 3.05–.08

MEASURABILITY, IN DESCRIPTION OF THE SYSTEM 4.71

MISSTATEMENTS. *See also* material misstatement, risk of
- Defined 3.09
- Identifying and evaluating ..... 3.09–.11, ... 3.64–.71, 3.184–.189, 3.193–.196
- Pervasive effects on subject matter 3.186–.187, 4.45, 4.54, 4.58
- Responding to other information included with auditor's report 4.102, 4.104
- Uncorrected ..... 3.193–.196, 4.10–.12, ... 4.68–.78

MODIFICATIONS TO SERVICE AUDITOR'S REPORT (SOC 2®) ..... 4.43–.88, ... Table 4-4 at 4.47
- Adverse opinion 3.29, 4.14, 4.54–.55
- Considering linkages among subject matters 4.14
- Criteria for 4.43–.44
- Description material misstatements, illustrative separate paragraphs 4.68–.78
- Disclaimer of opinion. *See* disclaimer of opinion
- Modified opinion ..... 3.10, 3.11, 3.29, 3.71, ... 3.185, 3.189, 4.43–.47
- Operating effectiveness of controls, illustrative separate paragraphs 4.83–.88
- Qualified opinion ..... 3.137, 4.14, 4.51–.53, ... 4.59–.60
- Qualitative and quantitative factors 4.50
- Scope limitation ..... 4.56–.60, 4.82, ... 4.85, Table 4-4 at 4.47
- SOC 3® report 4.118
- Suitability of controls, illustrative separate paragraphs 4.79–.82
- Testing of controls 3.119

N

NONCOMPLIANCE WITH LAWS OR REGULATIONS 2.122, 3.190–.196

O

OPERATING EFFECTIVENESS OF CONTROLS (TYPE 2 EXAM). *See also* tests of controls 3.106–.146
- Considering request to extend or modify period 2.80
- Controls not operating during examination period 3.156
- Deficiencies distinguished from those for design of controls 3.102
- Deviations in, identifying and evaluating 3.157–.160
- Entity-level controls 2.127–.131
- Impact of suitability of design of controls on 3.109
- Internal audit function, using work of 3.169
- Material deficiencies noted in service auditor's report 4.83–.88

OPERATING EFFECTIVENESS OF CONTROLS (TYPE 2 EXAM)—continued
- Materiality considerations 3.162, 3.164
- Monitoring as internal control function 2.119
- Scope limitation, illustrative separate paragraphs 4.85
- Service auditor's engagement requirements 1.06, 1.17
- Subservice organizations ...3.81, 3.153–.154
- Superseded controls in ...3.108, 3.140–.141
- Trust services criteria ...1.32–.35, 1.40–.43, ... 3.107, Table 1-2 at 1.41

OPINION, SERVICE AUDITOR'S
- Adverse 3.29, 4.14, 4.54–.55
- Disclaiming of. *See* disclaimer of opinion
- Evaluating the results of procedures performed 3.183
- Extended or modified period consideration 2.84
- Forming the opinion for service auditor's report .....4.04–.14, Table 4-3 at 4.32
- Illustrative .....Appendix D
- Modified. *See also* modifications to service auditor's report .....3.10, 3.11, 3.29, 3.71, ... 3.185, 3.189, 4.43–.47, 4.118
- Qualified ... 3.137, 4.14, 4.51–.53, 4.59–.60
- Service auditor's engagement requirements 1.06, 2.64
- SOC 3® report .....1.13, 4.111, 4.115, ... Table 4-4 at 4.116
- Type 1 and type 2 SOC 2® requirements .....Table 1-1 at 1.18

OTHER-MATTER PARAGRAPHS, IN SERVICE AUDITOR'S REPORT 4.89–.90

OTHER PRACTITIONER, USING WORK OF 2.154–.159, 4.42

OUTSOURCING. *See also* subservice organizations 1.01–.02, 2.06

P

PEOPLE, AS SYSTEM COMPONENT 1.20

PERFORMING A SOC 2® EXAMINATION 3.01–.229
- Applicable trust services criterion, multiple controls for 3.92–.94
- Business partner and vendor risks 3.147–.151
- Changes to the system during period covered by type 2 exam ..... 3.55–.56, 3.62, ... 3.108, 3.140–.141
- Changes to the system occurring between periods covered by type 2 exam ...3.57–.58
- Controls not operating during examination period 3.156
- CUECs and user entity responsibilities 3.36–.41

PEOPLE, AS SYSTEM COMPONENT—continued
- Deficiencies in controls .....3.101–.105, ... 3.193–.196
- Description of the system, evaluating and obtaining evidence 3.12–.78
- Design of controls, evaluating suitability of 3.79–.105
- Deviations in controls 3.157–.160
- Disclosures about individual controls ..... 3.30–.32, Table 3-1 at 3.30
- Documentation 3.221–.225
- Fraud consideration 3.190–.196
- Internal audit function, using work of 3.166–.177
- Management assertions, need for modification in 3.226–.229
- Materiality considerations .....3.05–.08, ... 3.72–.78, 3.161–.165
- Misstatements, identifying and evaluating .....3.09–.11, 3.64–.71, ... 3.184–.189, 3.193–.196
- Noncompliance with laws or regulations 3.190–.196
- Operating effectiveness of controls. *See also* tests of controls .....3.106–.146, ... 3.153–.154, 3.156–.165
- Reliability of information produced by service organization, evaluating 3.121–.130
- Responding to and communicating resulting issues 3.190–.196
- Results of procedures, evaluating 3.182–.189
- Revising the risk assessment 3.181
- Service commitments and system requirements 3.24–.29
- Specialist, using work of 3.178–.180
- Subsequent events and subsequently discovered facts 3.213–.220
- Subservice organizations .....3.42–.54, ... 3.88–.91, 3.99–.100, 3.152–.155
- Suitability of design of controls, evaluating 3.79–.105
- Uncorrected misstatements 3.193–.196
- Written representations, obtaining from management 3.197–.212

PERIODS. *See also* subsequent events
- Changes to the system between 3.57–.58
- Changes to the system during .....3.55–.56, ... 3.62, 3.108, 3.140–.141
- Controls that did not operate during 3.156
- Controls not suitably designed during portion of period 4.81
- Date of service auditor's report .....Table 4-3 at 4.32, ... Table 4-4 at 4.116
- Evidence from prior periods, in tests of controls 3.136–.137

PERIODS—continued
· Extending or modifying the period covered by the examination 2.79–.90
· Interim tests of controls 3.132
· Threats related to prior periods 3.163

PLANNING A SOC 2® EXAMINATION 2.91–.166
· Entity-level controls consideration 2.127–.131
· Inclusive method for presenting services of subservice organization 2.96–.103
· Internal audit function, understanding and planning to use 2.112, 2.132–.153
· Materiality consideration 2.104–.109
· Other practitioner, using work of 2.154–.159
· Performing risk assessment procedures 2.110–.126
· Service auditor's specialist, using work of 2.160–.166
· Strategy for examination 2.91–.95

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS. *See* service commitments and system requirements

PRIOR ENGAGEMENTS, EVIDENCE FROM 3.137

PRIVACY
· Applicable trust services criteria ..... Table 1-2 ..... at 1.41, Supplement B
· Boundaries of the system and 1.23
· Confidentiality distinguished from 1.25–.26
· Defined 1.37
· Service organization controls relevant to 1.04
· Service organization management disclosures relevant to 2.61

PROCESSING INTEGRITY
· Applicable trust services criteria ..... Table 1-2 ..... at 1.41, Supplement B
· Boundaries of the system and 1.22
· Defined 1.22, 1.37
· Service organization controls relevant to 1.04

PROFESSIONAL JUDGMENT
· Engagement acceptance and continuance 2.77
· Extent of sampling in tests of controls 3.144
· Internal audit function, using work of 2.145–.147, 3.170, 3.175
· Materiality consideration 2.107
· Modification of opinion basis 4.45
· Reliability of information produced by service organization 3.129
· Sufficiency and appropriateness of evidence 4.09

PROSPECTIVE USER ENTITIES OR BUSINESS PARTNERS 1.10

Q

QUALIFIED OPINION ..... 3.137, 4.14, ... 4.51–.53, 4.59–.60

QUALITATIVE AND QUANTITATIVE FACTORS
· In modifications to the service auditor's report 4.50
· Suitability of design of controls, evaluating 3.163–.164

QUALITY CONTROL CONSIDERATION ... 1.74–.76, 2.31–.34, ... 2.39–.42

R

REASONABLE BASIS FOR MANAGEMENT ASSERTION, DETERMINING ..... 2.26, ... 2.49–.56

REGULATORS, AS SPECIFIED PARTIES IN SERVICE ORGANIZATION RELATIONSHIP 1.09

REPERFORMANCE TESTING, IN USING THE WORK OF THE INTERNAL AUDIT FUNCTION 3.167–.168, 4.26

REPORT USERS, DEFINED. *See also* intended users 3.12

REPORTING. *See* service auditor's report

REPRESENTATION LETTER. *See* written representations

RESPONSIBLE PARTY
· Independence of service auditor in relation to 2.37
· Subservice organization as. *See also* management of service organization ... 2.96
· Written representation from engaging party that is not 3.212

RESTRICTIONS ON USE OF SERVICE AUDITOR'S REPORT
· SOC 2® report ..... 1.11–.12, 4.33–.35, ... 4.91–.93
· SOC 3® report 4.117

RISK ASSESSMENT
· Entity-level controls 2.127–.131
· Expected knowledge of intended users and 1.08
· Generally 1.03–.04
· Material misstatement, risk of. *See* material misstatement, risk of
· Planning SOC 2® examination procedures 2.104–.126
· Revising 3.181
· Service auditor's evaluation of 3.82–.84
· Business partners and vendor risk 3.147–.151
· By user entity management 1.04

S

SAMPLING. ***See*** **audit sampling**

SCOPE OF ENGAGEMENT
- Information not covered by service auditor's report 4.95–.104
- Change in terms of examination 2.75
- Modifications to service auditor's report due to limitation on ..... 4.56–.60, 4.82, ... 4.85, Table 4-4 at 4.47
- Service auditor's response to limitation on ..... 3.211, Appendix D-3
- SOC 3® .....Table 4-4 at 4.116

SCOPE LIMITATION
- Changed engagement 2.77
- Modify the service auditor's opinion 3.141
- Disclaim an opinion .....3.192, 3.211, ... 4.65, Appendix D-3
- Generally 4.56-4.60,
- Related to suitability of design of controls 4.82
- Related to suitability of operating effectiveness 4.85
- SOC 3® 4.117

SECURITY
- Applicable trust services criteria .....Table 1-2 ..... at 1.41, Supplement B
- Boundaries of the system and 1.22
- Defined 1.37
- Evaluating controls for 3.163
- Service organization controls relevant to 1.04

SERVICE AUDITORS
- Acceptance and continuance 2.30, 2.74
- Additional subject matters and criteria procedures .....1.50–.54, Table 1-3 at 1.50
- Agreeing on terms of engagement ...2.70–.74
- Agreement with management on intended users 1.08
- Changes to terms of engagement, considering 2.75–.78
- Confidentiality in regard to client information 3.195–.196
- Considering request to extend or modify period 2.79–.85
- Documentation responsibilities of 3.222
- Engagement requirements in type 2 examination 1.06, 1.17
- Independence of. *See* independence of service auditors
- Opinion from. *See* opinion
- Performing the examination. *See* performing a SOC 2 examination
- Planning the examination 2.91–.126
- Professional judgment. *See* professional judgment
- Reporting responsibilities of. *See also* service auditor's report ..... 4.01–.03, ... Table 4-3 at 4.32

SERVICE AUDITORS—continued
- Responsibilities of, generally 1.17, 2.30
- SOC 3® examination responsibilities 2.172
- Subsequent event responsibilities 3.215–.217
- Tests of controls responsibilities ..... 1.53, ... 3.110, 3.115–.120
- Withdrawal from engagement ..... 2.68, 2.78, ... 3.229

SERVICE AUDITOR'S ENGAGEMENTS

SERVICE AUDITOR'S REPORT (SOC 2®). ***See also*** **SOC 1® examination and report; SOC 3® report 4.01–.116**

Additional subject matters and criteria ..... 1.52–.54, Table 1-3 at 1.50
- Assessing usefulness of separate reports 2.114
- Carve-out method at subservice organization ..... 4.32, 4.39–.41, ... Appendix D-1
- Contents of .....Table 1-1 at 1.18
- On controls not operating during reporting period 3.156
- CUECs 4.36–.38
- Date of report ..... Table 4-3 at 4.32
- Defined 1.04
- Determining appropriateness for intended users 2.47–.48
- Disclaims an opinion because of a scope limitation ..... Appendix D-3
- Distribution of report by management 4.91–.93
- Elements of ..... 4.31–.32, Table 4-3 at 4.32
- Emphasis-of-matter and other-matter paragraphs 4.89–.90
- Forming the opinion. *See also* opinion, service auditor's 4.04–.14
- Information accompanying but not covered by 4.95–.104
- Inclusive method, illustrative report ..... Appendix D-2
- Illustrative type 2 report, Appendix D-4
- Intended users of 1.07–.13
- Internal audit function, using work of 4.23–.27
- Materiality in 4.16, 4.54–.55
- Modifications to. *See* modifications to service auditor's report
- Other practitioner in 2.156, 4.42
- Recommendations for improving controls 4.94
- Describing tests of reliability of information produced by service organization 4.28–.30
- Responsibilities of service auditor ... 4.01–.03
- Restrictions on use of report .....1.11–.12, ... 4.33–.35, 4.91–.93
- Risk assessment 1.04

Additional subject matters and criteria—continued
· SOC 3® reports distinguished from 1.55–.57
· Tests of controls and results of tests .... 4.15–.30, 4.42, Table 4-1 at 4.15, ... Table 4-2 at 4.17, Table 4-3 at 4.32
· Type 1 and type 2. *See* type 1 SOC 2® examination and report; type 2 SOC 2® examination and report

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS
· In description of the system .....1.44–1.49, ... 2.59–.65, 3.24–.29, Appendix D
· Evaluating appropriateness in accepting engagement 2.59–.65
· Generally 1.44–.49, 2.04
· Management responsibility for 2.04, 3.13
· Relevance of controls to achievement of 3.163
· SOC 3® report 4.112, 4.115

SERVICE ORGANIZATIONS 1.01–.77
· Commitments to user entities. *See also* service commitments and system requirements 1.44–.46, 1.49
· Controls responsibilities 1.40
· Defined 1.01
· Description. *See* description of service organization's system
· Management of. *See* management of service organization
· Other information accompanying auditor's report 4.95–.104
· Outsourcing. *See also* subservice organizations 1.01
· System. *See* system, service organization's
· Types of services provided 1.02
· User entities 1.01–.13

SOC 1® EXAMINATION AND REPORT (SOC FOR SERVICE ORGANIZATIONS: ICFR) .....1.60–.61, Appendix B

SOC 2® EXAMINATION. *See also* performing a SOC 2® examination; service auditor's engagements
· Accepting an engagement. *See* accepting a SOC 2® examination engagement
· Additional subject matter and additional criteria ..... 1.50–.54, Table 1-3 at 1.50
· Applicable trust services criteria ..... 1.05, ... 1.08, 1.27, Table 1-1 at 1.18, ... Supplement B
· Boundaries of the system and 1.21–.23
· Categories of criteria ..... 1.37–.38, 1.41, ... 4.76, Table 1-2 at 1.41
· Common criteria ..... 1.39–.43, ... Table 1-2 at 1.41
· Criteria for. *See also* description criteria; trust services criteria 1.27–.43

SOC 2® EXAMINATION—continued
· Cybersecurity risk management examination and report, distinguished from ... Appendix C
· Defined 1.04
· Distinguishing between confidentiality and privacy 1.25–.26
· Overview of 1.14–.49
· Performing the examination. *See* performing a SOC 2® examination
· Planning the examination. *See* planning a SOC 2® examination
· Professional standards applicable to 1.69–.76
· Scope of and boundaries of the system 1.23
· Scope of as set by management 2.04
· System definition 1.19–.20
· Time frame of 1.24
· Trust services criteria. *See* trust services criteria
· Type 1 distinguished from type 2 ... 1.05–.06, ... 1.14, 1.16–.17
· Use of SOC 2® reports internationally, Appendix H

SOC 2® REPORT. *See* service auditor's report

SOC 3® EXAMINATION
· Generally 1.55–.58
· Management's responsibilities 2.167–.171
· Service auditor's responsibilities 2.172
· SOC 2® engagements distinguished from ..... 1.55, Appendix B

SOC 3® REPORTS
· Elements of ..... 4.110–.116, ... Table 4-4 at 4.116
· Illustrative report .....Appendix F
· Management assertion, illustrative ..... Appendix F
· Modification of opinion on effectiveness of controls 4.118
· Restricting distribution of 4.117
· SOC 2® reports distinguished from ..... 1.55–.57, Appendix B

SOC FOR CYBERSECURITY 1.63–.68

SOC SUITE OF SERVICES 1.59–.68

SOFTWARE, AS SYSTEM COMPONENT 1.20

SPECIALIST, USING WORK OF 2.160–.166, 3.178–.180

SPECIFIED PARTIES. *See* intended users

SUBJECT MATTERS OF A SOC 2® EXAMINATION
· Addressing additional .....1.50–.54, ... Table 1-3 at 1.50
· Description of the system. *See* description of service organization's system
· Design of controls. *See* suitability of design of controls

SUBJECT MATTERS OF A SOC 2® EXAMINATION—continued
- Determining appropriateness of 2.44–.56
- Effectiveness of controls. *See* operating effectiveness of controls
- Evaluating pervasive effects of misstatements on 3.186–.187, 4.45, 4.54, 4.58
- Expressing the opinion on 4.13–.14
- Generally 1.05
- Management's written representations on 3.201, 3.205
- Service auditor's exam responsibilities ... 3.11
- Service auditor's report ..... Table 4-3 at 4.32

SUBSEQUENT EVENTS AND SUBSEQUENTLY DISCOVERED FACTS 3.213–.220

SUBSERVICE AUDITOR, USING WORK OF 2.157

SUBSERVICE ORGANIZATIONS
- Auditor independence from 2.15, 2.37
- Carve-out method. *See* carve-out method
- Controls of 2.06–.10, 3.43–.54
- Defined 2.06–.07
- In description of the system ..... 2.11–.16, ... 2.24–.25, 3.42–.54, 4.75
- Identification of complementary controls by service organization's management 2.17–.19
- Identification of controls for service organization to implement 2.24–.25
- Illustrative auditor's reports ..... Appendix D
- Inclusive method. *See* inclusive method
- Management responsibilities of ... 2.28, 2.101
- Not disclosed in description of the system, illustrative separate paragraph 4.75
- Operating effectiveness of controls, evaluating 3.81, 3.153–.154
- Planning for multiple 2.97
- As responsible parties 2.96
- In risk assessment 2.123, 3.82
- Service auditor's report ..... Table 4-3 at 4.32
- Service organization management's identification and evaluation of .... 2.06–.11, ... 2.98
- Suitability of design of controls, evaluating ..... 2.16, 3.86, 3.88–.91, ... 3.99–.100, 3.152
- Written assertions 2.28, 2.100, 2.103
- Written representations 2.28, 3.206

SUITABILITY OF CRITERIA, ASSESSING. *See also* description criteria; trust services criteria 2.57–.58

SUITABILITY OF DESIGN OF CONTROLS 3.79–.105
- Multiple controls to address applicable trust services criteria 3.92–.94, 3.114
- CUECs and 3.86, 4.36–.38
- Deficiencies, identifying and evaluating 3.101–.105, 4.79–.82

SUITABILITY OF DESIGN OF CONTROLS—continued
- Defined 1.34
- Fraud consideration 3.86, 3.162
- Generally 3.79–.87
- Illustrative separate paragraph 4.82
- Impact on evaluation of operating effectiveness of controls 3.109
- Intentional and unintentional acts in .... 3.163, ... 3.190
- Materiality considerations ..... 3.104, ... 3.161–.165
- Not suitably designed, illustrative separate paragraph 4.79–.82
- Procedures to obtain evidence 3.95–.100
- Qualitative and quantitative factors 3.163–.164
- Service auditor's engagement requirements 1.06
- Subservice organizations ..... 2.16, 3.86, ... 3.88–.91, 3.99–.100, 3.152
- Trust services criteria ... 1.32–.35, 1.40–.43, ... 3.94, Table 1-2 at 1.41
- Unknown threats and vulnerabilities 3.163

SUPERSEDED CONTROLS, IN OPERATING EFFECTIVENESS OF CONTROLS EVALUATION 3.108, 3.140–.141

SYSTEM
- Boundaries of the system .... 1.21–.23, 2.45, ... 2.113, 3.32
- Changes between periods 3.57–.58
- Changes during the period ... 3.55–.56, 3.62, ... 3.108, 3.140–.141
- Components of 1.20
- Controls for. *See* controls
- Defined 1.19–.20
- Description of. *See* description of service organization's system
- Objectives for 1.44
- Obtaining an understanding of 2.110–.119
- Requirements of. *See* service commitments and system requirements

SYSTEM AND ORGANIZATION CONTROLS (SOC). *See* SOC Suite of Services

SYSTEM INCIDENT DISCLOSURES 3.33–.35

T

TERMS OF ENGAGEMENT
- Agreeing on for a SOC 2® engagement 2.32, 2.70–.90
- Changes in 2.75–.78

TESTS OF CONTROLS 3.110–.146
- Audit sampling 3.142–.146
- Designing and performing 3.110–.114

TESTS OF CONTROLS—continued
- Deviations and deficiencies analysis 3.157–.160, 3.185–.189
- Extent of 3.134–.139, 4.18
- Internal auditor, using work of ... 3.167–.168, ... 4.23–.27
- Nature of 3.115–.120
- Reliability of information produced by service organization 3.121–.130
- Reporting tests and results in type 2 report ... 4.15–.30, 4.42, Table 4-1 at 4.15, ... Table 4-2 at 4.17, Table 4-3 at 4.32
- Service auditor's responsibilities ..... 1.53, ... 3.110, 3.115–.120
- Superseded controls 3.140–.141
- Timing of 3.131–.133
- Type of control and best procedure to test 3.118

TRUST SERVICES CATEGORIES. *See also* specific categories by name ..... 1.37–.38, 1.41, 1.46, ... 4.76, Table 1-2 at 1.41

TRUST SERVICES CRITERIA Supplement B
- Applicable trust services criteria ..... 1.05, ... 1.32, 3.92–.94, 4.77, Table 1-2 at 1.41, ... Table 4-4 at 4.116, Supplement B
- Assessing suitability of 2.57–.58
- Categories 1.37-1.38
- Common criteria 1.39-1.42
- Confidentiality criteria 1.25–.26
- Description of the system including irrelevant data, illustrative separate paragraph 4.87–.88
- Generally ..... 1.05, 1.08, 1.27, 1.31–.36, Supplement B
- Multiple controls to address an applicable trust services criterion 3.92-.94
- Operating effectiveness of controls ..... 1.32–.35, 1.40–.43, ... 3.107, Table 1-2 at 1.41
- Privacy criteria 1.25–.26
- Resource for ..... Supplement B
- Service commitments and system requirements 2.63–.64
- Suitability of design of controls ..... 1.32–.35, ... 1.40–.43, 3.94, Table 1-2 at 1.41

TYPE 1 SOC 2® EXAMINATION AND REPORT
- Contents of ..... 4.107–.109, ... Table 1-1 at 1.18, Appendix E
- Time frame for examination 1.24
- Type 2 SOC 2® examination distinguished from 1.05–.06, 1.14, 1.16–.17

TYPE 2 SOC 2® EXAMINATION AND REPORT. *See also* service auditor's report
- Changes to the system occurring between periods 3.57–.58
- Contents of ..... Table 1-1 at 1.18

TYPE 2 SOC 2® EXAMINATION AND REPORT—continued
- Defined 1.05
- Extending or modifying the period covered by 2.79–.90
- Illustrative ..... 4.105–.106, Appendix D
- Operating effectiveness of controls. *See* operating effectiveness of controls
- System changes implemented during the period 3.62, 3.108, 3.140–.141
- Tests of controls. *See* tests of controls
- Time frame for examination 1.24
- Type 1 SOC 2® examination distinguished from 1.05–.06, 1.14, 1.16–.17

U

USER ENTITIES
- Boundary of the system, clarity of reporting on 1.21
- Business relationships with service organizations 1.01–.13
- Categories of 1.09
- Controls. *See* complementary user entity controls
- Defined 1.01
- Management of 1.04
- Prospective 1.10
- Responsibilities of ..... 1.03, 1.08, 2.20–.23, ... 3.36–.41
- Risk assessment 1.04
- Service commitments and system requirements ..... 1.44–1.49, 2.59–.65, ... 3.24–.29

V

VENDOR AND BUSINESS PARTNER RISKS, CONSIDERATION OF. *See also* subservice organizations 3.147–.151

W

WRITTEN ASSERTIONS. *See also* management assertions
- To accompany description of service organization system 2.26
- Elements of 1.16
- Management refusing to provide ..... 2.68, ... 4.64–.67
- Requesting of service organization management 2.66–.69
- SOC 3® report 1.56
- From subservice organization's management 2.28, 2.100, 2.103

WRITTEN REPRESENTATIONS ... 3.197–.212
- At conclusion of engagement 2.26
- For extended or modified period 2.86
- Illustrative examples ..... Appendix G

WRITTEN REPRESENTATIONS—continued

- Management's refusal to provide ..... 3.211, ... 4.66
- Not provided or not reliable 3.209–.211
- Requesting of service organization management 2.66–.69

WRITTEN REPRESENTATIONS—continued

- On subject matters of the examination 3.201, 3.205
- Subservice organizations 2.28, 3.206
- When engaging party is not responsible party 3.212

